Mehr Sicherheit im Umgang mit dem World Wide Web

Knowhow für junge User

Materialien für den Unterricht

klicksafe wird kofinanziert von der Europäischen Union

überreicht von:

lfm: Landesanstalt für Medien Nordrhein-Westfalen (LfM)

MEDIENSCOUTS NRW
Ein Angebot der Landesanstalt für Medien Nordrhein-Westfalen (LfM)

klicksafe.de
Mehr Sicherheit im Internet durch Medienkompetenz

Titel:
Knowhow für junge User
Mehr Sicherheit im Umgang mit dem World Wide Web.
Materialien für den Unterricht.

AutorInnen:
Marco Fileccia, Birgit Kimmel, Stefanie Rack, Isabell Tatsch, Friederike Groschup

Unter Mitarbeit von:
Ina Brecheis, Annalena Artner und Thea Rohn

Verantwortlich:
Birgit Kimmel, Päd. Leitung klicksafe

1. vollständig überarbeitete Auflage März 2016
Erstauflage Mai 2008

Herausgeber:
klicksafe ist das deutsche Awareness Centre im CEF Telecom Programm der Europäischen Union. klicksafe wird gemeinsam von der Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz (Koordination) und der Landesanstalt für Medien Nordrhein-Westfalen (LfM) umgesetzt.

Koordinator klicksafe:
Peter Behrens, LMK

The project is co-funded by the European Union
http://ec.europa.eu/saferinternet

Verbindungsbüro Berlin:
LMK/Safer Internet DE/klicksafe
c/o die medienanstalten
Gemeinsame Geschäftsstelle der Landesmedienanstalten
Friedrichstraße 60, 10117 Berlin

Bezugsadresse:

Landesanstalt für Medien
Nordrhein-Westfalen (LfM)
Zollhof 2
40221 Düsseldorf
Email: medienkompetenz@lfm-nrw.de
Online-Bestellsystem:
www.lfm-nrw.de/publikationen

Dieses Modul steht unter der obigen Creative-Commons-Lizenz, d.h., die nichtkommerzielle Nutzung und Verbreitung ist unter Angabe der Quelle klicksafe und der Webseite www.klicksafe.de erlaubt.
Sollen über die genannte Lizenz hinausgehende Erlaubnisse gewährt werden, können Einzelabsprachen mit klicksafe getroffen werden. Wenden Sie sich dazu bitte an info@klicksafe.de.

Weitere Informationen unter:
https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de
Es wird darauf verwiesen, dass alle Angaben in diesem Modul trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung der Autoren ausgeschlossen ist.

Hinweis:
Männliche/weibliche Form: Die auf den meisten Seiten verwendete männliche Form impliziert selbstverständlich die weibliche Form. Auf die Verwendung beider Geschlechtsformen wird lediglich mit Blick auf die bessere Lesbarkeit des Textes verzichtet.

Layout und Umschlaggestaltung:
Designgruppe Fanz & Neumayer
Ludwigshafen und Heidelberg

Knowhow für junge User

Mehr Sicherheit im Umgang mit dem World Wide Web
Materialien für den Unterricht

AutorInnen:
Marco Fileccia, Birgit Kimmel, Stefanie Rack, Isabell Tatsch, Friederike Groschup

klicksafe.de

Überreicht von:

lfm: Landesanstalt für Medien Nordrhein-Westfalen (LfM)

MEDIENSCOUTS NRW
Ein Angebot der Landesanstalt für Medien Nordrhein-Westfalen (LfM)

Ob zu Hause auf der Couch, beim Warten auf den Bus oder kurz vor der Schule – das Internet ist aus unserem Alltag nicht mehr wegzudenken. Mit Laptops, Tablet-PCs und Smartphones steht auch Kindern und Jugendlichen das Internet nahezu überall und ständig zur Verfügung und damit auch die Möglichkeit, jederzeit mobil ins Internet zu gehen, sich mit anderen auszutauschen oder zu spielen.

Das Leben in und mit der digitalen Welt stellt vor allem die Bereiche Bildung und Erziehung vor besondere Herausforderungen und dabei hat die Schule eine Schlüsselrolle inne.

Hier besteht die Möglichkeit, frühzeitig die Grundlagen für einen kompetenten Umgang mit den digitalen Medien zu legen, denn in Schulen können alle Kinder und Jugendliche erreicht werden. Je früher ein reflektierter und kritischer Umgang mit dem Internet und den digitalen Medien eingeübt und für Chancen und Risiken sensibilisiert wird, desto nachhaltiger und substanzieller kann sich Medienkompetenz aufbauen.

Doch kennen und verstehen Eltern und Lehrkräfte angesichts einer sich täglich verändernden Medienwelt die mediale Lebenswirklichkeit ihrer Kinder noch gut genug? Wie funktionieren WhatsApp, Snapchat oder Instagram, auf was sollte man bei der Nutzung dieser Kommunikationsdienste achten? Wie verhalte ich mich, wenn ich im Internet belästigt und beleidigt werde? Wie schütze ich meine Privatsphäre?

Einen zentralen Aspekt des Auftrages von klicksafe sehen wir in der Information und Schulung von Lehrkräften und Eltern sowie von Pädagogen der außerschulischen Kinder- und Jugendarbeit. Durch die Aufbereitung von leicht verständlichen Hintergrundinformationen und konkreten Praxisprojekten möchte klicksafe Bildungsinstitutionen leicht handhabbares Arbeitsmaterial zur Verfügung stellen, das mit wenig Aufwand in der pädagogischen Praxis eingesetzt werden kann.

Acht Jahre nach der ersten Auflage des klicksafe-Lehrerhandbuchs „Knowhow für junge User" wurde das mittlerweile zum „klicksafe-Bestseller" gewordene Lehrerhandbuch völlig neu bearbeitet und aktualisiert. Das Ergebnis liegt nun vor und möchte wieder eine praxisnahe Einführung in die weiten Felder der digitalen Welten anbieten. Entscheidend ist, dass durch die niedrigschwellige Aufbereitung eine vorherige Schulung oder Fortbildung der Lehrkräfte nicht erforderlich ist. Als Basiswissen für alle Fachrichtungen und Schularten zum Thema Internet bietet auch das „neue" Lehrerhandbuch wichtige Grundlagen und wertvolle Unterstützung im Unterricht an.

Wir würden uns freuen, wenn das aktuelle und neu konzipierte Handbuch, wie auch die Erstauflage, bundesweit in vielen Schulen ein hilfreicher Begleiter für Ihre Arbeit wird. Für Ihre verantwortungsvolle Aufgabe, Kindern und Jugendlichen die umfassenden Aspekte der Chancen und Risiken des Internets näher zu bringen, wünschen wir Ihnen viel Erfolg.

Ludwigshafen und Düsseldorf, im März 2016

Für die EU-Initiative klicksafe

Renate Pepper
Direktorin der Landeszentrale für Medien und Kommunikation (LMK) Rheinland Pfalz

Dr. Jürgen Brautmeier
Direktor der Landesanstalt für Medien Nordrhein-Westfalen (LfM)

Eine Einführung
Das klicksafe-Handbuch richtet sich ausdrücklich an Lehrerinnen und Lehrer aller Fächer und nicht nur an Informatik-, Technik-, Computer-AG- o. ä. Kolleginnen und Kollegen. Wir haben auf eine Fächerzuordnung verzichtet, weil alle 16 Bundesländer z.T. unterschiedliche Bezeichnungen benutzen und aus diesem Grund eine Zuordnung manchmal nicht eindeutig ist.
So kann das Thema Chatten selbstverständlich als moderne Form der Kommunikation in den Fächern Deutsch, Englisch oder Französisch behandelt werden, vielleicht ist sogar ein Latein-Chat denkbar. Aspekte des respektvollen Umgangs miteinander in digitalen Medien (mit dem Thema Mobbing, Anonymität im Netz, Datenschutz) könnten in Sozialkunde, Politik, Gesellschaftslehre aber auch in Religion, Philosophie, Ethik thematisiert werden. Datenschutzrechtliche Aspekte haben sicherlich eine fachliche Heimat in Informatik, Physik, Technik oder in Computer-AGs. Ein Vergleich von Jugendkulturen früher und heute oder die Technikgeschichte lassen sicherlich die Herzen von Geschichtslehrerinnen und -lehrern höher schlagen. Schließlich sind Statistiken zur Beliebtheit des Chattens in der Mathematik auswertbar, Plakate zum sicheren Chatten im Kunstunterricht möglich, ein Theaterstück über das Problem denkbar u. v. a. mehr.
Kurzum, wir wollen Sie in dem fachlichen Einsatz nicht einengen, bringen Ihnen die Themen näher und hoffen auf einen breiten, fächerübergreifenden oder sogar fächerverbindenden Einsatz.

Die Bausteine des klicksafe-Handbuchs
Das Handbuch ist in neun „Bausteine" unterteilt. Jeder Baustein enthält verschiedene Kapitel zu einzelnen Themen. Jedes Kapitel kann unabhängig von den anderen im Unterricht eingesetzt werden.

Sachinformationen
Zu Beginn jedes Kapitels finden Sie Sachinformationen, die Sie auf das Thema einstimmen und informieren, sodass Sie Ihren Schülerinnen und Schülern als frisch gebackene/r Expertin/Experte gegenübertreten können.

Linkliste
Im Anschluss an die Sachinformation finden Sie eine Linkliste, die Sie bei Interesse zur Vertiefung hinzuziehen können. Aufgeführt sind ausschließlich Links zum jeweiligen Kapitel sowie den von uns zur Thematik geprüften und als qualitativ besonders hochwertig erachteten Seiten und Portalen. Dies gilt auch für die Links auf den Arbeitsblättern der Schülerinnen und Schüler. Wir erheben also keinen Anspruch auf Vollständigkeit; Qualität ging uns hier vor Quantität.

Methodisch-didaktische Tabelle
Der methodisch-didaktische Informationsteil gibt Ihnen einen tabellarischen Überblick über Planungsaspekte der Unterrichtsstunde/Unterrichtseinheit und soll Ihnen eine schnelle und effiziente Planung ermöglichen. Hier finden Sie:

- **Kompetenzen**
- **Methoden:** Damit schnell überblickt werden kann, welche Materialien benötigt werden. Viele Methoden orientieren sich am Konzept des „Kooperativen Lernens".
- **Material:** Damit Sie wissen, welche Vorbereitungen Sie treffen müssen (z. B. Filmmaterial downloaden).
- **Zeitaufwand** (in Minuten)
- **Benötigte Zugänge:** Wir haben großen Wert darauf gelegt, mehrere Unterrichtseinheiten auch ohne die Möglichkeit einer PC Benutzung oder/und eines Internetzugangs zu konzipieren, um diese auch im „PC-freien" Unterricht einsetzen zu können.
- **Hinweise für die Durchführung**

Arbeitsblätter
Die Arbeitsblätter sind nach zwei Schwierigkeitsgraden konzipiert.

= leicht

= schwer

Diese Abstufung ist an den Klassenstufen:
4. – 7.Klasse = leicht und
8. – 10. Klasse = schwer orientiert.

Entscheiden Sie aufgrund des Leistungsstandes Ihrer Klasse, welche Arbeitsblätter Sie in welcher Klassenstufe einsetzen.

In diesem Buch werden viele relevante Themen des Jugendmedienschutzes ausführlich behandelt. Jeder Baustein, z. T. auch jedes Kapitel ist so aufgebaut, dass Sie auch nur ein Thema herausnehmen und sich die Inhalte aneignen können, um sie anschließend in Ihrem Unterricht umzusetzen.

Möglichkeiten zur Weiterarbeit
In der Kategorie „Lust auf mehr" finden Sie einige Anregungen, die Lust auf mehr machen sollen, im Sinne einer Vertiefung des Themas im Unterricht z. B.:

- ein Projekt zu dem Thema durchführen
- das Thema zur Weiterbeschäftigung als Hausaufgabe geben
- während des Unterrichts (zum Beispiel für „besonders Schnelle") die Aufgabe als Differenzierungsmöglichkeit einsetzen

Symbole
Überschaubare Informationseinheiten werden mit einem Infokasten, der mit einem Dreieck eingeleitet wird, hervorgehoben:

Tipp: *Facebook bietet z. B. die Funktion* ***Meine Seite für Andere:*** *Das eigene Profil kann aus der Perspektive eines beliebigen anderen Nutzers betrachtet werden. So weiß man, welche Infos den anderen Nutzern zugänglich sind und kann gegebenenfalls Einstellungen anpassen.*

Ein persönlicher Tipp der AutorInnen, Tipps zur inhaltlichen Weiterbeschäftigung mit dem Thema oder Durchführungshinweise werden mit einem Handsymbol eingeleitet:

Aus der Praxis
Selbstverständlich steht in der Schule die kritische Auseinandersetzung mit Computerspielen im Vordergrund. Nicht minder wichtig ist es aber für den Lehrer, sich auf die Welt der Computerspiele einzulassen. Möglich ist das bspw. in sog. LAN-Partys – Computerspiele-Events – für Lehrer und Eltern.

Rechtliche Regelungen und Hintergründe finden sich in einem solchen Kasten:

Der § 202a StGB bezüglich des Ausspähens von Daten besagt:
„(1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft .
(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden."

Baustein 1 | Einstieg: Faszinierendes Internet
1_1 Wo liegt eigentlich das Problem? 9

Baustein 2 | Wie wir finden, was wir suchen: Suchmaschinen und Online-Lexika
2_1 Informationen aus dem Netz 21
2_2 Suchmaschinen 28
2_3 Wikipedia 38

Baustein 3 | Was wir lieben: Mobiles Internet, Kommunikation und Spiele
3_1 Mobiles Internet und Smartphones 53
3_2 Apps 63
3_3 WhatsApp und Co 70
3_4 Skype 76
3_5 Computerspiele 84

Baustein 4 | Wie wir uns vernetzen: Communitys, Nutzerkonten und Mikroblogging
4_1 Soziale Netzwerke: Facebook und Trends 101
4_2 YouTube: Ein Nutzerkonto für alles 113
4_3 Mikroblog: Twitter 123

Baustein 5 | Was wir kennen sollten: Recht und Gesetze im Internet
5_1 Jugendmedienschutz 133
5_2 Urheberrecht und Open Content 145

Baustein 6 | Worauf wir achten sollten: Herausforderungen im Netz
6_1 Cyber-Mobbing 161
6_2 Virtualität und Realität 170
6_3 Online-Sucht 179
6_4 Werbung und Abzocke 188

Baustein 7 | Was wir nicht brauchen: Unerwünschtes und Unnötiges
7_1 Spam und Schadsoftware 201
7_2 Hoaxes, Kettenbriefe und Shitstorms 213
7_3 Illegale Downloads und Tauschbörsen 220

Baustein 8 | Was wir immer tun sollten: Mindestschutz!
8_1 Kritisches Surfverhalten und Passwörter 229
8_2 WLANs und fremde Rechner 241
8_3 Digitaler Fußabdruck 249
8_4 Datensicherung und -löschung 257

Baustein 9 | Was wir beachten müssen: Regelungen für die Schule!
9_1 Spezielle Bestimmungen für die Schule 267
9_2 Datenschutzbestimmungen für Lehrer 271
9_3 Mediennutzung und Aufsichtspflicht 274

Einstieg: Faszinierendes Internet

1

1|1 Wo liegt eigentlich das Problem?

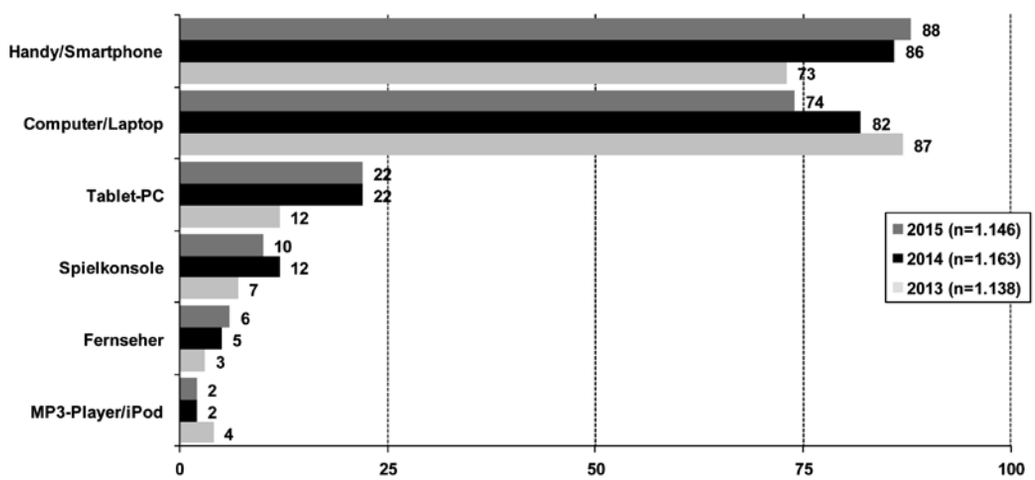
Wo liegt eigentlich das Problem?

Alltagsmedium Internet
Das Internet ist in Deutschland längst ein Alltagsmedium geworden. 79 % der Deutschen sind nach Angaben von **Statista** zumindest gelegentlich online, 58 % sogar täglich[1]. Weltweit nutzt rund mehr als ein Drittel der Menschheit – ca. 2,7 Milliarden Menschen[2] – **das Netz der Netze!**

Mobiles Internet
Ohne Frage übt das Internet vor allem auf Kinder und Jugendliche eine große Faszination aus. Mit Smartphones und einer Daten-Flatrate ausgestattet, sind immer mehr Jugendliche auch unterwegs online. Die Studie **Jugend, Information, (Multi-)Media** (JIM-Studie) des Medienpädagogischen Forschungsverbundes Südwest (MPFS) fragt einmal im Jahr das Mediennutzungsverhalten der Zwölf- bis 19-Jährigen repräsentativ ab. Sie stellte fest, dass die Zahl derjenigen, die das Internet über Smartphones nutzen, bei den Zwölf- bis 19-Jährigen von knapp 50 % im Jahre 2015 auf 88 % in 2015 stieg:

Kommunikation
Die JIM-Studie dokumentiert, dass die Kommunikation der wichtigste Aspekt der Internetnutzung ist: Nach Selbsteinschätzung der Jugendlichen sind sie an einem durchschnittlichen Tag (Mo–Fr) 208 Minuten online[4]. Der Großteil dieser Zeit, im Durchschnitt 40 %, wird darauf verwendet, mit anderen zu kommunizieren. Bei Mädchen liegt dieser Anteil mit 47 % deutlich höher als bei den Jungen mit 34 %[5]. Vor allem die Nutzung von Online-Communitys wie Facebook spielt dabei für viele eine zentrale Rolle. Neben dem Austausch über Online-Communitys bleiben die Jugendlichen über Mails, Chats oder Skype in Kontakt. Unterwegs werden v. a. mittels **WhatsApp** Nachrichten, Bilder und Videos ausgetauscht. Die App erfreut sich bei den Zwölf- bis 19-Jährigen großer Beliebtheit. Laut der JIM-Studie ist die Instant-Messaging App bei 90 % der befragten Jugendlichen die wichtigste App auf ihrem Smartphone[6].

Wege der Internetnutzung 2013–2015
– In den letzten 14 Tagen –



Quelle: MPFS (2015); Angaben in %; Basis: Befragte, die mind. alle 14 Tage das Internet nutzen[3].

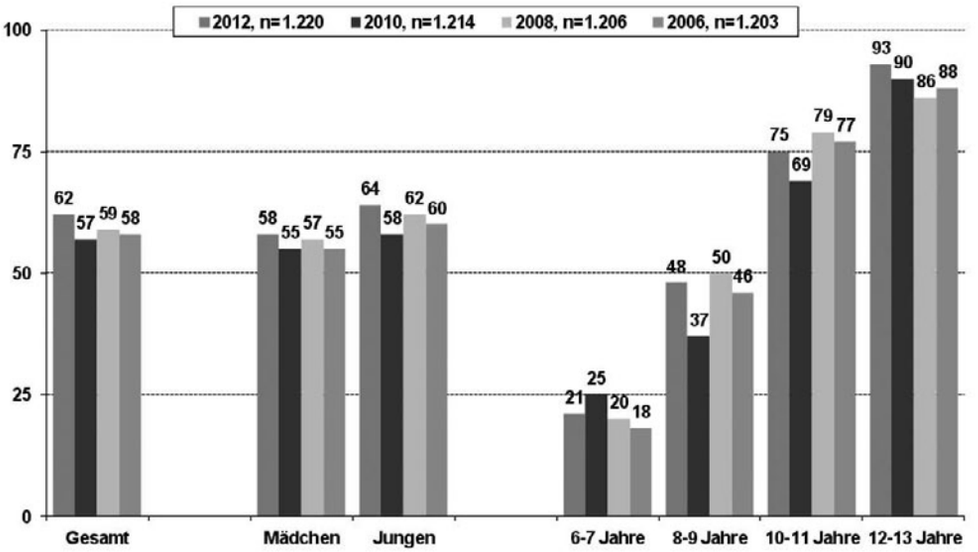
Verfrühungstendenzen

Was die JIM-Studie für Jugendliche, ist die KIM-Studie (= Kinder + Medien, Computer + Internet) für Kinder. Diese fragt als Basisuntersuchung im Zweijahresrhythmus das Mediennutzungsverhalten von Kindern im Alter von 6 bis 13 Jahren ab. Auch hier sind deutliche Trends abzulesen, die man unter **Verfrühungstendenzen** zusammenfassen könnte. So nutzen laut KIM-Studie 2012 bereits über 20 % der Sechs- bis Siebenjährigen das Internet (zumindest selten) und bei den Zehn- bis Elfjährigen sind es drei Viertel:

Besonders auffallend: Facebook ist auch bei den Sechs- bis Dreizehnjährigen die Nummer 1 der beliebtesten Seiten, gefolgt von YouTube (und 2012 noch von dem inzwischen abgeschalteten Sozialen Netzwerk SchülerVZ)[8]. Facebook und YouTube erlauben eine Nutzung aber eigentlich erst ab dem 13. Lebensjahr und das aus gutem Grund: Auf diesen Plattformen erfahren jüngere Kinder keinen ausreichenden Schutz.

Entwicklung Internet-Nutzer 2012–2006

– Nutzung zumindest selten –



Quelle: MPFS (2012); Angaben in %, Basis: alle Kinder[7]

Kinder surfen anders

Erwachsene dürfen nicht den Fehler begehen, Kindern die gleiche Medienkompetenz zu unterstellen und ihren Umgang mit dem Internet mit dem von Kindern zu vergleichen. Kinder surfen anders und sehen sich vielseitigen Herausforderungen ausgesetzt:

- Sie treffen **selten** auf wirklich kindgerechte Seiten
- Sie sind **gefährdet**, denn zahlreiche Seiten bieten jugendgefährdende oder -beeinträchtigende Inhalte
- Sie werden leicht **verführt**, denn redaktionelle Inhalte sind nicht immer deutlich von Werbung getrennt
- Sie sind **überfordert**, denn die Struktur des Internets ist komplex
- Sie gehen **spielerisch** mit dem Internet um, denn das WWW ist für sie ein einziger Spielplatz
- Sie sind **orientierungslos**, denn eine Suche im Internet überfordert vielfach
- Sie werden stark **gefordert**, denn das Surfen erfordert hohe Lese- und Schreibkompetenz

Das **Learning by Doing** im Internet hat seine Grenzen und Kinder sind nicht **die** Experten im Internet, auch wenn es angesichts ihrer „technologisch-instrumentellen Fertigkeiten“[9], als einen Teil der Definition von Medienkompetenz, in der Bedienung von Handys und Computern manchmal so erscheinen mag. Sie eignen sich fast mühelos und atemberaubend schnell neue Software oder unbekannte Geräte an. Es verwundert daher nicht, dass dies oft mit wahrer Medienkompetenz (zu der auch Aspekte wie Reflexionsvermögen, Wissen und Kritikfähigkeit gehören) verwechselt wird.

Worin liegen Gefährdungen?

Nach Nigel Williams liegen die Gefahren in verschiedenen Bereichen: ungeeignete und gefährdende Inhalte (Pornografie, Gewalt, Geschmacklosigkeiten, Rassismus), gefährdende Kontakte, sowie Kommerz (Werbung und Marketing, Datenschutz, Kosten)[10]. Ergänzen könnte man den Bereich der unangemessenen Kommunikation, wie z. B. Cyber-Mobbing.

Content
Contact
Commerce
Conflict

Quelle: Angelehnt an Williams (2000)[11]

Ein ähnliches Schema entwickelte die englische Psychologin Sonia Livingstone in der Studie **EU Kids Online** im Jahre 2009. Sie stellte die verschiedenen Rollen des Kindes als Rezipient (Content), als Teilnehmer (Contact) und als Akteur (Conduct) in ein Raster von Chancen und Risiken[12]:

Kategorisierung von Chancen und Risiken der Internetnutzung

		Content Kind als Rezipient	**Contact** Kind als Teilnehmer	**Conduct** Kind als Akteur
Chancen	Bildung, Lernen und digitale Kompetenz	Bildungsressourcen	Kontakt mit Gleichgesinnten	Eigeninitiative oder gemeinsames Lernen
	Teilnahme und soziales Engagement	Allgemeine Informationen	Austausch in Interessengruppen	Konkrete Formen sozialen Engagements
	Kreativität und Selbstdarstellung	Ressourcenvielfalt	Eingeladen/inspiriert werden, kreativ zu sein oder mitzumachen	Erstellung von benutzergenerierten Inhalten
	Identität und soziale Beziehungen	Beratung (Persönliches/Gesundheit/Sexualleben usw.)	Soziale Netzwerke, Erfahrungen mit anderen teilen	Ausdruck eigener Identität
Risiken	Kommerzielle Interessen	Werbung, Spam, Sponsoring	Verfolgung/Sammlung von persönlichen Informationen	Glücksspiel, illegale Downloads, Hacken
	Aggression/Gewalt	Gewaltverherrlichende/grausame/volksverhetzende Inhalte	Mobbing, Belästigung oder Stalking	Andere mobben oder belästigen
	Sexualität	Pornographische/schädliche Inhalte	Treffen mit Fremden, missbräuchliche Annäherungsversuche	Erstellen/Hochladen von pornographischem Material
	Werte	Rassistische/verzerrte Informationen/Ratschläge (z. B. Drogen)	Selbstverletzung, ungewolltes Zureden/Überredung	Ratschläge z. B. zu Selbstmord/Magersucht geben

Quelle: Landesanstalt für Medien Nordrhein-Westfalen (LfM) (2011)[13], nach Livingstone & Haddon, 2009

Aus der Praxis

Im Alter von zwölf oder dreizehn Jahren fühlen sich viele Kinder schon kompetent genug, um selbständig – also ohne Begleitung oder Regelwerk – mit den Risiken im Internet umgehen zu können. Diese Einschätzung erweist sich – wie viele Fälle zeigen – häufig als Überschätzung und bringt nicht selten Überforderung mit sich. Dass dennoch ein generelles Risiko- bzw. Gefahrenbewusstsein in dieser Altersgruppe existiert, sieht man, wenn man sie dazu auffordert (evtl. fiktiv), für ein jüngeres Geschwisterkind Regeln für die Internet-Nutzung aufzustellen. Hier zeigen sie sich als „strenge Eltern".

Die neuen Herausforderungen im Jugendmedienschutz

Trotz der vielfältigen positiven Möglichkeiten, die das Internet bietet, ist nicht zu vergessen, dass Kinder und Jugendliche besonders schutzbedürftig sind. Deshalb ist es Aufgabe des Jugendschutzes, ihre körperliche, geistige und seelische Entwicklung zu fördern. Es geht jedoch nicht nur darum, junge Menschen zu bewahren – sie sollen ebenso befähigt werden, sich selbst zu schützen und Entscheidungs- und Kritikfähigkeit sowie Eigenverantwortlichkeit zu entwickeln. Diese Ziele für den Jugendmedienschutz umzusetzen, stellt eine besondere Herausforderung dar[14].

Die nachgeordnete Grafik stellt die verschiedenen Verantwortungsbereiche mit den jeweils verantwortlichen Organen, Institutionen und Gruppen dar. Daneben liegt der Fokus auf dem Schutzbedürfnis von Kindern und Jugendlichen. Mit zwei Altersaufteilungen werden jüngere Kinder, bis ca. zwölf Jahre, und ältere Kinder und Jugendliche ab ca. zwölf Jahren in den Blick genommen. Für jüngere Kinder hat Risikovermeidung höchste Priorität, d. h. die Webseiten für diese Altersgruppe müssen in sicheren Surf- und Kommunikationsräumen angeboten werden. Dies beinhaltet die Nutzung von Kindersuchmaschinen zum Suchen und Recherchieren im Netz sowie das Surfen auf altersgerechten Angeboten. Daneben braucht es technische Tools (Jugendschutzprogramme), die zufällige Konfrontation mit problematischen Inhalten verhindern bzw. reduzieren. Parallel sind Erziehungsbeauftragte wie z. B. Kita, Schule und Elternhaus herausgefordert, bei Kindern Medienkompetenz anzubahnen und aufzubauen.

Jedoch verschieben sich bei den über zwölfjährigen Kindern und Jugendlichen die Prioritäten, denn für diese geht es vor allem um Risikoreduzierung. Hier gilt es, über Erziehungsbeauftragte Medienkompetenz und (Selbst-)Risikomanagement weiter auszubauen und zu stärken, sodass vorhandene Schutzmaßnahmen in den Internetangeboten angemessen eingesetzt und genutzt werden. Technik zur Reduzierung von Konfrontationsrisiken spielt in dieser Altersgruppe eine zunehmend geringere Rolle.

Verteilte Verantwortung für zeitgemäßen Jugendschutz

<table>
<tr><td colspan="6">Staat
Rechtliche Regulierung, Anreizsysteme, Evaluation</td></tr>
<tr><td>Inhalteanbieter, Plattformbetreiber, Initiativen</td><td>Anbieter technischer Tools</td><td>Eltern, pädagogische Fachkräfte</td><td>Eltern, pädagogische Fachkräfte</td><td>Inhalteanbieter, Plattformbetreiber</td><td>Anbieter technischer Tools</td></tr>
<tr><td colspan="3">Jüngere Kinder (unter 12 Jahre)
Risikovermeidung</td><td colspan="3">Ältere Kinder und Jugendliche (ab 12 Jahre)
Risikoreduzierung</td></tr>
<tr><td>Sichere Surf-und Kommunikations-räume</td><td>Technik zur Vermeidung von Konfrontation</td><td>Befähigung zur elementaren Medienkompetenz</td><td>Befähigung zum (Selbst-) Risiko-management</td><td>Redaktionelle und technische Unterstützung in Internetangeboten</td><td>Technik zur Reduzierung von Konfrontation</td></tr>
<tr><td colspan="6">Internetnutzerinnen und -nutzer
Peer-Unterstützung, Bewertung/Tagging, Gegenaktivitäten/Beschwerden, Partizipation, Weiterentwicklung der Tools</td></tr>
<tr><td colspan="6">Drei zusammenwirkende Säulen mit unterschiedlicher Wichtigkeit für die jeweilige Altersgruppe: ■ hoch ■ mittel ■ gering</td></tr>
</table>

Eigene Darstellung in Anlehnung an Jugendmedienschutz als Risikomanagement*, I-KIZ 2014*[15]

Quelle: I-KiZ – Zentrum für Kinderschutz im Internet, Berlin, 2014

[1] STATISTA. (2014, September). *Anteil der Internetnutzer in Deutschland von 1997 bis 2014.* Aufgerufen am 03.03.2015 unter http://de.statista.com/statistik/daten/studie/36009/umfrage/anteil-der-internetnutzer-in-deutschland-seit-1997/

[2] STATISTA. (2014, Februar). *Anzahl der Internetnutzer weltweit von 1997 bis 2014 (in Millionen).* Aufgerufen am 26.02.2015 unter http://de.statista.com/statistik/daten/studie/186370/umfrage/anzahl-der-internetnutzer-weltweit-zeitreihe/

[3] MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.) (2015). *JIM-Studie 2015, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland* (S.30). Aufgerufen am 05.01.2016 unter http://www.mpfs.de/fileadmin/JIM-pdf15/JIM_2015.pdf

[4] S. 30, ebd.

[5] S. 31, ebd.

[6] S. 50, ebd.

[7] MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.). (2012). *KIM-Studie 2012, Kinder+Medien, Computer+Internet, Basisuntersuchung zum Medienumgang 6- bis13-Jähriger in Deutschland* (S. 24). Aufgerufen am 14.07.2014 unter http://www.mpfs.de/fileadmin/KIM-pdf12/KIM_2012.pdf

[8] S. 36, ebd.

[9] GROEBEN, N. (2002). Dimensionen der Medienkompetenz: Deskriptive und normative Aspekte. In N. Groeben, N. & B. Hurrelmann (Hrsg.), *Medienkompetenz. Voraussetzungen, Dimensionen, Funktionen.* Weinheim u. München: Juventa. (S. 160–192).

[10] WILLIAMS, N. (2000). *Childnet International submission to the COPA Commission.* (S. 1). Aufgerufen am 28.02.2015 unter http://www.childnet.com/ufiles/copa-commision-report.pdf

[11] Ebd.

[12] LIVINGSTONE, S. & Haddon, L. (2009). *EU Kids Online: Final report.* Aufgerufen am 10.10.2014 unter http://www.lse.ac.uk/media@lse/research/eukidsonline/eu%20kids%20i%20%282006-9%29/eu%20kids%20online%20i%20reports/eukidsonlinefinalreport.pdf

[13] LANDESANSTALT für Medien Nordrhein-Westfalen (LfM) (2011). *Heranwachsen mit dem Social Web.* Bd.: 62. Düsseldorf (S. 277). Aufgerufen am 14.07.2014 unter https://www.lfm-nrw.de/fileadmin/lfm-nrw/Forschung/LfM-Band-62.pdf

[14] I-KIZ ZENTRUM FÜR KINDERSCHUTZ IM INTERNET (2014). Aufgaben und Ziele. Aufgerufen am 28.02.2015 unter https://www.i-kiz.de/fachpublikum

[15] I-KIZ ZENTRUM FÜR KINDERSCHUTZ IM INTERNET (2014). *Jahresbericht* (S. 11). Aufgerufen am 04.03.2015 unter http://www.i-kiz.de/wp-content/uploads/2015/01/I-KiZ_Jahresbericht_Download.pdf

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Wo ist Klaus?**	**Vor- und Nachteile der Internet-Nutzung für Kinder**
Kompetenzen	Die Schülerinnen und Schüler listen die Handlung des Klicksafe-Spots auf, erkennen die Zusammenhänge zur Internet-Sicherheit und gestalten eine Lernhilfe in Form eines Plakats.	Die Schülerinnen und Schüler veranschaulichen die Ergebnisse der KIM-Studie in Form einer Zeitungsmeldung und beurteilen sie gemeinsam. Sie benutzen die Klassifizierung von Livingstone und leiten daraus eigene Beispiele ab, mit denen sie ein Plakat für jüngere Schülerinnen/Schüler kreieren.
Methoden	Tabelle, Plakat	Statistik-Analyse, Tabelle, Plakat
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	nein

Hinweise für die Durchführung

AB 1: Wo ist Klaus?

Grundlage des Arbeitsblattes ist der Werbe-Spot „Wo ist Klaus?“ der EU-Initiative klicksafe. Er ist kostenlos im Internet zu sehen auf der Internetseite **www.klicksafe.de**
Daran sollen die Schülerinnen und Schüler sich die dargestellten Probleme (gewalthaltige Seiten, pornografische Inhalte, gewalthaltige Spiele und pädophile Kontakte) erarbeiten.
Als Produkt soll ein Plakat mit Tipps zur sichereren Nutzung entstehen.

AB 2: Vor- und Nachteile der Internet-Nutzung für Kinder

Die Schülerinnen und Schüler erkennen durch die Auswertung der KIM-Studie Probleme, die im Internet auftauchen können und beschäftigen sich intensiv mit diesen, indem sie Regeln für sicheres Chatten formulieren.
Wie oben, ergänzt durch eine Statistik der KIM-Studie die die Schülerinnen und Schüler in Textform zusammenfassen sollen. Die Vorgabe der Kategorien von Sonia Livingstone ist sicherlich anspruchsvoll und sie bedürfen der Erläuterung und vielleicht auch der konkreten Beispiele, wobei die Unterscheidung nach „Empfänger/Rezipient“, „Teilnehmer“ und „Handelnde/Akteur“ sicherlich anschaulich ist, aber auch manchmal schwierig zu unterscheiden.

		Content Kind als Rezipient	**Contact** Kind als Teilnehmer	**Conduct** Kind als Akteur
Chancen	Bildung, Lernen und digitale Kompetenz	Bildungsressourcen	Kontakt mit Gleichgesinnten	Eigeninitiative oder gemeinsames Lernen
	Teilnahme und soziales Engagement	Allgemeine Informationen	Austausch in Interessengruppen	Konkrete Formen sozialen Engagements
	Kreativität und Selbstdarstellung	Ressourcenvielfalt	Eingeladen/inspiriert werden, kreativ zu sein oder mitzumachen	Erstellung von benutzergenerierten Inhalten
	Identität und soziale Beziehungen	Beratung (Persönliches/Gesundheit/Sexualleben usw.)	Soziale Netzwerke, Erfahrungen mit anderen teilen	Ausdruck eigener Identität
Risiken	Kommerzielle Interessen	Werbung, Spam, Sponsoring	Verfolgung/Sammlung von persönlichen Informationen	Glücksspiel, illegale Downloads, Hacken
	Aggression/Gewalt	Gewaltverherrlichende/grausame/volksverhetzende Inhalte	Mobbing, Belästigung oder Stalking	Andere mobben oder belästigen
	Sexualität	Pornographische/schädliche Inhalte	Treffen mit Fremden, missbräuchliche Annäherungsversuche	Erstellen/Hochladen von pornographischem Material
	Werte	Rassistische/verzerrte Informationen/Ratschläge (z. B. Drogen)	Selbstverletzung, ungewolltes Zureden/Überredung	Ratschläge z. B. zu Selbstmord/Magersucht geben

Lust auf mehr? Die KIM-Studie wird alle zwei Jahre erhoben und unter **www.mpfs.de** veröffentlicht. Dort finden sich zahlreiche andere statistische Daten zur Mediennutzung von Kindern.

Wo ist Klaus?

Es klingelt … und die komischsten Typen stehen vor der Türe und fragen nach Klaus. Was macht die Mutter? Sie öffnet bereitwillig die Türe und lässt alle hinein.

Wie im wahren Leben?
Nein, sicherlich nicht. Aber im Internet? Der Video-Spot der EU-Initiative klicksafe.de macht es in Form eines Werbe-Clips deutlich: Es gibt Gefahren im Internet und Kinder sollten davor geschützt werden.

Schaue dir den Werbe-Spot auf der Webseite der EU-Initiative klicksafe.de an: **www.klicksafe.de**

1. Arbeitsauftrag:
Fülle folgende Tabelle aus:

Szene	Wer kommt?	Welches Problem wird dargestellt?	Wie könnte das Problem im Internet auftreten?
Szene 1			
Szene 2			
Szene 3			
Szene 4			

Bildet mehrere Gruppen (4 – 5 Schüler pro Gruppe).

2. Arbeitsauftrag:
Sammelt Tipps, wie das Surfen im Internet für Kinder sicherer sein kann.
Formuliert (oder zeichnet) diese gemeinsam auf einem Plakat.

Ruft folgende Internetseite auf:
www.klicksafe.de/fuer-kinder/internet-abc/sicher-surfen/wissen-wies-geht
Dort findet ihr Tipps zum sicheren Surfen im Internet!

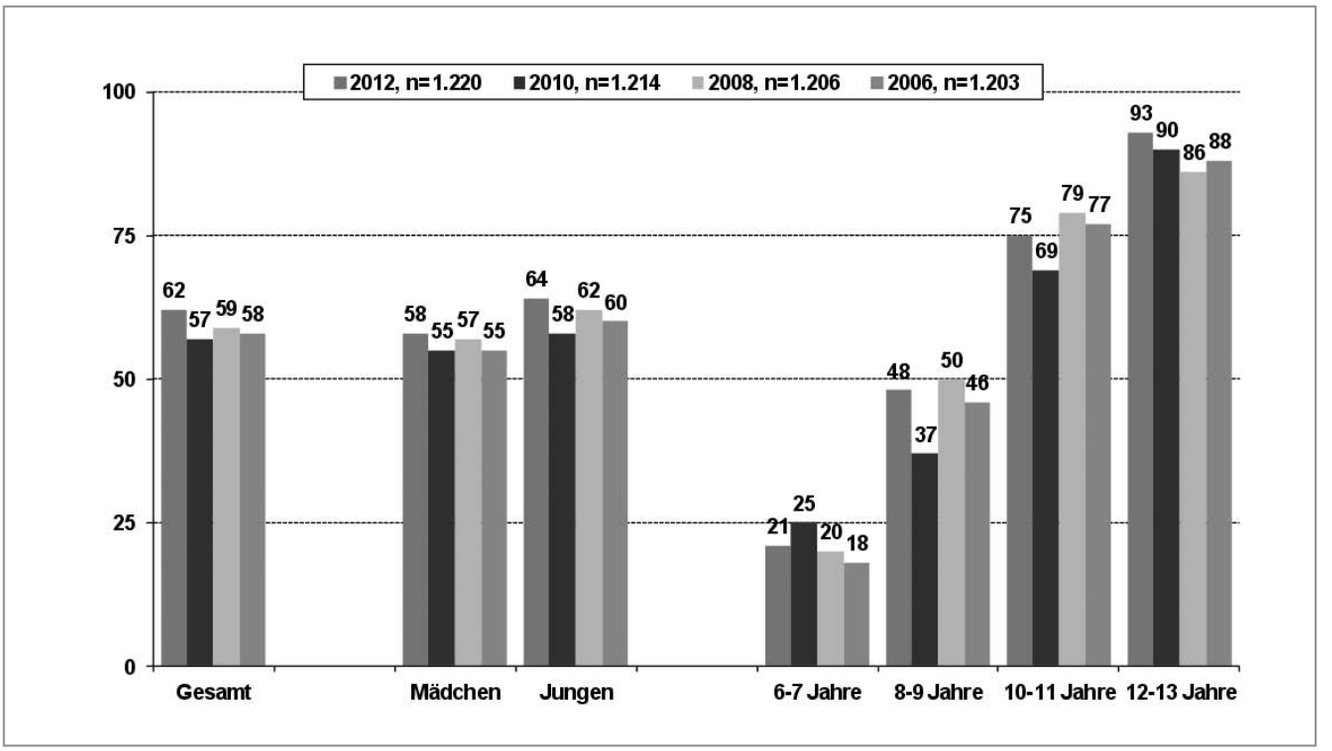
3. Arbeitsauftrag:
Vergleicht eure Tipps mit denen von klicksafe.de und ergänzt sie evtl. auf eurem Plakat.

Vor- und Nachteile der Internet-Nutzung für Kinder (1/2)

Das Internet ist aus eurem Alltag nicht mehr wegzudenken und auch viele jüngere Kinder nutzen das Internet bereits, häufig über Smartphones und mit einem ständigen Online-Zugang.

Wie sich diese Entwicklung in den letzten Jahren vollzog, zeigt die Grafik aus der Studie „Kinder + Medien, Computer + Internet“, kurz „KIM-Studie“, die alle zwei Jahre repräsentativ in Deutschland erhoben wird:

Entwicklung Internet-Nutzer 2006 – 2012
– Nutzung zumindest selten –



Quelle: MPFS, 2012, S.33 ; Angaben in %, Basis: alle Kinder

Vor- und Nachteile der Internet-Nutzung für Kinder (2/2)

Neben den zahlreichen Vorteilen, die sich für Kinder bei der Nutzung des Internets ergeben, gibt es leider auch viele Nachteile. Die englische Psychologin Sonia Livingstone entwickelte in der Studie „EU Kids Online" folgendes Raster von Chancen und Risiken:

	Bereich	Kind als Rezipient	Kind als Teilnehmer	Kind als Akteur
Chancen	Lernen			
	Soziales Engagement			
	Kreativität			
	Soziale Beziehungen			
Risiken	Kommerzielle Interessen			
	Aggression/ Gewalt			
	Sexualität			
	Werte			

Arbeitsaufträge:

1. Bitte wertet das Diagramm der KIM-Studie aus. Fasst das Ergebnis in Form einer kurzen Zeitungsmeldung (Überschrift und kurzer Text) zusammen.

2. Hättet ihr diese Zahlen erwartet? Bitte diskutiert – zunächst in kleinen Gruppen, danach mit der ganzen Klasse – was diese Entwicklung bedeutet. Welche Veränderungen ergeben sich daraus?!

3. Bitte setzt euch zu zweit zusammen und füllt das Raster von Sonia Livingstone mit Beispielen. Klärt zuvor in der Klasse, was unter Rezipient, Teilnehmer und Akteur zu verstehen ist. Findet euch danach in 6er-Gruppen zusammen und stellte eure Ergebnisse gegenseitig vor und ergänzt das eigene Raster. Fasst danach die Ergebnisse der Klasse an der Tafel zusammen.

4. Setzt euch danach wieder in die 6er-Gruppe und erstellt ein Plakat mit dem Titel „Sicheres Surfen im Internet", das man in einer Grundschulklasse aufhängen könnte.

2

Wie wir finden, was wir suchen: Suchmaschinen und Online-Lexika

2|1 Informationen aus dem Netz

2|2 Suchmaschinen

2|3 Wikipedia

2

Informationen aus dem Netz

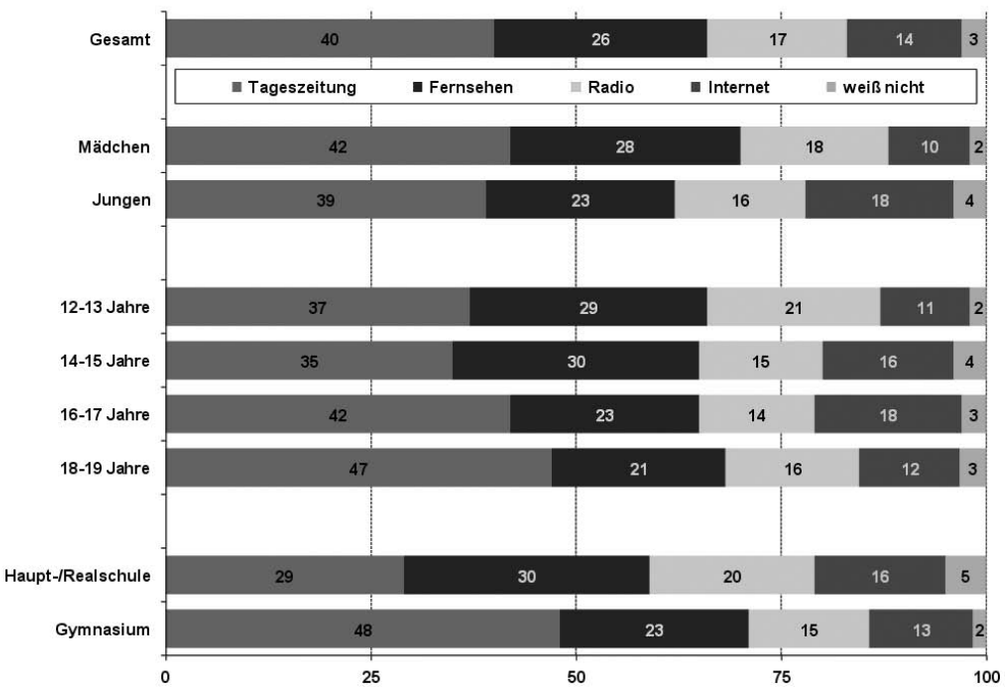
Fülle an Informationen

Das Internet ist nicht nur ein Kommunikationsmedium, sondern bietet auch eine schier unüberschaubare Fülle an Informationen. Jeder kann sich in diesem interaktiven Medium an der Erstellung und Veröffentlichung der Informationen beteiligen, die Kontrolle über ein Lektorat und einen Verlag – wie im Falle eines Buches – entfällt. Die Kosten und damit das finanzielle Risiko einer Veröffentlichung sind minimal. Deshalb stellt sich das Internet auf der Suche nach Informationen als eine kostengünstige und schnelle Quelle zur Recherche dar. Zeitschriften, Online-Lexika, private Internetseiten, Videoportale, Wörterbücher, Blogs, Online-Fach-Datenbanken von beispielsweise Museen, Organisationen, Institutionen, Behörden, Universitäten, aber auch wissenschaftliche Abhandlungen, Foren und Online-Meinungsumfragen, in- und ausländische Online-Zeitungen, Fernsehsender und Radiosender sind nur einige Angebote, die dabei genutzt werden können. Hinzu kommen weltweite Projekte wie etwa **Google Books:** Der Konzern digitalisiert millionenfach Bücher, stellt diese ins Internet und macht sie mittels Volltextsuche allgemein verfügbar.

Glaubwürdigkeit von Internetquellen

Stellt man Jugendlichen die Frage, welchem Medium sie bei widersprüchlicher Berichterstattung am ehesten glauben würden (Fernsehen, Radio, Internet und Tageszeitung stehen zur Auswahl), so entscheiden sich mit 40 % die meisten der befragten Zwölf- bis Neunzehnjährigen für die Tageszeitung. Ein knappes Viertel würde am ehesten dem Fernsehen Glauben schenken, 17 % dem Radio und 14 % dem Internet.[1]

Würde bei widersprüchlicher Berichterstattung am ehesten vertrauen auf …



Quelle: MPFS (2014); Angaben in %, Basis: alle Befragten, n=1.200[2]

Splittet man die Ergebnisse derselben Frage nach dem Bildungshintergrund der Jugendlichen auf, so ergeben sich für das Vertrauen in die Informationen aus dem Internet bei Haupt- und Realschülern 16 % und bei Gymnasiasten 13 %[3].

Kriterien

Eine wirklich fundierte Quellenanalyse ist ohne Hintergrund und Vorwissen nahezu unmöglich und somit stellt sich immer die Frage nach der Quellenkritik, auch in Büchern. Wie viel schwieriger ist da eine fundierte Quellenkritik (nicht nur) für Kinder und Jugendliche im Internet.

Für die schulische Arbeit mit Internetquellen könnte man folgende Leitfragen formulieren, die vor der Wahl einer Quelle von den SchülerInnen beantwortet werden sollten:

1. Wird meine Frage genau und vollständig und verständlich beantwortet?
2. Wer hat es geschrieben?
3. Welchen Hintergrund hat die Information?
4. Wie und warum wurde der Text geschrieben/ die Information veröffentlicht?
5. Wie aktuell ist die Webseite?
6. Welchen Rang nimmt die Quelle in Suchmaschinen ein?

Es ließen sich noch weitere Kriterien formulieren, aber aus Gründen der Überschaubarkeit, insbesondere für jüngere SchülerInnen, reicht o. a. Liste sicherlich aus.

Aus der Praxis

*Bei SchülerInnen ist diese penible Arbeit bei der Internetrecherche ausgesprochen unbeliebt. Man kann sie extrinsisch mit „schönen" Recherche-Aufgaben, die einen Aha-Effekt bieten, motivieren: Wer weiß zum Beispiel schon was **Easter-Eggs** mit Computerspielen und dem russischen Zaren gemein haben?*

In der Schule

Die Notwendigkeit der Quellenkritik ist an sich nicht neu. In Zeiten des Internets aber ist sie noch wichtiger geworden. Schon immer gab es die Maßgabe, Schülerinnen und Schüler in ihrer Quellenkritikfähigkeit zu schulen und darin zu bestärken nachzufragen, wer mit welchem Interesse warum welchen Text in welchem Kontext schreibt. Die Grundlage dazu liefert die LASSWELL-Formel der Kommunikation[4]:

- **Wer** sagt
- **was** zu
- **wem**
- auf welchem **Kanal**
- mit welchem **Effekt**

Quelle: Lasswell, 1948 entnommen aus McQuail/Windahl (1981)[5]

Diese Formel wird häufig noch um folgende Fragen ergänzt:

- **Warum?**
- **Wie?**

Was kann man als Lehrkraft im Zeitalter des Internets tun? Hier einige Tipps:

- *Schüler für das Thema „Quellenkritik" sensibilisieren*
- *Im Zuge der kritischen Medienbetrachtung das Medium „Internet" immer einbinden*
- *Schülern Kriterien (Identität, Referenz, Objektivität und Qualität) an die Hand geben und diese altersgerecht benennen*
- *Schüler mit offensichtlich falschen Inhalten bzw. Propaganda im Netz konfrontieren, dann reflektieren und diskutieren*
- *Unterrichtseinheiten zum Thema Glaubwürdigkeit von Quellen durchführen*

Links und weiterführende Informationen

Weiterführende Literatur

LfM-Broschüre *„Der Info-Kompass. Orientierung für den kompetenten Umgang mit Informationen"* http://lfmpublikationen.lfm-nrw.de/

LfM-Broschüre *„Informationskompetenz im Alltag – Informationen finden, bewerten, weitergeben"* http://lfmpublikationen.lfm-nrw.de/

Endnoten

[1] MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.). (2014). *JIM-Studie 2014, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland (S. 15). Aufgerufen am 03.03.2015 unter http://www.mpfs.de/fileadmin/JIM-pdf14/JIM-Studie_2014.pdf*

[2] Ebd.

[3] Ebd.

[4] MCQUAIL, D. & Windahl, S. (1981). *Communication Models for the Study of Mass Communications.* London, New York: Longman. (S. 10)

[5] Ebd.

Methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Internet, alles wahr?**	**Internet = Wahrheit?**
Kompetenzen	Die Schülerinnen und Schüler vergleichen Informationen und beurteilen sie. Sie handhaben vier Tipps zur Internetrecherche an einem eigenen Beispiel.	Die Schülerinnen und Schüler legen die Vor- und Nachteile des Internets als Informationsquelle dar und führen eine Internetrecherche anhand einer Vorlage aus.
Methoden	Quellenanalyse, Internetrecherche	Quellenanalyse, Internetrecherche
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Internet, alles wahr?	Die Schülerinnen und Schüler sollen an einem (erfundenen) Beispiel vier Tipps kennen lernen und üben, wie sie Informationen aus dem Internet überprüfen können. Sie sollen den Urheber der Seite herausfinden, wobei sie mit der Einschätzung der Seriosität sicherlich überfordert sind. Hier könnten Sie Hilfestellungen leisten. Sie sollen die Informationen kontrollieren, zum Beispiel mit einem Buch oder einer weiteren Internetseite. Und sie sollen die Informationen auch mit ihrem klaren Verstand oder einem Bauchgefühl überprüfen. Manchmal kommt einem etwas schon „komisch" vor, ohne genau zu wissen, warum. Oder man weiß selbst schon etwas über ein Thema und die Informationen aus dem Internet passen nicht dazu. Zum Schluss schließlich ist das Datum nicht unerheblich, wobei davon ausgegangen werden kann, dass aktuellere Informationen auch besser sind (was nicht zwingend und immer der Fall sein muss!). Die Schülerinnen und Schüler sollen nun zu einem Thema bei der Kindersuchmaschine Blinde Kuh zwei Seiten heraussuchen und die Tipps anwenden. Vielleicht finden sie ja im Gespräch noch weitere wichtige Tipps.
AB 2: Internet = Wahrheit?	Mit diesem Arbeitsblatt sollen die Schülerinnen und Schüler eine elaborierte Methode zur (Internet-) Quellenanalyse kennenlernen und anwenden. Dabei ist die Vorgabe relativ streng und sicherlich im Alltag nicht immer anwendbar. Trotzdem sollten die Schülerinnen und Schüler im Sinne von „Best Practice" diese einmal vollständig und genau durchgeführt haben. Je nach Quelle sind nicht alle Fragen zu beantworten, diese Spalten können/müssen selbstverständlich leer bleiben. Vielleicht hilft bei Schritt 6 (Analyse) die Eselsbrücke AEIOU: (**A**ktualität, R**e**ferenz, **I**dentität, **O**bjektivität) … und das **U** für „unbedingt!".

Lust auf mehr?
Das Thema Quellenanalyse lässt sich mit vielen Beispielen durchführen. Sehr anschaulich sind auch die veröffentlichten Fehler von bspw. Journalisten, die keine sorgfältige Quellanalyse betrieben. Gut dokumentiert ist das Beispiel von Karl-Theodor zu Guttenberg und seinen falschen Vornamen, das man recherchieren kann.

Internet, alles wahr?

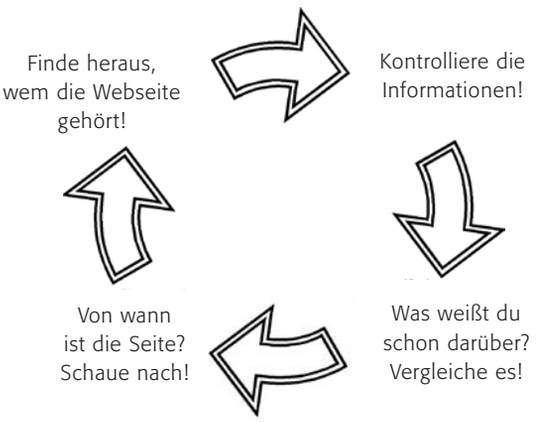
Informationen im Internet: *Das Internet ist eine tolle Sache. Wenn du ein Tierfreund bist, kannst du hier wie in einem Buch-Lexikon viel über deine Lieblingstiere lernen. In einem Buch steht immer, wer es geschrieben hat, aber im Internet? Das ist das Blöde an Informationen aus dem Internet: du kannst nie sicher sein, wer sie geschrieben hat und ob sie auch wirklich stimmen. Jeder kann Sachen ins Internet schreiben und wie im wirklichen Leben werden Fehler gemacht oder sogar Lügen verbreitet. Und wie schwer es ist, eine Lüge zu erkennen, das weißt du sicherlich!*

Wir machen eine kleine Übung: Stelle dir vor, du hast diese Seiten gefunden. (Die Beispiele sind frei erfunden!)

Die Mega-Wal-Seite	**Walforum weltweit**	**Walschützer online**
Hier findest du alles über Wale. Wale sind Säuger und es gibt über 180 verschiedene. Der Blauwal ist der größte Wal und wird 50 Meter lang und meistens über 300 Tonnen schwer.	Wale gehören zur Ordnung der Säugetiere und es gibt knapp 80 Arten weltweit. Der Blauwal ist das größte Tier, das jemals auf der Erde lebte. Er kann 33,5 m lang und bis zu 200 Tonnen schwer werden.	Wale, diese wunderbaren Verwandten des Menschen! 79 Arten tummeln sich in den Weltmeeren. Blauwale, die sanften Giganten, wurden nur von den Dinosauriern an Größe übertroffen und werden sehr lang (knapp 35 m) und sehr schwer (200 Tonnen).

1. Arbeitsauftrag:
Findest du die Fehler? Vergleiche die Informationen über Wale zusätzlich mit einem Buch-Lexikon!

2. Arbeitsauftrag:
Was kannst du beim nächsten Mal tun? Im Kästchen unten sind einige Tipps:



TIPP: *Finde heraus, wem die Webseite gehört (Schaue mal ins so genannte „Impressum"). Haben diese Leute einen guten Ruf? Wenn du nicht sicher bist, frage deine Lehrerin oder deinen Lehrer. Vergleiche das, was du im Internet findest mit Informationen aus Büchern oder Zeitschriften. Vergleiche dies weiterhin mit dem, was du selber schon zu diesem Thema weißt. Schau auf das Datum der Webseite. Wenn es lange her ist, dass die Webseite aktualisiert wurde, dann ist die Information wahrscheinlich schon veraltet.*

3. Arbeitsauftrag:
Dies kannst du nun an einem Beispiel üben. Wähle ein Thema aus (zum Beispiel Wale) und rufe über die Suchmaschine Blinde Kuh zwei unterschiedliche Seiten dazu auf. Vergleiche sie mithilfe der Tipps. **www.blinde-kuh.de**

4. Arbeitsauftrag:
Schreibe die Tipps ab und male ein Bild dazu! Vielleicht hängst du es neben deinen Bildschirm, damit du beim nächsten Mal daran denkst!

Internet = Wahrheit? (1/2)

Zeitschriften, Online-Lexika, private Internetseiten, Videoportale, Foren, in- und ausländische Online-Zeitungen, Fernsehsender und Radiosender. Das Internet ist nicht nur ein Kommunikationsmedium, sondern bietet auch eine schier unüberschaubare Fülle an Informationen. Bedingt durch die Interaktivität des Mediums kann sich jeder Einzelne selbst an der Erstellung und Veröffentlichung der Informationen beteiligen, die Kontrolle mittels eines Lektorats – wie im Falle eines Buches – entfällt.

Quelle: Das fehlende Puzzle-Teil/Tim Reckmann/pixelio.de

Wie aber kann ich in dieser unüberschaubaren Fülle eine seriöse Quelle erkennen? Wie kann ich sicher sein, dass die Informationen wahr sind? Wie erkenne ich Unwahrheiten – absichtliche und unabsichtliche?

Folgende Leitfragen können helfen:

- Wird meine Frage genau, vollständig und verständlich beantwortet?
- Wer hat es geschrieben?
- Welchen Hintergrund hat die Information?
- Wie und warum wurde der Text geschrieben/ die Information veröffentlicht?
- Wie aktuell ist die Webseite?
- Welchen Rang nimmt die Quelle in der Suchmaschinen-Trefferliste ein?

Arbeitsaufträge:

1. Bitte beschreibt die Vor- und Nachteile des Internets als Quelle für Informationen. Fasst die Ergebnisse in einer Pro- und Contra-Tabelle zusammen.

2. Ist es euch schon einmal passiert, eine falsche Information gefunden zu haben? Berichtet in der Klasse von solchen Fällen. Wie seid ihr dem Fehler/der Unwahrheit auf die Schliche gekommen?

3. Stellt euch einen aktuellen Fall vor, bei dem eine Gruppe von Menschen bewusst eine Unwahrheit im Internet verbreitet hat. Warum machen Menschen das? Diskutiert die Motive dafür.

Führt danach die folgende Übung vollständig – Schritt für Schritt – durch!

Internet = Wahrheit? (2/2)

Übung zur Überprüfung von Internet-Quellen

In 8 Schritten zum Such-Profi!

	Stichwort	Arbeitsauftrag	Ergebnis/Notizen
1	Frage	Formuliere das, was du wissen möchtest, möglichst genau und schriftlich in Form einer Frage!	
2	Quelle	Überlege zunächst (ohne Internet), wo du die Antwort finden könntest. Schreibe die möglichen Quellen auf!	
3	Schlag-worte	Überlege zunächst (ohne Internet), mit welchen Schlagworten = Suchbegriffen du die Antwort finden könntest. Schreibe sie auf!	
4	Internet-Suche	Gib nun die möglichen Quellen und die Schlagworte in eine Suchmaschine ein. Schreibe auf, wie viele Treffer du erhältst. Grenze eventuell deine Suche noch stärker ein.	
5	Auswahl	Wähle nun aus den Treffern mindestens drei (oder auch mehr!) Quellen aus. Begründe kurz, aber schriftlich, warum du diese Quellen ausgewählt hast!	1. 2. 3.
6	Analyse	**Suche in den drei Quellen die Antwort auf deine Frage. Vergleiche sie miteinander! Wenn es Unterschiede gibt, versuche herauszufinden, warum! Nimm eine Bewertung der Quellen mit folgenden Fragen vor. Notiere bitte schriftlich:**	
		Aktualität: Wie aktuell ist die Seite? Welchen Rang nimmt die Seite bei den Treffern ein?	1. 2. 3.
		Referenz: Was weißt du über den Autor des Textes/den Verfasser der Seite? (Evtl. woanders zu dem Namen suchen!)	1. 2. 3.
		Identität: Was steht im Impressum der Seite? Kann man daraus etwas erkennen?	1. 2. 3.
		Objektivität: Wie ist der Text geschrieben? Warum wurde er geschrieben? Kann man eine Meinung/Absicht erkennen?	1. 2. 3.
		Unbedingt	Misstrauisch sein und immer kontrollieren!
7	Reorgani-sation	Schreibe die Antwort auf deine Frage in eigenen Worten oder als Zitat auf (kein Copy+Paste!). Notiere die genaue Quelle und das Datum dahinter!	
8	Präsen-tation	Präsentiere dein Ergebnis in einer ansprechenden Form und mit eigenen Worten.	

Suchmaschinen

Suchmaschinen sind ohne Zweifel eine der wichtigsten Anwendungen im Internet. Sie stellen den Mittler dar zwischen uns und der Fülle an Informationen im Internet. Doch – auch wenn es angesichts der oft Millionen Ergebnisse in Bruchteilen von Sekunden nicht so scheint – die Möglichkeiten der Suchmaschinen sind begrenzt! Alle Suchmaschinen suchen bei einer Anfrage nicht das gesamte Internet ab, sondern nur den eigenen Index der gespeicherten Seiten – ähnlich einer Bibliothekarin, die nur bestimmte Bücher aus dem Bestand herausgibt. Dabei nimmt seit Jahren **Google** als Marktführer mit weltweit knapp 70 % aller Suchanfragen eine nahezu unanfechtbare Vormachtstellung ein[1]. In Deutschland erreicht die Google-Suchmaschine einen Marktanteil von 95 %. Anders ausgedrückt: Nur ca. 5 % der deutschen Internetnutzer suchen mit **Bing** von **Microsoft, Yahoo!** oder anderen Suchmaschinen[2]. Nach eigenen Angaben hatte **Google** im Jahr 2012 weltweit 1200 Milliarden Suchanfragen in 146 Sprachen[3].

Suchmaschinen-Arten im Überblick

Indexbasierte Suchmaschinen
Die indexbasierte Suchmaschine liest mit Hilfe von einer Software namens **Crawler** automatisch eine Vielzahl von Internet-Quellen ein, analysiert sie algorithmisch (also mithilfe eines Computerprogramms) und legt dann einen Suchindex an, der bei späteren Suchanfragen kontaktiert wird.
Die bekanntesten Beispiele für indexbasierte Suchmaschinen sind **Google, Bing** oder **Ask**. Der Vorteil ist die Schnelligkeit, mit der die jeweiligen Suchergebnislisten angezeigt werden, sowie der Umfang des Indexes.

Alternativen?
*Die Auswahl an alternativen Suchmaschinen schrumpft von Jahr zu Jahr. Denn wer mit **Yahoo!** sucht, benutzt in Wahrheit **Bing** und hinter **T-Online, AOL, Web.de** oder **GMX** verbirgt sich **Google**[4].*

Katalogbasierte Suchmaschinen
Ein Katalog enthält Suchergebnisse, die von Menschen vorher zusammengetragen, geordnet und ggf. auch manuell gewichtet wurden. Im Normalfall steckt hinter einem Katalog eine alphabetische oder nach thematischen Kriterien geordnete Liste. Beispiele sind **Open Directorys** (wie dmoz.org oder dmoz.de) und Kindersuchseiten (wie **www.fragfinn.de** oder **www.blindekuh.de**). Der Vorteil dieses manuellen zusammengestellten Angebots ist, ein Mensch und keine Software für den späteren Nutzer bereits eine Vorauswahl getroffen hat. Bei Katalogen, die speziell für Kinder erstellt wurden, kann man daher sicher sein, keine entwicklungsbeeinträchtigenden Inhalte unter den Ergebnissen zu finden.

Metasuchmaschinen
Eine Metasuchmaschine erstellt keinen eigenen Suchindex, sondern greift auf die Datenbestände (mehrerer) indexbasierter Suchmaschinen zurück. Die einzelnen Suchergebnisse der durchsuchten Index-Suchmaschinen werden durch die Metasuchmaschine gewichtet und in einer neuen Ergebnisliste zusammengefügt. Beispiele sind **www.metager.de** und **www.ixquick.de**. Der Vorteil einer Metasuchmaschine liegt in dem potenziell größeren Datenbestand, der aus der Verknüpfung der Einzelbestände resultiert.

Diskrete Suchmaschine

- *Die Suchmaschine ixquick wirbt damit die „diskreteste Suchmaschine der Welt" zu sein und bietet ausdrücklich einen besseren Schutz der Privatsphäre: Das niederländische Unternehmen bietet mit **www.startpage.com** eine Google-Suche an, die keine IP-Adresse speichert, keine Tracking-Cookies verwendet, die Suchanfragen verschlüsselt etc. – Google mit Datenschutz sozusagen.*
- *Auch die indexbasierte Suchmaschine **DuckDuckGo** wirbt mit ihrer Diskretion und verzichtet darauf, IP-Adresse, Nutzer-Client und Cookies zu speichern.*

Weitere Typen

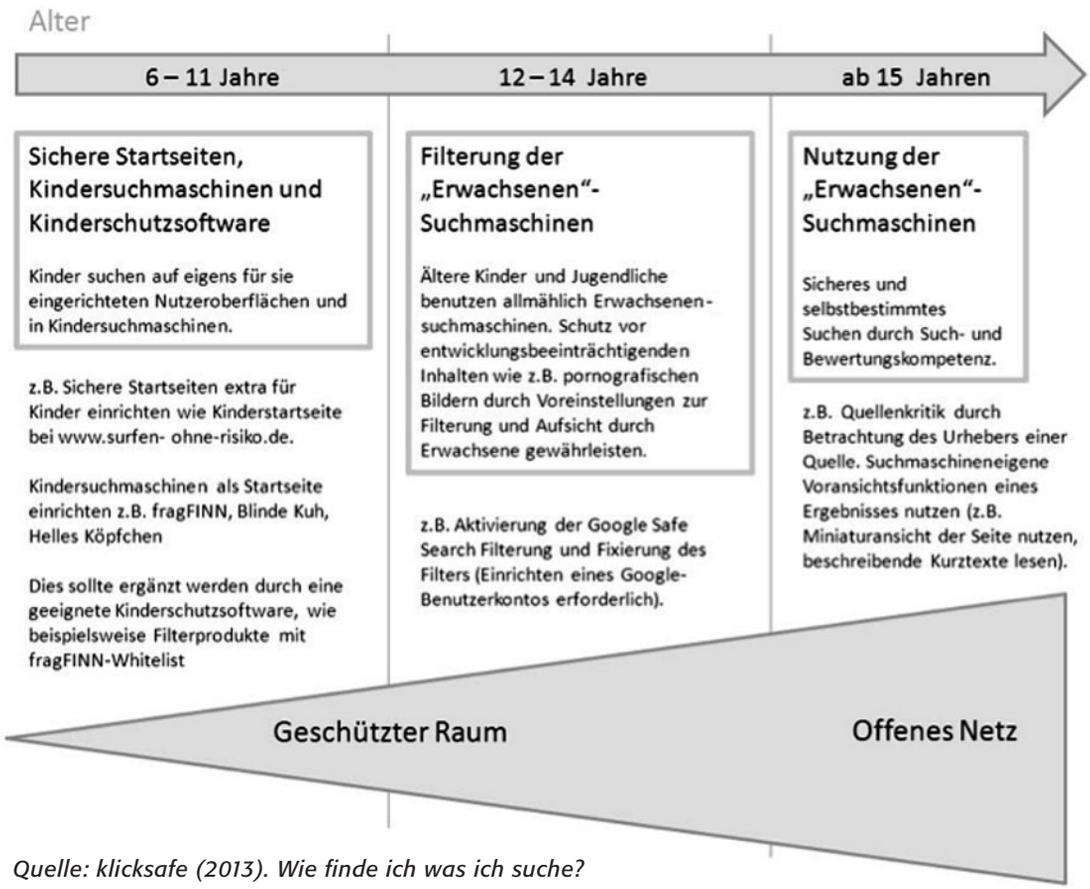
Neben den Websuchmaschinen, die prinzipiell das gesamte öffentlich zugängliche World Wide Web durchsuchen, gibt es eine Vielzahl weiterer Suchmaschinen für spezielle Zwecke, wie Themen- oder Intranet-Suchmaschinen. Andere Suchmaschinen durchsuchen nur eine einzige Domain. So findet z. B. die YouTube-Suchmaschine nur Videos auf der Video-Plattform YouTube. Außerdem gibt es Suchmaschinen, die nur CC-Inhalte finden, also Inhalte, die unter einer Creative-Commons-Lizenz stehen und somit weitestgehend frei verwendbar sind (eng.letscc.net oder search.creativecommons.org).

Folgende Tabelle kann eine Orientierung für einen altersgerechten Umgang mit Suchmaschinen geben:

Suchmaschinen und Jugendmedienschutz

Problematische Inhalte

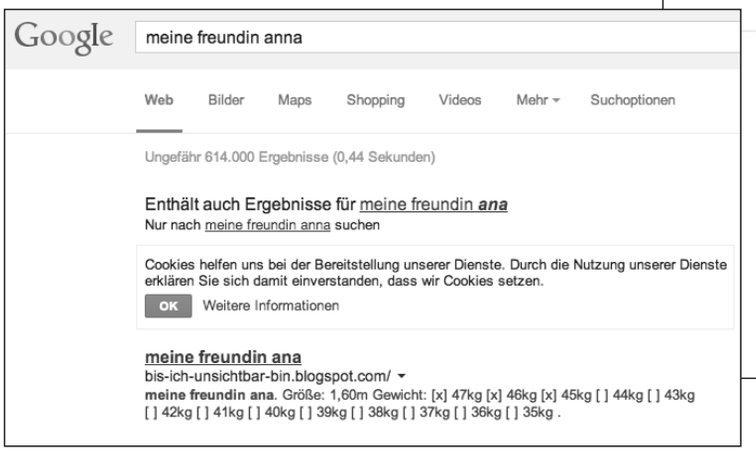
Gerade jüngere Kinder müssen wirksam vor problematischen Inhalten geschützt werden und sollten deshalb (ausschließlich) Kinder-Suchmaschinen wie **www.blinde-kuh.de, www.fragfinn.de** und **www.helles-koepfchen.de** nutzen. Ältere Kinder ab zehn Jahren sollten für die Problematik sensibilisiert werden. Außerdem sollten sie über das reden können, was sie belastet (z. B. wenn sie sich mal „verirrt" haben). Und die Großen schließlich (Klasse 8 und 9) wollen vielleicht Grenzen austesten und sind neugierig auf nicht ganz unproblematische Inhalte. In der Schule helfen im Umgang mit Suchmaschinen das rechte Augenmaß und verbindliche, schriftlich fixierte Regeln für die Nutzung im Unterricht weiter. An vielen Schulen gibt es Vereinbarungen über die Zusammenarbeit mit dem Elternhaus, angelehnt an „Ausbildungsverträge". Auch hier ist ein Kapitel über die Nutzung digitaler Medien sinnvoll.



Quelle: klicksafe (2013). Wie finde ich was ich suche? Suchmaschinen kompetent nutzen. S. 23

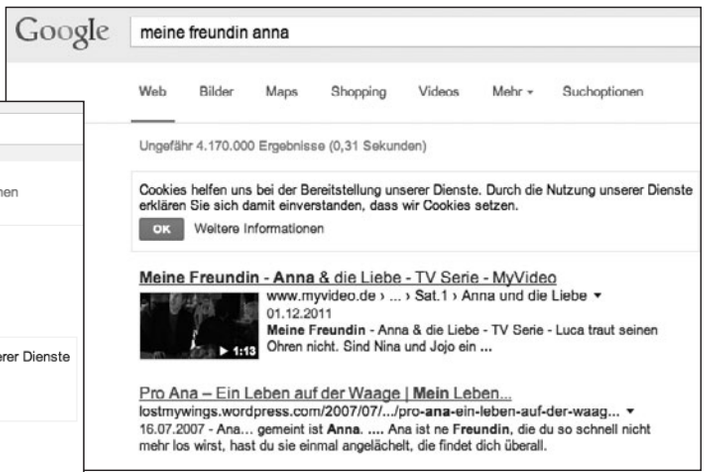
Das Problem beim Jugendschutz

Suchmaschinen listen auf, was Webseiten-Betreiber ihnen vorgeben und so kann sich hinter der harmlos lautenden Seite „Meine Freundin Anna" eine Porno-Seite oder ein anderer Inhalt verbergen, der nicht für Kinderaugen geeignet ist. Tatsächlich gerät man mit der Suchanfrage „Meine Freundin Ana" (mit einem „n") sehr schnell auf Seiten zum Thema Anorexie:



Bedingt durch Googles Autocomplete-Funktion (die automatische Vervollständigung von Suchanfragen) führt die Anfrage „Meine Freundin Anna" leicht zu einer Ergebnisliste, die auch Treffer zu „Meine Freundin Ana" aufführt.

Quelle: eigener Screenshot Google Suche; Stand: 14.10.2014



Bei einer Eingrenzung auf „Anna" ist der zweite Eintrag auch wieder ein Treffer zum Thema Anorexie.

Quelle: eigener Screenshot Google Suche; Stand: 14.10.2014

Ebenso problematisch sind Vertipper, auf die einige Webseiten-Betreiber gezielt spekulieren und entsprechende Domains anmelden. Google registriert die Vertipper der Nutzer bei Suchanfragen. In Deutschland laufen monatlich folgende Suchanfragen zu „Google" über die Google-Suchmaschine:

Google: 11.100.000
Googel: 246.000
Goggle: 135.000
Gogel: 14.800
Gugel: 4400

Quelle: Engelien & Denkena, 2012, nach eigenen Angaben von Google[5]

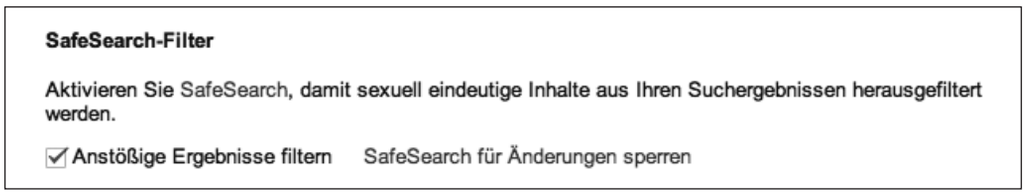
Suchmaschinen und Werbung

Normale Suchanfragen im Internet sind kostenlos. Die allermeisten Such-Hilfen finanzieren sich über Werbung, wobei wiederum Google das System über spezielle Verfahren (z. B. **AdSense** und **AdWord**, s. u. und Kapitel: Werbung) perfektioniert hat. Diese Werbung muss laut §6 des E-Commerce-Gesetzes (ECG) klar und eindeutig als solche erkennbar und damit gekennzeichnet sein. Die Bezeichnung der Werbung ist nicht einheitlich und kann „Anzeige", „Werbung", „Sponsoren-Links", „Partner-Links" o. ä. heißen, was die Erkennung für Kinder und Jugendliche erschwert.

Google-Suchanfragen im Spiegel der Zeit

Auf der Seite **www.google.com/trends** kann man sehen, nach welchen Begriffen aktuell gesucht wird bzw. nach welchen in der Vergangenheit gesucht wurde. Unter den Top-Charts der beliebtesten Suchanfragen der vergangenen Jahre lassen sich die Themen, die die Welt bzw. die Google-Nutzer bewegten, recht gut nachvollziehen.

Einige Betreiber bieten die Möglichkeit eines Jugendschutz-Filters. Bei Google nennt sich dieser Filter **Safe Search** und kann über das Zahnrad-Symbol im Browser eingerichtet werden.



Über die Google-Sucheinstellungen unter ***www.google.com/preferences*** *kann der SafeSearch-Filter ebenfalls aktiviert werden.*

Quelle: eigener Screenshot, SaferSearch-Filter; Stand: 14.10.2014

Allerdings sollte man sich auf diese Systeme nicht verlassen, denn eine hohe Filterquote ist zwar für pornografische Inhalte gegeben (aber auch hier gehen noch Seiten durch), jedoch gilt die Filterung nicht für gewalthaltige und extremistische Webseiten.

Die „ersten 20"

Der kompetente Umgang mit Ergebnissen von Suchmaschinen setzt das Wissen voraus, dass viele Anbieter von Internetseiten ein starkes Interesse daran haben, ihre Angebote in den Ergebnislisten der Suchmaschinen möglichst weit oben platziert zu sehen. Es gibt mittlerweile Berufsbilder wie den **Suchmaschinenoptimierer**, dessen Anliegen genau das ist: Er überprüft Webseiten auf ihre Platzierung innerhalb der Suchergebnisse und versucht dieses Ranking durch verschiedene Maßnahmen zu verbessern. Dies wird **Search Engine Optimization** (SEO), zu Deutsch „Suchmaschinenoptimierung" genannt. Dies können sich i. d. R. nur Firmen leisten, weshalb kommerzielle Seiten großer Anbieter bessere Ergebnisse in der Trefferliste erzielen.

Such-Algorithmus

Google benutzt angeblich über 200 Kriterien, um einem Suchergebnis seinen Platz auf der Trefferliste zuzuordnen. Die genauen Kriterien sind nicht bekannt, allerdings weiß man, dass für die Platzierung bspw. die Aktualität eines Angebots, die Anzahl der Verlinkungen durch andere Seiten sowie die Häufigkeit von themenrelevanten Keywords im Webseitentext eine zentrale Rolle spielen.

Autocomplete

Autocomplete heißt die Funktion, die aus den ersten eingegebenen Buchstaben einer Suchanfrage automatisch Suchvorschläge generiert, die dem Nutzer als Dropdown-Menü angezeigt werden. Per Mausklick kann man einen Vorschlag annehmen, ohne den vollständigen Suchbegriff eingeben zu müssen. Diesen Vorschlägen liegt ebenfalls ein Algorithmus zugrunde. Im Regelfall ist die **Autocomplete**-Funktion eine praktische Sache, dennoch ist hier Vorsicht geboten, denn populäre Vorschläge müssen nicht immer die besten sein. Mit der **Autocomplete**-Funktion befasste sich 2013 sogar der Bundesgerichtshof: Geklagt hatte ein Unternehmer, dessen Name bei einer Google-Suchanfrage automatisch mit „Scientology" und „Betrug" verknüpft wurde. Das Gericht sah darin eine Persönlichkeitsrechtsverletzung und sprach sich in seinem Urteil in einem solchen Fall für das Recht auf Unterlassung aus[6].

Filterblase?
Der Internet-Aktivist Eli Pariser machte vor einigen Jahren eine interessante Entdeckung, die er 2011 in seinem Buch „The Filter Bubble: What the Internet Is Hiding from You" vorstellte: Die Suchergebnisse sind personalisiert und hängen bspw. davon ab, von welchem Standort aus ein Nutzer sucht, welche Suchanfragen der Nutzer zuvor getätigt hat (die sog. **Search-History**) und was er oder sie angeklickt hat. Um auf das Bild der Bibliothekarin wie eingangs beschrieben zurück zu kommen: Die Bibliothekarin hat nicht nur einen eigenen Katalog an Büchern (den **Index**), sondern sortiert die Titel (das **Page Ranking**), entsprechend ihrer Einschätzung, was die Vorlieben und Interessen des Kunden sein könnten (die **Filterblase**).
Ein Beispiel aus dem Buch von Eli Pariser zeigt, wie sich diese **Filterblase** ganz konkret darstellen kann: Die Suchanfrage „BP" bringt bei dem einen Nutzer Suchergebnisse zu den Investitionsmöglichkeiten der Firma **British Petroleum** hervor, bei dem anderen Ergebnisse zur Ölpest im Golf von Mexiko, die durch die Havarie der **Deepwater Horizon** (Ölbohrplattform von BP) ausgelöst wurde[7]. Die **Filterblase** hüllt den Nutzer mit auf ihn angepassten Informationen ein, wohingegen alles außerhalb dieser Blase für ihn nicht erreichbar oder zumindest schwerer zugänglich ist. Dieser Sachverhalt wird kontrovers diskutiert:
Die einen halten ein solches System angesichts der Informationsflut für unabdingbar, die anderen fürchten die informative und intellektuelle Isolation. Dies könnte ein spannender Diskurs mit Schülerinnen und Schülern sein.

Snippets reichen
Die einzelnen Einträge in der Ergebnisliste werden bestehend aus dem Link zur Seite und einer kurzen Beschreibung, dem sog. **Snippet**, zu Deutsch „Schnipsel", dargestellt. Diese Technik wurde immer weiter verfeinert, so dass heute nicht die ersten Zeilen einer Ergebnisseite, der Titel der Seite o. ä. dargestellt werden, sondern bestenfalls eine kurze und aussagekräftige Zusammenfassung der Seiteninhalte. Den Snippet können Seiten-Betreiber entweder gezielt selbst erstellen oder von Google automatisch generieren lassen. Vielen Nutzern reicht die Zusammenfassung offenbar zur Orientierung und es wird nicht tiefergehender recherchiert. Das heißt: Die Suchmaschinensuche ist Start- und Endpunkt der Recherche. Für eine gute Recherche im schulischen oder universitären Kontext reicht das allerdings nicht aus.

Informationskompetenz
SchülerInnen müssen **Informationskompetenz** erwerben, was sie und ihre LehrerInnen angesichts der (ungefilterten) Informationsfülle vor ganz neue Herausforderungen stellt: Wichtig ist dabei, den Informationsbedarf zu allererst zu erkennen und dann zielgerichtet, auch in verschiedenen Medien, recherchieren zu können. Die Kinder und Jugendlichen müssen die Fülle der Informationsangebote analysieren können und dann effizient eine begründete Auswahl treffen. Zu guter Letzt gehört zur **Informationskompetenz** auch die Reorganisation der Informationen, bspw. in Form von Plakaten oder Schaubildern, eigenen Texten o. ä. und deren Präsentation.

Aus der Praxis
Die Schülerinnen und Schüler am Elsa-Brändström-Gymnasium Oberhausen dürfen in die Rolle eines Umweltschützers und in die Rolle eines Mitarbeiters eines Chemiekonzerns schlüpfen und für einige Zeit Google (auf getrennten Systemen) nutzen. Danach wird die Probe gemacht und für die beiden Rollen werden die jeweiligen Suchergebnisse zu ein und demselben Begriff im Plenum zusammen getragen. Das erstaunt Jugendliche wirklich! Sie fühlen sich regelrecht betrogen.

Informationskompetenz in der Schule bedeutet:

- *Erkennen des Informationsbedarfs und*
- *zielgerichtete Recherche*

durch:

- *Analyse der Informationsangebote,*
- *eine begründete Auswahl und*
- *effizienten Einsatz*

mit

- *Reorganisation und*
- *Präsentation.*

Links und weiterführende Informationen

Webseiten

www.klicksafe.de
Informationen rund um das Thema Suchmaschinen u.v.m.

www.klicksafe.de/service/fuer-lehrende/zusatzmodule-zum-lehrerhandbuch/#c15935
Das klicksafe Zusatzmodul *Wie finde ich, was ich suche* mit weitergehenden Informationen und Unterrichtsmaterialien zum Thema Suchmaschinen

Endnoten

[1] STATISTA (2015, Februar). *Marktanteile der Suchmaschinen weltweit nach mobiler und stationärer Nutzung Februar 2015.* Aufgerufen am 03.03.2015 unter http://de.statista.com/statistik/daten/studie/222849/umfrage/marktanteile-der-suchmaschinen-weltweit/

[2] STATISTA (2014, Dezember). *Suchmaschinenverteilung in Deutschland im Dezember 2014.* Aufgerufen am 03.03.2015 unter http://de.statista.com/statistik/daten/studie/167841/umfrage/marktanteile-ausgewaehlter-suchmaschinen-in-deutschland/

[3] GOOGLE (2012). *Zeitgeist 2012.* Aufgerufen am 03.03.2015 unter http://www.google.com/intl/de/zeitgeist/2012/index.html#the-world

[4] SEO-UNITED.DE (2014, Oktober). *Suchmaschinenverteilung in Deutschland* (Absatz 2). Aufgerufen am 10.10.2014 unter www.seo-united.de/suchmaschinen.html

[5] ENGELEN, M. & Denkena, J. (2012, 27. September). Feierfox bis eBya – die häufigsten Google-Vertipper. *welt.de* (Absatz 2). Aufgerufen am 10.10.2014 unter http://www.welt.de/wirtschaft/webwelt/article109493467/Feierfox-bis-eBya-die-haeufigsten-Google-Vertipper.html

[6] HAUCK, M. (2013, 14. Mai). Googles Autocomplete verletzt Persönlichkeitsrechte. *sueddeutsche.de* (Absatz 5). Aufgerufen am 09.10.2014 unter http://www.sueddeutsche.de/digital/bgh-urteil-zu-google-vervollstaendigung-autocomplete-funktion-verletzt-persoenlichkeitsrechte-1.1671964

[7] PARISER, E. (2011). *The Filter Bubble: What the Internet Is Hiding from You.* London: Penguin Press HC.

Methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1**	**AB 2**
Titel	**Blinde Kuh – auch du?**	**Orientierung auf der Ergebnisseite**
Kompetenzen	Die Schülerinnen und Schüler benutzen eine Kindersuchmaschine und können die Ergebnisse beurteilen.	Die Schülerinnen und Schüler erlangen einen ersten Überblick auf der Ergebnisseite der Suchmaschine Google.
Methoden	Internetrecherche	Internetrecherche
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	45	45
Zugang Internet/PC	ja	ja

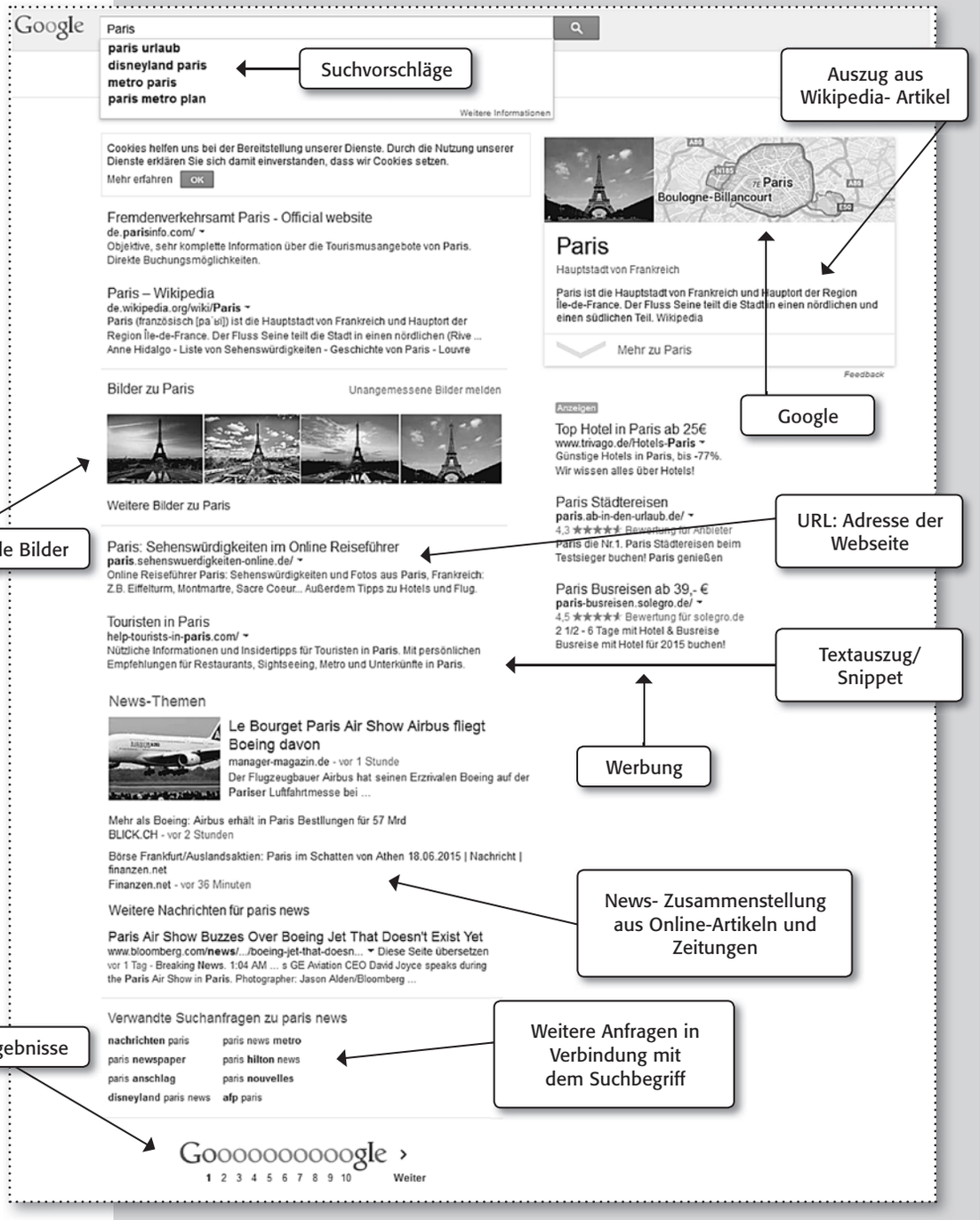
Hinweise für die Durchführung

AB 1: Blinde Kuh – auch du?	Mit diesem Arbeitsblatt sollen die Schülerinnen und Schüler die Suchmaschine Blinde Kuh kennen lernen. Durch den Suchbegriff „Meerschweinchen", den sie selbstverständlich durch ein anderes Beispiel ersetzen können, sollen sie erkennen, dass es viele „Treffer" gibt, die es einzuordnen gilt. Glücklicherweise gibt die für Kinder gemachte Suchmaschine auch nur kinderrelevante sowie eine überschaubare Anzahl von Seiten aus. Nach der Blinden Kuh sollen die Schülerinnen und Schüler die Suchmaschine FragFinn kennen lernen und einen Vergleich anstellen. Vielleicht arbeiten Sie auch hier „kooperativ": Eine Gruppe (A) benutzt Blinde Kuh, eine andere FragFinn (Gruppe B). Danach sitzt jeweils einer/eine aus Gruppe A mit Gruppe B am Computer, sie stellen die „eigene" Suchmaschine vor und tauschen ihre Ergebnisse aus. Eine Expertenrunde im naturwissenschaftlichen Unterricht, in der alle inhaltlichen Informationen zusammen getragen werden, bietet sich ebenfalls an.
AB 2: Orientierung auf der Ergebnisseite	Zeigen Sie die Trefferseite zur Suchanfrage „Paris" auf **www.google.de**, falls Internetzugang vorhanden (PDF des Screenshots auch auf **www.klicksafe.de** im Bereich Suchmaschinen). So können Sie den Aufbau einer Ergebnisseite der Suchmaschine Google, die für die Suche relevanten Bereiche sowie einzelne für Schüler eher unbekanntere Funktionen besprechen. Die Schülerinnen und Schüler füllen selbstständig die Kästchen aus. **Variation:** Lösungen auf Kärtchen oder an der Tafel vorgeben und von den Schülern zuordnen lassen.

Tipp: Hier können Sie sich selbst informieren. Tutorials zur Suche im Internet finden Sie unter **www.suche-im-internet.de/treffervideo.html**

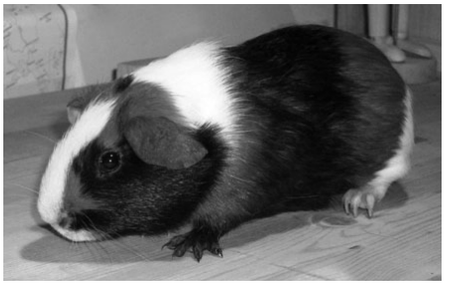
Lust auf mehr?
klicksafe hat ein umfassendes Unterrichtsmaterial zum Thema Suchmaschinen unter **www.klicksafe.de** im Bereich Materialien. Titel: Wie finde ich, was ich suche? Suchmaschinen kompetent nutzen und darüber hinaus Extra-Arbeitsblätter zum Download:
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Suchmaschine/Zusatz_AB_Suchmaschinen.pdf

Lösung:



Quelle Screenshot Google-Suche: https://www.google.de/#q=paris, 8.4.2015; 16.19 Uhr

Blinde Kuh – auch du?



Ein Meerschweinchen!
… endlich konntest du deine Eltern überzeugen, dir eines zu schenken. Du solltest dich aber vorher über Meerschweinchen informieren, damit du es auch wirklich gut pflegen und richtig behandeln kannst. Du hast auch sofort die richtigen Ideen: Einen Besuch in der Bibliothek und eine Suche im Internet werden dir sicherlich weiterhelfen.

Es gibt sehr viele Suchhilfen im Internet, sie werden „Suchmaschinen" genannt, obwohl es eigentlich Software-Programme sind. Viele der Suchmaschinen helfen Erwachsenen, etwas im riesigen Internet zu finden, wie z.B. Google. Aber es gibt auch Suchmaschinen speziell für dich. Die bekanntesten heißen ***Blinde Kuh*** *und* ***Helles Köpfchen****. Aber es gibt auch noch mehr.*

www.blinde-kuh.de
www.helles-koepfchen.de
www.frag-finn.de

1. Arbeitsauftrag:
Rufe die Internet-Seite **www.blinde-kuh.de** auf. Schreibe in das Suchfeld das Wort „Meerschweinchen", mache ein Häkchen bei „sortiert für KIDS" und klicke dann auf **Suchen**!

2. Arbeitsauftrag:
Du siehst eine Aufzählung mit so genannten „Treffern" (also Seiten, auf denen etwas über Meerschweinchen zu finden ist). Findest du auch die „weiteren Treffer"? (siehe Tipp unten!) Rufe nun einige der Seiten auf und informiere dich über Meerschweinchen, denn nachher solltest du Experte sein!

3. Arbeitsauftrag:
Wiederhole das Ganze mit den Suchmaschinen **www.helles-koepfchen.de** und **www.frag-finn.de**. Erkennst du Gemeinsamkeiten und Unterschiede? Mit welcher Suchmaschine konntest du besser umgehen?

TIPP: *Mit dem grünen Pfeil nach rechts oder mit den Zahlen 1 2 3 4 findest du noch mehr Treffer.*

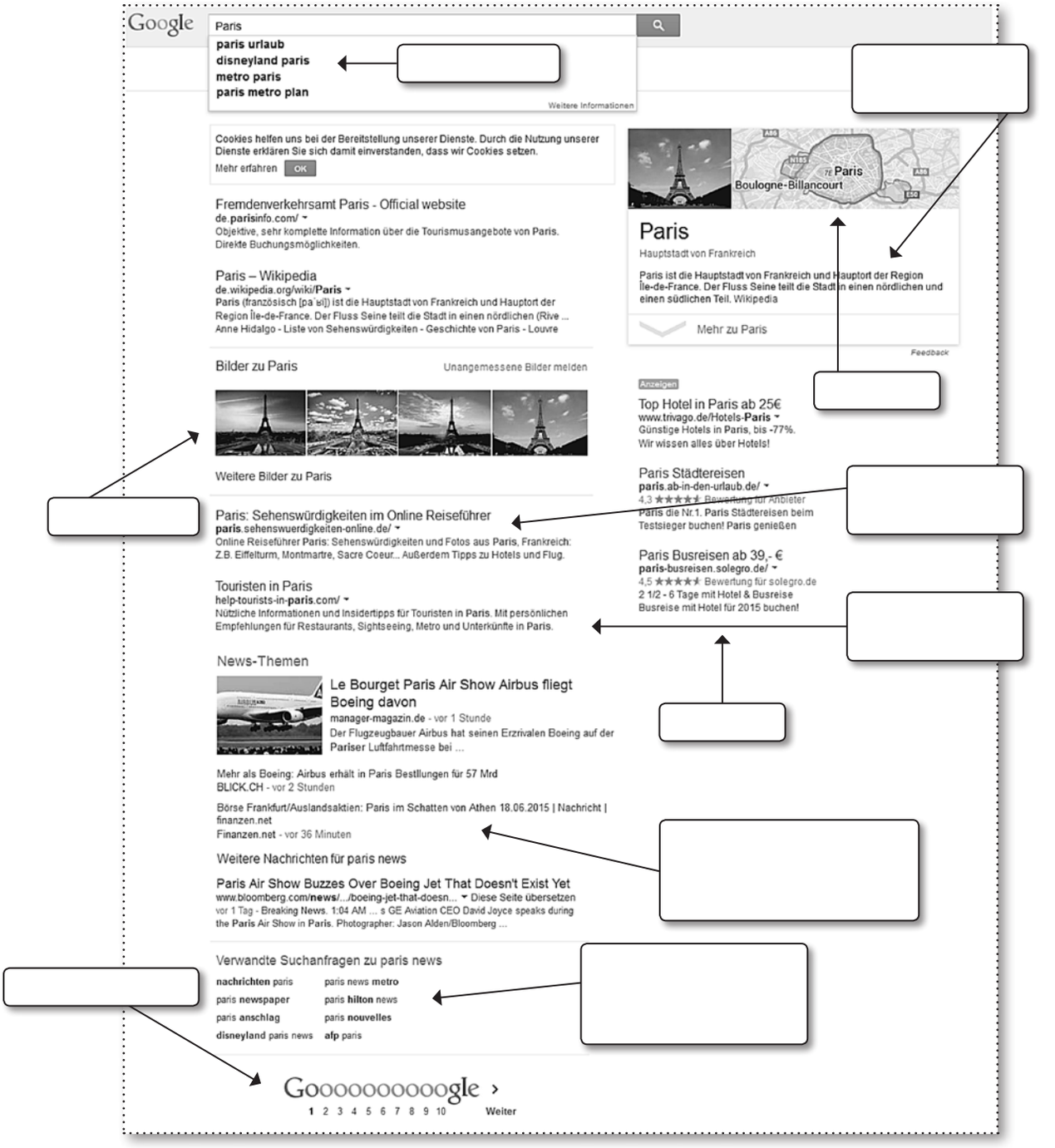
Lies die Vorschau in der Trefferliste genau und überprüfe, ob es auch wirklich das ist, was du suchst. Denn so kannst du Zeit sparen!

Orientierung auf der Ergebnisseite

Wusstest du schon: Die überwiegende Anzahl der Nutzer von Suchmaschinen klicken auf die ersten fünf Treffer. Nach der KIM-Studie 2010 arbeiten Mädchen häufiger die Ergebnisse durch. Je älter die Nutzer, desto eher schauen sie sich auch weitere Treffer an.

ORIENTIERUNG IST WICHTIG!

Arbeitsauftrag: 1. Hier siehst du einen Screenshot (= Bildschirmfoto) der Suchmaschine Google mit der Suchanfrage **[Paris]**. Nimm dir Zeit und verschaffe dir zuerst einmal einen Überblick. Wozu sind die Funktionen da, auf die die Pfeile zeigen? Fülle die Kästchen aus.



2. Vielleicht hast du dich schon über das Pfeilsymbol » gewundert, das auf dem Screenshot auftaucht. Finde selbst im Internet heraus, wozu es da ist.
Gibt es in anderen Suchmaschinen, wie z.B. **www.bing.de,** auch solche Funktionen?

Wikipedia

Wikipedia kann man eine Erfolgsgeschichte nennen, denn mittlerweile gibt es das Online-Lexikon in 287 Sprachversionen – inklusive Esperanto und Latein (Vicipædia Latina) – mit über 33 Millionen Artikeln und sie gehört international zu den Top Ten Websites! Die deutsche Wikipedia ist mit über 1,8 Millionen Artikeln die drittgrößte – täglich kommen 400 Artikel hinzu[1]. Wikipedia hat keinen kommerziellen Hintergrund, d. h. sie finanziert sich nicht über Werbung, sondern über Spenden und wird inhaltlich von vielen ehrenamtlichen Autoren getragen. Wichtig für den Einsatz von Wikipedia im Kontext der Schule: Alle Inhalte, wie Texte und Bilder, dürfen kostenfrei von jedem genutzt werden!

Längst ist Wikipedia im Schulalltag angekommen: Der (N)Onliner-Atlas stellte schon 2011 fest, dass über die Hälfte aller Lehrerinnen und Lehrer Wikipedia regelmäßig für die Unterrichtsvorbereitung nutzen[2]. Umso wichtiger ist es da, sowohl für Lehrende als auch für Lernende, zu wissen, wie Wikipedia funktioniert und welche Herausforderungen sich bei deren Nutzung stellen.

Wikimedia Foundation

Hinter der Wikipedia steht die **Wikimedia Foundation**, eine internationale gemeinnützige Stiftung mit inzwischen rund 170 Mitarbeitern. Sie wurde 2003 gegründet, hat ihren Sitz in San Francisco (USA) und betreibt alle Wikimedia-Projekte, d. h. die verschiedenen Wikipedia-Sprachversionen und ihre Schwesterprojekte, wie z. B. **Wiktionary, Wikibooks** etc. Sie ist unter anderem mit den Aufgaben betraut, Spenden zu sammeln, Markenrechte zu verteidigen, Öffentlichkeitsarbeit zu leisten sowie Software und Technik weiterzuentwickeln.

Wikimedia Deutschland e. V.

Wikimedia Deutschland e. V. ist ein eigenständiger, gemeinnütziger Verein mit rund 60 Mitarbeitern und Sitz in Berlin. Seit der Gründung von Wikimedia Deutschland im Jahr 2004 unterstützt der Verein verschiedene Wikimedia-Projekte – allen voran die deutsche Wikipedia.

MediaWiki

MediaWiki ist eine 2003 eigens für Wikipedia entwickelte, frei verfügbare Verwaltungssoftware für Inhalte in Form eines Wiki-Systems. MediaWiki ist für jedermann frei und kostenlos nutzbar und wird daher für eine Vielzahl anderer Projekte im Internet oder in Intranets verwendet. Für die Schule bedeutet das: Man kann sich sein eigenes Wiki-Projekt einrichten, bspw. im Rahmen eines Unterrichtsprojektes. Ein Anleitung dazu findet man hier: **www.mediawiki.org**

Das Grundproblem

Das Grundproblem von Wikipedia liegt in ihrer Offenheit für alle, wobei dies gleichzeitig ihre Stärke und letztendlich ihr Prinzip ist. Wikipedia hat in den letzten Jahren ein System geschaffen, mit dem eine Balance zwischen der Offenheit für jeden einerseits und der Qualitätskontrolle andererseits hergestellt werden soll. Wikipedia-Autoren können nach einiger Zeit zum sog. **Sichter** aufsteigen. Gesichtete Artikel sind frei von offensichtlichem Vandalismus und erhalten ein kleines Auge als Label:

Nach der Stufe des **Sichters,** kann man zu einem **erfahrenen Nutzer** werden und einige wenige steigen gar zum **Administrator** mit weitgehenden Rechten zur Bearbeitung/Löschung usw. auf.

Ein männliches Rudel

Es ist es eine Illusion zu glauben, dass sehr viele Menschen Wikipedia-Einträge schreiben. Der „Schwarm" – wie es so oft heißt – ist eher ein Rudel, denn nur ein harter Kern von Autoren ist sehr aktiv. Laut Wikipedia-Statistik waren es in Deutschland 2014 knapp 1000 Autoren, die sehr regelmäßig aktiv waren und monatlich um die 100 Beiträge eingestellt haben. Hinzu kommen etwa 6000 Autoren, die regelmäßig aktiv waren und ca. 5 Beiträge monatlich beisteuerten. Immer noch sind es vor allem Männer, die aktiv sind: Einer Online-Umfrage der Universität Würzburg 2005 zufolge, waren nur 10 % der deutschen Wikipedia-Autoren weiblich[4]. Nach einer Umfrage der TU Ilmenau 2009 waren es sogar nur 6 %. Bis 2015 will Wikipedia international auf einen Frauenanteil von 25 % kommen[5]. Das spricht dafür, dass dieses Ziel noch lange nicht erreicht ist. Wikipedia bemüht sich seit langem, mehr Menschen und insbesondere Frauen zur Mitarbeit zu bewegen.

Die Mitarbeit in der Wikipedia ist vielleicht ein interessantes Unterrichtsprojekt: Wikipedia-Artikel erstellen / ergänzen / verbessern! Die SchülerInnen müssen jedoch darauf vorbereitet werden, dass die Wikipedia-Community mitunter erbarmungslos ist und Artikel bspw. wegen fehlender Relevanz sofort wieder entfernt werden. Zudem ist der Ton in den Diskussionen mitunter rau und nicht umsonst gibt es einen eigenen Begriff für den Kampf verschiedener Autoren um einen Artikel: **Edit-War** oder **Bearbeitungskrieg**[6].

Aus der Praxis

*In sog. **Projektkursen** der 11. Jahrgangsstufe am Elsa-Brändström-Gymnasium Oberhausen wird immer wieder das Thema „Werde ein Wikipedianer!" vergeben. Ein oder zwei SchülerInnen dokumentieren für einige Monate ihre Mitarbeit als AutorInnen bei Wikipedia. In den letzten Jahren war diese Aktivität aus den oben genannten Gründen meist mit Frustration verbunden.*

Vandalismus, Dummheit und Manipulation

Die Wikipedia unternimmt große Anstrengungen, die Qualität der Artikel sicherzustellen s. o. und doch ist das System einer offenen Enzyklopädie nicht vor Vandalismus, Dummheit oder gezielter Manipulation gefeit. Im Oktober 2013 sperrte die Wikipedia Stiftung 250 Nutzerprofile, weil sie dahinter Personen vermutete, die Artikel im Auftrag von Firmen schreiben[7]. Es gibt immer wieder Fälle von Vandalismus, wenn etwa Artikel bewusst verfälscht werden. Selbstverständlich finden sich manchmal schlicht auch falsche Informationen in den Artikeln. Berühmt wurde bspw. der **Bicholim-Konflikt,** ein ganz und gar erfundener Krieg, der für fünf Jahre in der Wikipedia nachzulesen war[8] (welt.de, 2013, Abs. 4). Weitere Beispiele solcher Falschinformationen sind die frei erfundene Band **Tillery,** die 6 Jahre in Wikipedia aufzufinden war oder das erfundene Volk der Adyhaffen, dem ganze 5 Jahre ein eigener Artikel gewidmet war[9].

Bewertungssymbole
Wikipedia benutzt ein System von Auszeichnungen, die sie für besonders gute Artikel vergibt:

Exzellente Artikel
Diese Artikel sind außergewöhnlich gut geschrieben und wurden mit dem Prädikat exzellent ausgezeichnet. Die Artikel sind sowohl vom Inhalt als auch von Sprache, Form, Verlinkung und Bebilderung her überzeugend. Zurzeit sind 2354 Artikel (Statistik) ausgezeichnet.

Lesenswerte Artikel
Die lesenswerten Artikel sind gut geschriebene Artikel, die fachlich korrekt, gut illustriert und ansprechend formatiert sind, jedoch die Grenze zur Exzellenz (noch) nicht erreichen. Momentan sind 3754 Artikel (Statistik) mit diesem Prädikat versehen.

Informative Listen und Portale
Informative Listen und Portale sind fachlich korrekte und im Wesentlichen vollständige Artikellisten und Portale. Sie erfüllen bestimmte Qualitätsstandards, wodurch sie aus der Vielzahl von Listen und Portalen in der Wikipedia herausragen.

Exzellente Bilder
Hier sind Fotos und Grafiken, welche außerordentlich gut gelungen und perfekt zur Illustration der Wikipedia geeignet sind, ausgezeichnet. Sie sind technisch hochwertig, zeigen ein interessantes Motiv und besitzen einen enzyklopädischen Charakter.

Exzellente Aufnahmen (eingestellt)
Die exzellenten Aufnahmen sind sprachlich und aufnahmetechnisch besonders gelungene Aufnahmen gesprochener Artikel.

Quelle: Wikipedia (2015)[10]

Das gleiche geschieht mit Artikeln, die mehrere Nutzer als kritisch einschätzen. Solche Artikel erhalten eines der folgenden Symbole:

Der Schraubenschlüssel signalisiert Bearbeitungsbedarf

Das Buch signalisiert fehlende Quellen

Die Lücke signalisiert lückenhafte Informationen

Das Ausrufezeichen signalisiert fehlende Neutralität

Das Fragezeichen signalisiert, dass der Artikel nicht allgemeinverständlich formuliert ist

Quelle: Wikipedia (2014)[11]

Links und weiterführende Informationen

Webseiten

www.klicksafe.de
Informationen rund um das Thema Wikipedia u.v.m.

www.klicksafe.de/service/fuer-lehrende/zusatzmodule-zum-lehrerhandbuch/#c18286
Das klicksafe Zusatzmodul *Wikipedia – Gemeinsam Wissen gestalten* mit weitergehenden Informationen und Unterrichtsmaterialien zum Thema Wikipedia

Endnoten

[1] WIKIPEDIA (2015, 7. März). *Wikipedia:Sprachen.* Aufgerufen am 09.03.2015 unter https://de.wikipedia.org/wiki/Wikipedia:Sprachen

[2] INITIATIVE D 21. (2011). *Bildungsstudie: Digitale Medien in der Schule. Eine Sonderstudie im Rahmen des (N)ONLINER-ATLAS 2011.* Aufgerufen am 05.03.2015 unter http://www.initiatived21.de/wp-content/uploads/2011/05/NOA_Bildungsstudie_140211.pdf

[3] WIKIPEDIA (2015, 3. März). *Wikipedia-Statistik Deutsch*. Aufgerufen am 05.03.2015 unter http://stats.wikimedia.org/DE/TablesWikipediaDE.htm

[4] WIKIPEDIA (2015, 6. Februar). *Wikipedia: Wikipedistik/Soziologie – Geschlechterverteilung.* Aufgerufen am 05.03.2015 unter http://de.wikipedia.org/wiki/Wikipedia:Wikipedistik/Soziologie#Geschlechterverteilung

[5] LISCHKA, K. (2011, 2. Februar). Mitmach-Enzyklopädie: Männer schreiben die Wikipedia voll. *spiegel-online.de*. Aufgerufen am 05.03.2015 unter http://www.spiegel.de/netzwelt/web/mitmach-enzyklopaedie-maenner-schreiben-die-wikipedia-voll-a-742951.html

[6] KLEINZ, T. & Wendt, P. (2013, 25. November). Die Wikipedia und die Autoren: Die Online-Enzyklopädie soll attraktiver werden. *heise.de*. Aufgerufen am 05.03.2015 unter http://www.heise.de/newsticker/meldung/Die-Wikipedia-und-die-Autoren-Die-Online-Enzyklopaedie-soll-attraktiver-werden-2053316.html

[7] DPA (2013, 22. Oktober). Wikipedia geht gegen bezahlte Manipulation vor. *zeit.de*. Aufgerufen am 05.03.2015 unter http://www.zeit.de/digital/internet/2013-10/wikipedia-lobbyismus-sperrung-nutzer

[8] WELT.DE. (2013, 9. Januar). *Ausgedachter Krieg steht jahrelang auf Wikipedia*. Aufgerufen am 05.03.2015 unter http://www.welt.de/vermischtes/article112655248/Ausgedachter-Krieg-steht-jahrelang-auf-Wikipedia.html

[9] WIKIPEDIA (2015, 3. März). *Wikipedia: List of hoaxes on Wikipedia.* Aufgerufen am 05.03.2015 unter http://en.wikipedia.org/wiki/Wikipedia:List_of_hoaxes_on_Wikipedia

[10] WIKIPEDIA (2015, 12. Februar). *Wikipedia:Bewertungen.* Aufgerufen am 09.03.2015 unter https://de.wikipedia.org/wiki/Wikipedia:Bewertungen

[11] WIKIPEDIA (2015, 7. März). *Wikipedia Bewertungsbausteine.* Aufgerufen am 09.03.2015 unter http://de.wikipedia.org/wiki/Wikipedia:Bewertungsbausteine

Methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Orientierung auf der Artikelseite**	**Wikipedia – alles richtig?**
Kompetenzen	Die Schülerinnen und Schüler lernen, sich auf einer Wikipedia-Seite zurecht zu finden.	Die Schülerinnen und Schüler lernen die Wirkungsweise von Wikis kennen und lernen, diese kritisch zu reflektieren.
Methoden	Stummer Impuls, Analyse einer Wikipedia-Seite, Entdecker-Fragebogen	Memory, Merkzettel
Material	Wikipedia-Puzzle-Ball als Grafik, evtl. Schere und Klebstoff	Blätter DIN A3, Scheren
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	nein

Hinweise für die Durchführung

AB 1: Orientierung auf der Artikelseite

Einstieg mit einem Stummen Impuls: Zeigen Sie den Wikipedia-Puzzle-Ball (Download über die Bildersuche der Suchmaschinen, Sucheingabe „Wikipedia“).
Weisen Sie auf die Funktion hin, dass man mit einem Klick auf den Puzzle-Ball immer wieder zurück zur Wikipedia-Hauptseite kommt. Die Schülerinnen und Schüler lernen nun weitere Funktionen von Wikipedia kennen.
Auf dem Arbeitsblatt 1 „Orientierung auf der Artikelseite“ werden verschiedene Funktionen Bereichen auf der Wikipedia-Artikelseite zugeordnet. Die Schülerinnen und Schüler können die Funktionen eintragen oder die Kästchen ausschneiden und aufkleben.
Auswertung im Plenum.
Lösungsblatt zum Download auf **www.klicksafe.de/wikipedia**

Auswertungsfragen:
- Welche Funktionen sind wofür besonders nützlich und warum?
  z. B. Hinweis auf fremdsprachige Artikel (Sprachen üben), die Zitierfunktion (schnelle Zitat-Angabe) etc.
- Welche Funktion gefällt euch am besten und warum?
- Welche Funktion ist schwer zu verstehen und warum?

Mit dem Arbeitsblatt **„Entdecker-Fragebogen“** werden die benannten Bereiche selbst erkundet.

AB 2: Wikipedia – alles richtig?

Die Schülerinnen und Schüler sollen das Prinzip „Wiki“ kennen lernen und auf Papier ausprobieren. Erfahrungsgemäß kommen viele Informationen auf diese Weise zusammen, die auf Papier schwer zu sortieren sind. Dies ist mit digitalen Dokumenten einfacher.
Die Schülerinnen und Schüler sollen – selbstverständlich anhand der Wikipedia – die grundlegende Kritik an Wikipedia kennenlernen. Der Artikel ist sehr umfangreich, weshalb eine gruppenteilige Auswahl von einzelnen Überschriften/Aspekten sinnvoll ist.
Vielleicht lassen Sie die Schülerinnen/Schüler nach Interesse/Neugierde selbst auswählen.
Um zu verstehen, dass es Kontrollen durch die Wikipedianer gibt, können Sie nun ein Memory durchführen, durch das die Schüler spielerisch die verschiedenen Kontrollmöglichkeiten kennen lernen. In Form eines Merkzettels sollen die Schülerinnen und Schüler das Gelernte festhalten und bei der nächsten Anwendung von Wikipedia zur Verfügung haben.

Methode Memory (für 30 Schülerinnen und Schüler/15 x 2 Kartenpaare)
Zerschneiden Sie die Kopiervorlage Memory und verteilen Sie die einzelnen Kärtchen an die Schülerinnen und Schüler. Diese sollen sich frei im Raum bewegen und sich zu richtigen Kombinationen zusammenfinden (bei großen Gruppen entsprechend mehr Kopien anfertigen). Die Schülerinnen und Schüler erklären jeweils das von ihnen gezogene Kärtchen.
Variationen: Wählen Sie nur bestimmte Kärtchen aus (die ersten 7 Kärtchen sind leichter zu verstehen als die folgenden 7). Verteilen Sie alle Kärtchen auf dem Boden und lassen Sie die Schülerinnen und Schüler in einem Sitzkreis die passenden Teile zusammenbringen, die dann erklärt und durch das Plenum ergänzt werden können.

Auswertung des Memorys: Welche Funktionen oder Prinzipien findet ihr am sinnvollsten (Ranking 1 bis 3)?

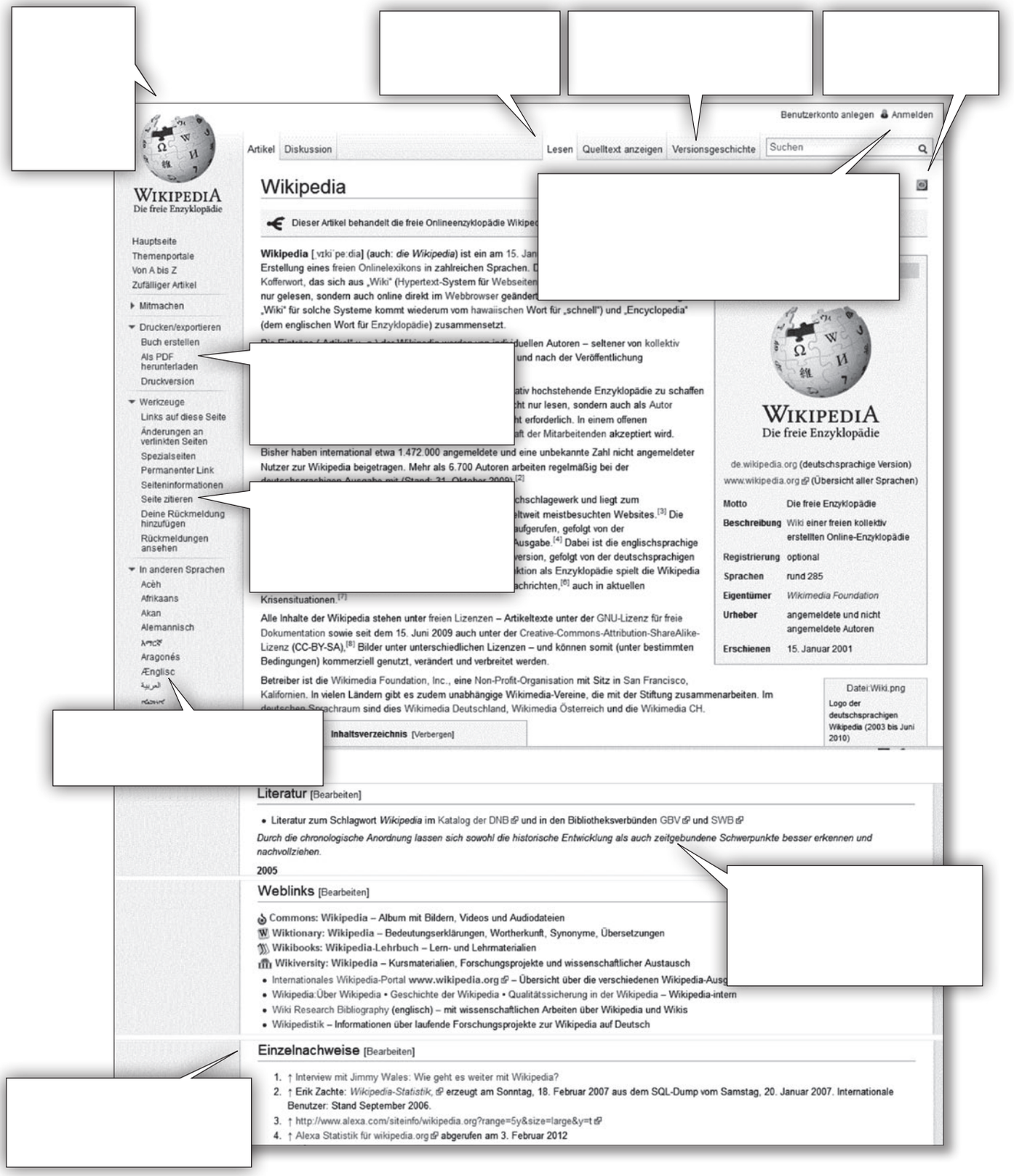
Lust auf mehr?
Methode „Der schnellste Weg“
Die Schülerinnen und Schüler sollen sich mit möglichst wenigen Klicks von einem Wikipedia-Artikel zu einem anderen klicken. Dazu werden vorher 2 Begriffe an die Tafel geschrieben. Die Schülerinnen und Schüler bekommen folgende Aufgabe (hier das Beispiel: von Artikel „Vampir“ zu „Sexualität“):

1. Tippt bitte diesen Begriff ins Suchfenster von Wikipedia: Vampir.
2. Ab jetzt dürft ihr nur noch die Maus, aber nicht die Tastatur benutzen.
3. Sucht den schnellsten Weg zwischen den beiden Artikeln „Vampir“ und „Sexualität“.
4. Wer glaubt, einen Weg zu kennen (oder eine Idee hat), soll laut rufen. (Der Lehrer notiert diesen Weg an die Tafel.)
5. Die Klicks werden gezählt. Wer die wenigsten Klicks benötigt, gewinnt.
6. Die Schülerinnen und Schüler sollen den Weg nachvollziehen.

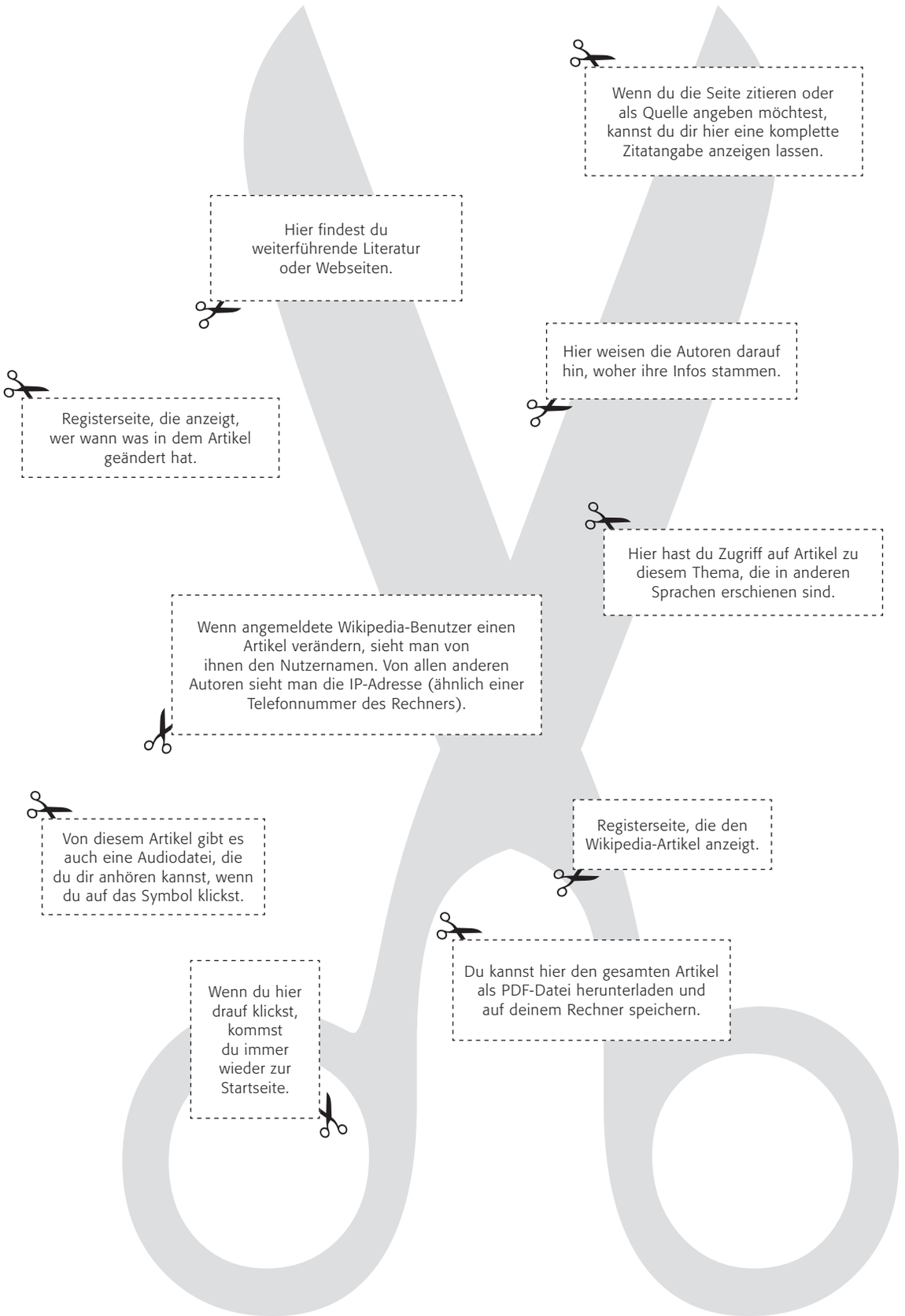
Anderes Beispiel: von Artikel „Harlem Shake“ zu Artikel „Angela Merkel“
Möglicher Weg: Harlem Shake – YouTube – Deutschland – Angela Merkel

Orientierung auf der Artikelseite (1/3)

Arbeitsauftrag: *Ordne die Kästen mit den Erklärungen den passenden Stellen auf der Wikipedia-Artikelseite zu. Du kannst sie ausschneiden und aufkleben oder die Sätze abschreiben.*



Orientierung auf der Artikelseite (2/3)



Orientierung auf der Artikelseite (3/3)

Entdecker-Fragebogen

	Auftrag	**Zum Beispiel** Stand 22.7.2013	**Dein Ergebnis:**
1.	Trage den Namen deines Wohnortes ein oder den Namen der nächstgrößeren Stadt, zu der es einen Wikipedia-Eintrag gibt.	Hannover	
2.	Wechsle zur Versionsgeschichte. Wann ist die letzte Änderung erfolgt?	4. Juli 2013	
3.	Wer hat die Änderung vorgenommen?	Horst Gräbner	
4.	Wird deine Schule/Einrichtung in dem Artikel direkt oder indirekt erwähnt?	nein	
5.	Wenn ja, an welcher Stelle (Welches Kapitel)?	–	
6.	Wenn nein: An welcher Stelle könnte sie erwähnt werden?	Kapitel Schulen	
7.	Sieh dir die Abbildungen an. Gibt es eine Gesamtansicht des Ortes?	ja	
8.	Klicke dieses (oder ein anderes) Bild an und notiere die Bildbeschreibung auf Wikimedia Commons.	Neues Rathaus	
9.	Wer hat das Foto gemacht?	Axel Hindemith	
10.	Gehe zurück zum Artikel und dort zum Abschnitt „Literatur“. Notiere den neuesten hier genannten Titel.	Oliver Falkenberg, Linda Sundmaeker: Hannover – Ein Porträt. Edition Temmen, Bremen 2008	
Falls du noch Zeit hast:			
11.	Gehe zu „Einzelnachweise“ und prüfe, ob die Links noch funktionieren. Tun sie das?	ja	
12.	Gehe auf die Abrufstatistik. Du findest sie unter jedem Artikel. Wie oft wurde der Artikel in den letzten 30 Tagen aufgerufen?	50490 Mal	
13.	Gibt es einen Artikel über deinen Ort auf Englisch? Wenn ja: Wie wird der Ortsname dort geschrieben?	Hanover	

Urheber: cc-by-sa Dr. Andreas Müller; lizensiert unter creativecommons.org/licenses/by-sa/3.0/de

Wikipedia – alles richtig? (1/3)

Wikiwiki – das heißt auf hawaiianisch „schnell" und schnell ist eine Suche in „Wikipedia" wirklich. Du kennst sicherlich die Online-Enzyklopädie, in der man wirklich fast alles schnell findet! Das Wort „Wikipedia" ist übrigens ein Kunstwort aus „Wikiwiki" und „Encyclopedia", dem englischen Wort für „Enzyklopädie". (Schlag doch mal bei Wikipedia nach, was „Wikiwiki" bedeutet …)

Die Idee einer Internet-Enzyklopädie ist alt und wechselvoll. Seit 2001 gibt es Wikipedia in seiner heutigen Form (um genau zu sein, am 15.1.2001 ging die Seite **www.de.wikipedia.org** online). Und seit damals hat Wikipedia eine einfache wie geniale Idee: Viele wissen viel! Seit damals darf jeder bei Wikipedia Texte schreiben oder ändern.

1. Arbeitsauftrag:
Eine kleine Übung: Erstellt ein Wiki zum Thema FC Bayern München (wahlweise über euren Heimat- oder Lieblingsverein) oder zum Thema Reiten. Nehmt bitte ein großes Blatt (DIN A3) und schreibt das Thema darauf. Lasst das Blatt herumgehen und jede/jeder schreibt das auf, was sie/er weiß. Jeder darf auch Änderungen an den Texten der anderen vornehmen!

Was am Computer gut geht, sieht auf Papier sicherlich ziemlich chaotisch aus, oder? Aber trotzdem finden sich bestimmt viele Informationen, weil jeder etwas beitragen konnte. Genau darin liegt aber auch ein großes Problem von Wikipedia. Niemand weiß, ob die Informationen wirklich richtig sind oder nicht! Deshalb gibt es für Wikipedia immer einen guten Tipp: Kontrolliere die Information immer aus einer weiteren Quelle!

2. Arbeitsauftrag:
Wikipedia ist wirklich einmalig. Dort findet sich sogar ein Artikel über „Kritik an Wikipedia" unter **http://de.wikipedia.org/wiki/Kritik_an_Wikipedia**. Bitte sucht euch gruppenteilig einzelne Überschriften aus und informiert euch anschließend über die Kritik an Wikipedia.

Wie kann man die einzelnen Probleme umgehen?
Die Antworten findet ihr in einem Memoryspiel.

Hier findest du eine Checkliste, die dir hilft, Wikipedia-Artikel besser einschätzen zu können.
http://bit.ly/1AeZlKU

Wikipedia – alles richtig? (2/3)

Schurken, Trolle und Vandalen

de.wikipedia.org/wiki/Wikipedia:WikiProjekt_Vandalismusbekämpfung/Troll-Dokumentationsseiten

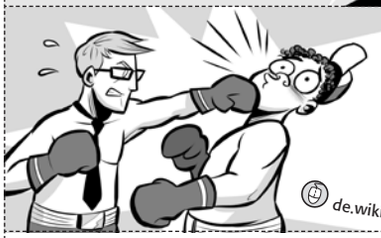
Benutzer, die Seiten absichtlich zerstören – sei es, um einen Artikel oder Teile davon zu löschen oder Unsinn einzufügen.

Vandalismusbekämpfer

de.wikipedia.org/wiki/Wikipedia:Vandalismus

Wikipedianer, die Änderungen an Artikeln kontrollieren und Vandalismus an Artikeln (z. B. eingefügten Unsinn, Löschen von Artikelinhalten) rückgängig machen. Diesen Vorgang nennt man „Sichtung".

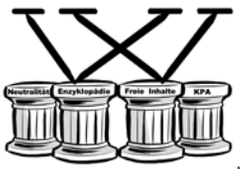
Edit-War („Bearbeitungskrieg")



de.wikipedia.org/wiki/Wikipedia:Edit-War

Benutzer machen immer wieder abwechselnd die Änderungen anderer Benutzer rückgängig oder überschreiben diese wieder mit neuen Änderungen.

Grundprinzipien



de.wikipedia.org/wiki/Wikipedia:Grundprinzipien

Zu den Grundprinzipien gehört: Die Urheberrechte beachten, einen neutralen Standpunkt einnehmen und niemanden beleidigen.

Sichtung von Artikeln

de.wikipedia.org/wiki/Wikipedia:Gesichtete_Versionen

nicht gesichtet | gesichtet

Ein gesichteter Artikel ist eine speziell gekennzeichnete Version eines Artikels. Die Kennzeichnung sagt aus, dass ein erfahrener Wikipedia-Autor den Artikel durchgesehen hat und die Version frei von offensichtlichem Vandalismus ist. Sie sagt nichts über die Qualität des Artikels aus oder darüber, ob der Artikel fachlich geprüft wurde.

Exzellente/Lesenwerte Artikel

de.wikipedia.org/wiki/Wikipedia:Bewertungsbausteine

Der Artikel wurde von vielen Nutzern für besonders gut und fehlerfrei befunden. Beachte: Fehler sind selten, aber trotzdem nicht ausgeschlossen!

Kritische Artikel

de.wikipedia.org/wiki/Wikipedia:Meinungsbilder/Symbole_der_Artikelbausteine

Einige Nutzer bemängeln diesen Artikel wegen fehlender Quellen oder mangelnder Neutralität.
Tipp: Beachte die Argumente der Diskutierenden, wenn du den Artikel trotzdem benutzen möchtest. Schaue dazu in der Versionsgeschichte oder auf der Diskussionsseite nach.

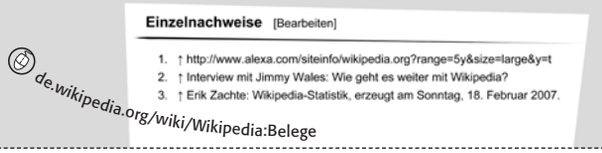
Versionsgeschichte

de.wikipedia.org/wiki/Wikipedia:Versionsgeschichte

Sie enthält alle Versionen der angezeigten Seite. Hierdurch kann man zurückverfolgen, wie eine Seite entstanden ist und wer in letzter Zeit etwas an der betreffenden Seite geändert hat.

Wikipedia – alles richtig? (3/3)

Quellenangaben/Belege

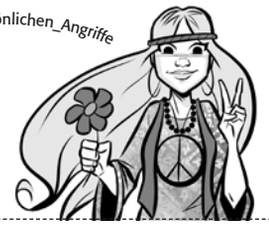


de.wikipedia.org/wiki/Wikipedia:Belege

In Wikipedia-Artikeln sollen Belege angegeben werden (Belegpflicht). Artikel sollen sich nur auf zuverlässige Quellen stützen (Glaubwürdigkeit). Belege in Wikipedia-Artikeln sollen die Nachprüfbarkeit von Informationen gewährleisten.

de.wikipedia.org/wiki/Wikipedia:Keine_persönlichen_Angriffe

„KPA"



Eine der Regeln für Wikipedia-Autoren: „Keine persönlichen Angriffe", auch wenn man unterschiedlicher Meinung ist.

„3M"

de.wikipedia.org/wiki/Wikipedia:3M

Auf den Diskussionsseiten der Artikel wird oft über inhaltliche Dinge diskutiert. Wenn es bei diesen Diskussionen zu keiner Lösung kommt, kann man auf der 3M („Dritte Meinung") andere Wikipedianer um ihre Meinung bitten, um so eine festgefahrene Diskussion zu klären.

Spielwiese

de.wikipedia.org/wiki/Wikipedia:Spielwiese

Hier kann man das Bearbeiten von Artikeln üben. Sie wird täglich „gemäht", d. h. der eigene Eintrag ist dann nur noch in der Versionsgeschichte sichtbar.

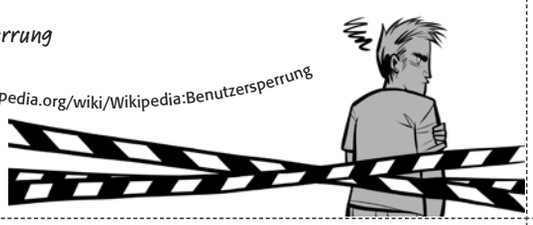
Mentorenprogramm

de.wikipedia.org/wiki/Wikipedia:Mentorenprogramm

Auf dieser Seite wird neuen Autoren, die in Wikipedia mitarbeiten wollen, auf freiwilliger Basis ein persönlicher Ansprechpartner für die ersten Schritte bei Wikipedia vermittelt.

Benutzersperrung

de.wikipedia.org/wiki/Wikipedia:Benutzersperrung



Sie ist ein Mittel, um einem Benutzer, der die Grundprinzipien missachtet, eine Zeit lang oder auf unbeschränkte Zeit die Schreibrechte zu entziehen. Nur ein Administrator kann einen solchen Schritt durchführen.

Helferlein

de.wikipedia.org/wiki/Wikipedia:Helferlein

Kleine Softwaretools, die von vielen Autoren genutzt werden, um Artikel zu verbessern (z. B. Korrekturprogramme für die Rechtschreibung).

Bildquelle: Sarah Burrini

3

Was wir lieben: Mobiles Internet, Kommunikation und Spiele

3|1 Mobiles Internet und Smartphones

3|2 Apps

3|3 WhatsApp und Co

3|4 Skype

3|5 Computerspiele

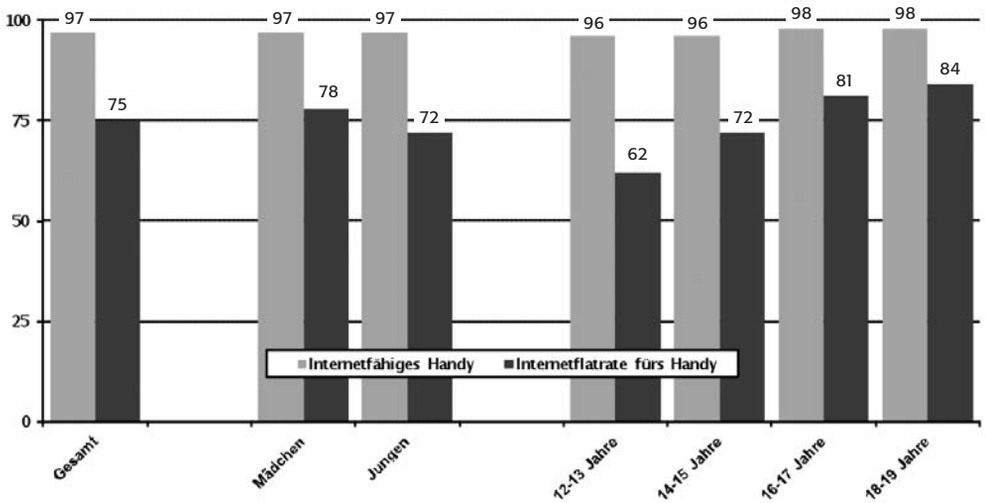
Was wir lieben: Mobiles Internet, Kommunikation und Spiele
3_1 Mobiles Internet und Smartphones
3_2 Apps
3_3 WhatsApp und Co
3_4 Skype
3_5 Computerspiele

Mobiles Internet und Smartphones

Trends: Mobiles Internet + Smartphone
Der Trend hin zu mobilen, internetfähigen Endgeräten wie u.a. Laptops, Tablets, mobile Spielekonsolen oder Smartphones ist weiterhin ungebrochen: Nach der **Jugend, Information, (Multi-)Media**-Studie (JIM) 2015 sind 97 % der befragten Jugendlichen mit einem internetfähigen Handy und 75 % mit einer Internet-Flatrate ausgestattet[1].

Vermutlich werden diese Zahlen in den kommenden Jahren noch weiter steigen und schon bald wird man in Bezug auf das Smartphone von einer Vollausstattung unter den Jugendlichen sprechen können. Ungeahnte Möglichkeiten bietet dies für den Unterricht, denn bspw. eine Internetrecherche ist dann nicht mehr an Informatikräume gebunden.

Mobiles Internet 2015
– Ausstattung des eigenen Handys –



Quelle: MPFS (2015); Angaben in %; Basis: Handy/Smartphone, n=1.179[2]

Exkurs: Mobile Internetnutzung
Möglich wurde dieser Trend durch die technischen Entwicklungen eines schnellen Mobilfunk-Standards und die massenhafte Verbreitung von WLAN (**W**ireless **L**ocal **A**rea **N**etwork) an öffentlichen Orten, in Privathaushalten, in Institutionen etc. WLAN bezeichnet ein Funknetz, das räumlich begrenzt mittels eines Routers eine Internet-Verbindung ermöglicht. In einigen Ländern wird dafür der Begriff **WLAN-Hotspot** oder auch **Wi-Fi** verwendet. Anders als oft angenommen, steht **Wi-Fi** nicht für **Wireless-Fidelity**, sondern ist schlicht ein aus Marketinggründen erfundener Kunstbegriff[3].

Erwähnt sei auch die Möglichkeit, eine Internetverbindung über Satellit herzustellen, die allerdings sehr langsam und teuer ist. Sie wird nur dort genutzt, wo es keine andere Verbindungsmöglichkeit gibt, z. B. wegen fehlender Infrastruktur. Dies könnte sich allerdings ändern, wenn der Google-Konzern seine Tests zur Internet-Verbindung per Fesselballon erfolgreich abschließt. 2013 hat Google in Neuseeland das Projekt **Loon** ins Leben gerufen und 30 Ballons in 20 Kilometer Höhe in die Stratosphäre aufsteigen lassen. Diese Ballons sind mit einer Technik versehen, die eine Kommunikation per UMTS (Universal Mobile Telecommunications System) ermöglicht. Die Ballons fungieren sozusagen als fliegende Sendemasten, die überall eingesetzt werden können – auch in den entlegensten Gebieten der Erde[4].

Der Internetzugang ist damit nicht mehr an ein fest installiertes Kabel gekoppelt und damit ortsunabhängig.

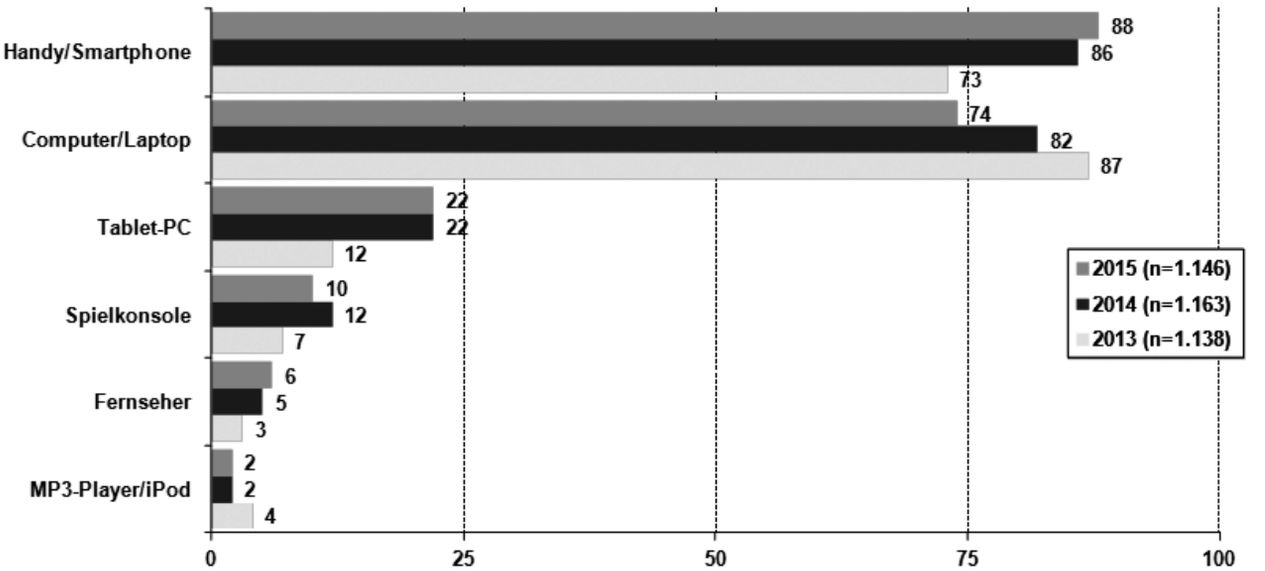
Jugendliche zu drei Viertel mobil online

Parallel zur Verbreitung des mobilen Internets haben sich die einst nur zum Telefonieren verwendeten Handys zu wahren Alleskönnern entwickelt – zu Smartphones – die eine Vielzahl an Funktionen bieten.

Während die JIM-Studie einen Rückgang der Internetnutzung über Computer/Laptop feststellt, verzeichnet sie gleichzeitig eine Zunahme der Internetnutzung mittels Handy/Smartphone:

Wege der Internetnutzung 2013–2015

– in den letzten 14 Tagen –



Quelle: MPFS (2015). JIM 2013–JIM 2015. Angaben in %; Basis: Befragte, die mind. alle 14 Tage das Internet nutzen[5]

Jugendliche ständig am Handy?!

Die repräsentativen Daten der JIM-Studie bestätigen, was sich auch im Alltag oft beobachten lässt: Jugendliche verbringen viel Zeit mit ihrem Smartphone. Laut der JIM-Studie liegt alleine die Internetnutzung Jugendlicher, bedingt durch die hohe Dichte internetfähiger Smartphones, bei durchschnittlich 208 Minuten pro Tag[6]. Das Handy bzw. Smartphone ist also ständig im Gebrauch, um bspw. mit anderen zu kommunizieren, Bilder oder Videos anzusehen etc. Dazu kommen jedoch noch all die anderen Anwendungen, die nicht auf einer Internetverbindung basieren, wie Musikplayer, Kamera etc. Im pädagogischen Sinne spannend ist sicherlich eine Diskussion um einen zeitweisen Verzicht auf das Handy (sog. **Handyfasten**) und über die Frage, wann man für wen eigentlich erreichbar sein muss oder möchte.

Smartphones: Die Anfänge

Die letzten Jahrzehnte haben der Technikgeschichte so manches Kapitel hinzugefügt. Technische Errungenschaften, die noch vor einigen Dekaden als nicht zu verwirklichen galten, sind längst Teil der Alltagsrealität geworden. Noch 1860 sagte der deutsche Physikprofessor Johann Christian Poggendorf: „It is impossible to transmit speech electrically. The 'telephone' is as mythical as the unicorn"[7]. Nur ein Jahr später stellte Philipp Reis den Prototyp seines **Telephons** öffentlich vor. Seine Erfindung diente als Grundlage für die Weiterentwicklung durch Alexander Graham Bell, der in den USA dann ein Patent auf „sein" Telefon anmeldete[8]. Rund 120 Jahre später, Anfang der 90er Jahre, kommt der **Simon Personal Communicator** der Firmen **BellSouth** und **IBM** auf den Markt – das erste Smartphone ist geboren[9].

Die eigentliche Revolution aber stellte das **iPhone** der Firma Apple aus dem Jahre 2007 dar, denn dieses besaß bereits eine Multitouch-Bedienoberfläche, einen sog. **Touchscreen**. Die kleinen Tasten der Handys mit der Mehrfachfunktion einer Taste – auf der Taste 2 findet man bspw. die Buchstaben a, b, c, die man der Reihe nach per Tastendruck aufruft – waren damit überholt. Der Benutzer hat nun eine vollständige, virtuelle Tastatur zur Verfügung, was die Bedienung vereinfacht.

Das englische Adjektiv „smart" bedeutet „klug", „schlau" oder auch „geschickt". Ein „smartes Phone" bezeichnet also ein Gerät, das gegenüber einem herkömmlichen Handy weitaus mehr Funktionen und daher mehr Möglichkeiten bietet (s. u.).

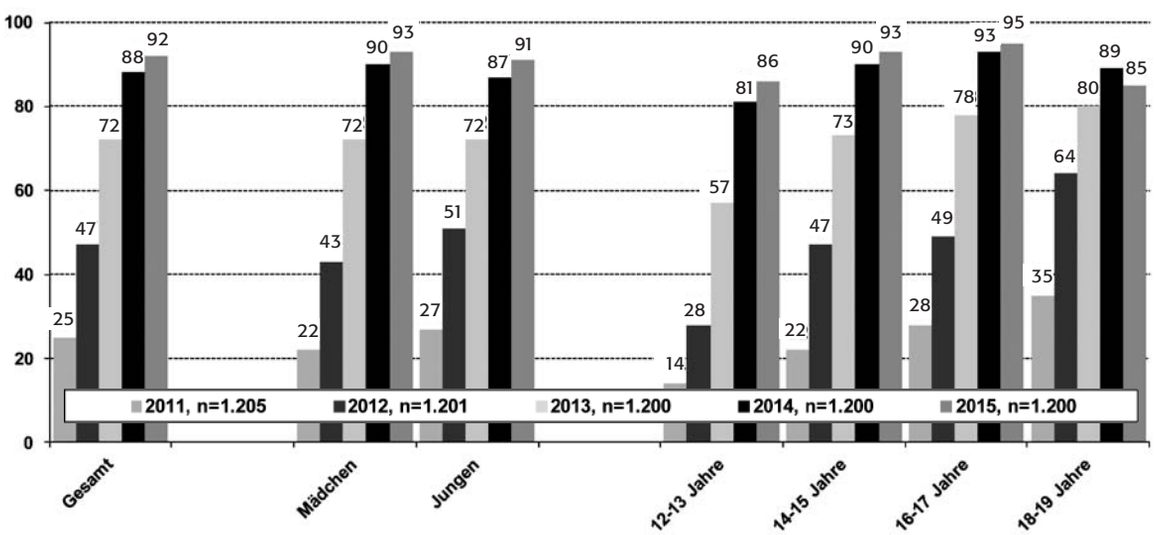
Der Siegeszug

Mit der Markteinführung des iPhones 2007 setzt das Smartphone zu einem weltweiten Siegeszug an: Alleine in Deutschland wurden 2010 über zehn Millionen Smartphones verkauft, 2011 knapp 15 Millionen, 2012 über 21 Millionen und 2013 schließlich 26,4 Millionen. Der Umsatz für die Branche stieg in dieser Zeit von 3,4 Milliarden auf 8,3 Milliarden Euro[10].

Diffusion in die Taschen der Jugendlichen

Die **Diffusionstheorie** beschreibt verschiedene Phasen bis eine Innovation eine Gesellschaft vollständig durchdrungen hat. Jugendliche sind allgemein in besonderem Maße sog. **early adopters**. Darunter versteht man eine Personengruppe, die etwas Neues, wie bspw. eine technische Innovation, schnell aufgreift und ausprobiert. So ist es leicht verständlich, weshalb sich der Anteil der Smartphone-Besitzer unter den Jugendlichen unabhängig von Geschlecht und Schulform von 25 % im Jahr 2011 auf 92 % 2015 nahezu vervierfacht hat[11].

Smartphone-Besitzer 2011–2015



Quelle: MPFS (2015). JIM 2011–JIM 2015. Angaben in %; Basis: alle Befragten[12]

Das Taschenmesser-Pendant
Das digitale **Schweizer Taschenmesser**, der **Alleskönner** – so lauten Spitznamen für das Smartphone. Und tatsächlich vereinen diese viele Funktionen in sich, die andere Geräte dadurch überflüssig erscheinen lassen. Zudem gibt es für (beinahe) alles eine App, die sich der Nutzer problemlos auf das Smartphone laden kann.

Das Smartphone ist …

- Digitalkamera (Foto und Video)
- Armbanduhr/Wecker/Stoppuhr
- Navigationsgerät/Fahrtenbuch
- Telefonzelle/Festnetzanschluss
- Taschenlampe
- Papierkalender/Timer/Notizbuch
- CD-Player/MP3-Player
- Radio
- Diktiergerät
- DVD-Player/Festplattenreceiver
- Spielekonsole
- Fahrplan für den Öffentlichen Personennahverkehr
- Bahn-Fahrkarte/Flugticket
- Lexikon/Sprach-Wörterbücher
- Scanner
- Kreditkarte/EC-Karte/Bargeld
- WLAN-Router
- Wasserwaage
- u. v. a.

Quelle: Eigene Darstellung, In Anlehnung an Müller (2011)[13]

Aus der Praxis
Zum Thema „Smartphone" bietet sich für den Unterricht sowohl die Frage nach den Nutzungsgewohnheiten (Wie oft?/Wie lange?/Wozu?) der Jugendlichen an als auch ein 24-Stunden-Experiment: Die Schüler sollen in den nächsten 24 Stunden zählen, wie oft sie ihr Smartphone (sinnhaft) in die Hand nehmen. Die Dauer der einzelnen Nutzung ist schwieriger zu erfassen und spielt daher keine Rolle. Konkretes Bsp.: Eine WhatsApp-Nachricht ist ebenso eine einzige Nutzung wie ein 30-Minuten-Telefonat oder ein Spiel über 20 Minuten. Die SchülerInnen machen das wirklich gerne und sind sehr gespannt auf die Auswertung. Diese sollte anonym erfolgen.

Die Herausforderungen
Jugendliche vergessen gerne, dass sie mit dem Smartphone in gewisser Weise auch einen Spion in der Tasche tragen. Ist es in Betrieb, erfasst es mittels eines Systems namens **Global System for Mobile Communications** (GSM), in welche Funkzelle das Gerät eingeloggt ist – in Ballungsgebieten auf 100 Meter genau. Ist bei einem Smartphone das **Global-Positioning-Signal** (GPS) aktiviert, so kann darüber ein Bewegungsprofil erstellt werden. Für Android-Nutzer ist dieses über ihren Google-Account einsehbar.

Tipp: *Ein Erklärfilm zu Bewegungsprofilen bei* ***Handysektor*** *unter:*
http://www.handysektor.de/navigation-paedagogen/paedagogenecke/videos.html

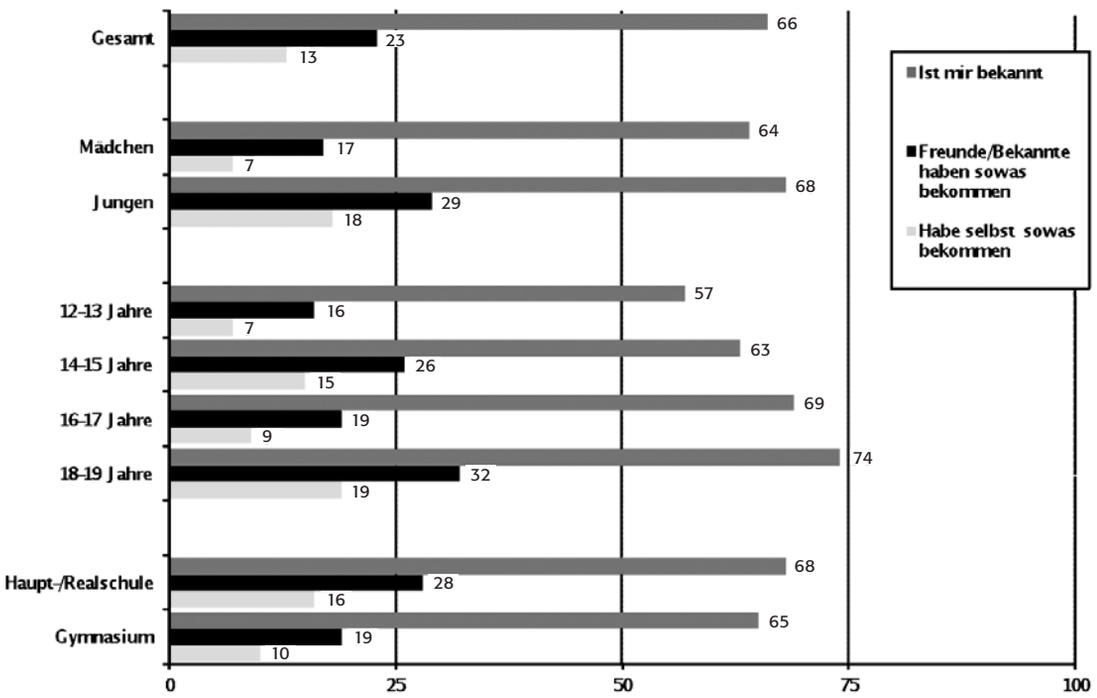
Nutzt man sein Smartphone, hinterlässt man gleichzeitig eine deutlich sichtbare Datenspur:

- evtl. den Inhalt der Kommunikation (Texte, Bilder, Videos)
- die Daten auf der SIM-Karte, z. B. Adressbücher
- die persönlichen Daten beim Mobilfunkanbieter mit Bestandsdaten und Personenauskunft wie Adresse, Telefonnummer
- die Standortdaten des Handys/die Funkzelle, in der sich das Handy befindet
- die Rechnungsdaten über den Mobilfunkanbieter
- die Verkehrsdaten über die Kommunikation
- u. a.

Neben dem Datenschutz (mehr dazu im Kapitel 5_3) gibt es zahlreiche weitere Herausforderungen. 2006 beschrieb die Medienpsychologin Nicola Döring die problematischen Aspekte der Handynutzung, die heute aktueller sind denn je[14]:

- Kriminelle Risiken bspw. durch Voyeurismus, Cyber-Mobbing, Verletzung der Persönlichkeitsrechte
- Kostenrisiken durch Abzocke-Methoden, Warteschleifen, teure Sondernummern, Mehrwertdienste (in Bezug auf das Smartphone sind es v. a. auch die In-App-Käufe)
- Normverletzungen bedingt durch die schnelle Kommunikation, z. B. unangemessene Telefonate oder problematische Nachrichten zwischen Partnern (z. B. Schlussmachen per SMS)
- Abhängigkeit mit allen Folgen
- Gesundheitsrisiken, die durch die Handystrahlung entstehen können
- Jugendgefährdende Inhalte, mit denen die Nutzer leicht konfrontiert werden, v. a. Gewalt-Videos und Pornografie. In der JIM-Studie 2015 gaben 23 % der Jugendlichen an, ein Bekannter hätte so etwas schon erhalten. 13 % erhielten selbst brutale Videos oder Pornofilme auf ihr Handy:

Verschicken von brutalen Videos oder Pornofilmen aufs Handy 2015



Quelle: MPFS (2015); Angaben in %; Basis: Besitzer Handy/Smartphone n=1.179 [15]

Aus der Praxis

Das Thema „Smartphone bzw. Handy" berührt die Alltagswelt der Jugendlichen, weshalb diese motiviert sind, sich zu diesem Thema im Unterricht einzubringen. Wichtig ist es v. a. Risiken und Chancen gleichermaßen im Blick zu behalten.

Das **Bundesamt für Sicherheit in der Informationstechnik** (BSI) hat 2011 ein sehr umfassendes Überblickspapier zu Smartphones veröffentlicht. Darin sind die folgenden technischen Risiken aufgelistet[16]:

- Gefahr des Diebstahls der Hardware und damit u. U. sensibler Daten
- über unsichere Datenverbindungen (z. B. USB, WLAN oder Bluetooth) können Daten entwendet werden
- Schadsoftware kann aufgespielt werden (z. B. Anwahl teurer Sondernummern, Verschicken gefährlicher Links an bekannte Adressen aus dem Adressbuch, Spam-Angriffe auf andere, Missbrauch von Apps)
- Gefahr von Phishing Angriffen besteht
- die Kontrolle von Internet-Links ist schwieriger
- Lokalisierungsdienste ermöglichen die Erstellung von Bewegungsprofilen

So kann man seine Daten schützen

Da ein Smartphone viele teils auch sehr persönliche Daten, wie z. B. Bilder, Videos, Nachrichten etc. enthält, sollten diese Daten vor unbefugten Dritten unbedingt geschützt werden. Aus diesem Grund sind unsichere Pins (wie z. B. 1234 oder 0000), die schnell zu „knacken" sind, zu vermeiden. Auch Sperrmuster sind nicht unproblematisch, denn leicht lassen sich verräterische Fettflecken auf dem Touchscreen erkennen. Der **FaceUnlock** gilt darüber hinaus als unsicher und sollte nicht benutzt werden – ein Foto reicht, um das System auszutricksen.

Gegen den Diebstahl eines Handys kann man sich zwar kaum schützen, jedoch besteht die Möglichkeit Apps zu installieren, die das Auffinden des Smartphones zumindest möglich machen, z. B. über eine Standort-Überwachung mittels Kamera und GPS-Daten. Wichtig ist v. a. den Schaden nach dem Verlust des Smartphones zu begrenzen und dafür Sorge zu tragen, dass die gespeicherten Daten nicht von Unbefugten heruntergeladen werden können. Hier gibt es die Möglichkeit, das Smartphone so einzustellen, dass alle Dateien automatisch gelöscht werden, wenn die PIN mehrere Male falsch eingegeben wurde.

Viele Apps verlangen Zugriff auf Informationen, die für das Funktionieren der App nicht zwingend erforderlich sind. Diese Informationen, z. B. Telefonbuchdaten, Nachrichten, Bilder etc., stehen damit dem Zugriff durch App-Anbieter offen. Unklar bleibt oft, was genau mit diesen Daten geschieht. Deshalb sollte man auf jeden Fall vor dem Download einer App die Berechtigungen, die sich eine App einräumen möchte, kontrollieren und beschränken. Hilfreich ist hier auch ein Blick auf die App-Bewertungen in Foren von anderen Nutzern.

Funktionen wie **GPS, WLAN** oder **Bluetooth** sind nützlich, stellen aber u. U. auch Sicherheitsrisiken dar: Über GPS kann ein Smartphone-Besitzer leicht „getrackt" d. h. sein Aufenthaltsort ausfindig gemacht werden. Daten, die über ein unverschlüsseltes, öffentliches WLAN-Netzwerk gesendet werden, können von Dritten abgegriffen werden. Mittels Bluetooth können andere Geräte aus der Umgebung auf das eigene Gerät zugreifen, sofern dieses nicht geschützt und bspw. verschlüsselt ist. Aus diesem Grund sollten diese Funktionen deaktiviert werden, wenn man sie gerade nicht benötigt.

Wer eine **Cloud** benutzt um Daten abzuspeichern, muss sich bewusst sein, dass diese nur schwer sicher geschützt werden können. Sensible Daten sollten daher besser nicht dort gespeichert werden. Wichtig bei **Cloud-Computing** ist ein guter Passwortschutz. Ein Passwort sollte ausreichend lang sein und auch Sonderzeichen umfassen.

Sicherheits-Tipp
Die IMEI immer notieren! IMEI steht für ***International Mobile Equipment Identity*** *und ist eine international gültige Kennung mobiler Geräte. Das bedeutet, jedes Smartphone hat eine eindeutige IMEI. Um die IMEI anzuzeigen, muss die Tastenkombination *#06# gewählt werden. Zudem findet sich die IMEI hinter dem Geräte-Akku und wird oft auch beim Kauf des Geräts auf der Rechnung angegeben. Im Falle eines Diebstahls sollte diese Nummer der Polizei unbedingt weitergeben werden!*

Endnoten

[1] MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.) (2015). JIM-Studie 2015, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland. Aufgerufen am 05.01.2016 unter http://www.mpfs.de/fileadmin/JIM-pdf15/JIM_2015.pdf

[2] ebd.

[3] TELECLICK (2005, 26. Dezember). *What is the True Meaning of Wi-Fi?* Aufgerufen am 05.03.2015 unter http://www.teleclick.ca/2005/12/what-is-the-true-meaning-of-wi-fi/

[4] SPIEGEL.DE (2013, 15. Juni). Ballon-Projekt: *Google testet fliegende Internetverbindung.* Aufgerufen am 05.03.2015 unter http://www.spiegel.de/netzwelt/web/project-loon-google-testet-internetzugang-aus-ballons-a-905917.html

[5] MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.) (2015). *JIM-Studie 2015, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland.* Aufgerufen am 01.12.2015 unter http://www.mpfs.de/fileadmin/JIM-pdf15/JIM_2015.pdf

[6] S. 30, ebd.

[7] JARSKI, R. (2008). *Dim Wit: The Funniest, Stupidest Things Ever Said.* London: Random House. (S. 314)

[8] FOCUS.DE (2011, 25. Oktober). *Historische Erfindung: Das Telefon ist 150 Jahre alt.* Aufgerufen am 05.03.2015 unter http://www.focus.de/digital/handy/tid-23991/historische-erfindung-das-telefon-ist-150-jahre-alt_aid_677652.html

[9] SAGER, I. (2012, 29. Juni). *Before iPhone and Android came Simon, the first Smartphone.* Aufgerufen am 05.03.2015 unter http://www.businessweek.com/articles/2012-06-29/before-iphone-and-android-came-simon-the-first-smartphone

[10] BITKOM (2013, 9. September). *Smartphones – Neuer Rekord bei Smartphones.* Aufgerufen am 05.03.2015 unter http://www.bitkom.org/de/presse/78284_77345.aspx

[11] MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.) (2015). *JIM-Studie 2015, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland* (S.46). Aufgerufen am 05.01.2016 unter http://www.mpfs.de/fileadmin/JIM-pdf15/JIM_2015.pdf

[12] ebd.

[13] MÜLLER, C. (2011, 18. November). *Multifunktionswerkzeug – 50 Funktionen, die Ihr Smartphone erfüllt* (Abs. 5). Aufgerufen am 14.10.2014 unter http://karrierebibel.de/mutlifunktionswerkzeug-50-funktionen-die-ihr-smartphone-erfullt/

[14] DÖRING, N. (2006). Handy-Kids: Wozu brauchen sie das Mobiltelefon? In U. Dittler & M. Hoyer (Hrsg.), *Machen Computer Kinder dumm? Wirkung interaktiver, digitaler Medien auf Kinder und Jugendliche aus medienpsychologischer und mediendidaktischer Sicht* (S. XX-YY). München: KoPaed Verlag.

[15] MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.) (2015). *JIM-Studie 2015, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland.* Aufgerufen am 05.01.2016 unter http://www.mpfs.de/fileadmin/JIM-pdf15/JIM_2015.pdf

[16] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (Hrsg.) (BSI). (2011). *Überblickspapier – Smartphones* (S. 2 ff). Aufgerufen am 14.10.2014 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Smartphone_pdf

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Der Klassen-Handy-Check**	**Du und dein Smartphone: Ständige Kontrolle garantiert!**
Kompetenzen	Die Schülerinnen und Schüler führen eine Umfrage zur Handynutzung durch, werten die Ergebnisse aus und beurteilen sie im Vergleich mit repräsentativen Daten der JIM- und KIM-Studien.	Die Schülerinnen und Schüler formulieren anhand eines Erklärvideos grundlegende – problematische – Funktionen eines Handys.
Methoden	Umfrage durchführen, statistische Auswertung, Internet-Recherche	Video-Analyse, Internet-Recherche, Gruppen-Puzzle
Material	Arbeitsblatt	Online-Video, Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Der Klassen-Handy-Check	Die Schülerinnen und Schüler sollen in Form einer internen Klassen-Umfrage ihre eigene Handy-Nutzung im Vergleich mit anderen reflektieren. Lassen Sie den Klassen-Handy-Check anonym ausfüllen und anschließend auswerten. Die Fragen können Sie per Stichwort an die Tafel bringen und die Ergebnisse von 2-3 Schülerinnen/Schülern kurz auszählen lassen, so dass es relativ schnell ein Ergebnis gibt. Wichtig ist der darauffolgende Schritt der Beschreibung, Analyse und Bewertung, für den Sie sich Zeit nehmen sollten. Interessant ist auch der Vergleich der Klassen-Daten mit den für Deutschland repräsentativen Studien JIM und KIM und die Frage, ob das Klassen-Ergebnis typisch ist für Jugendliche. **Arbeitsaufträge:** **1.** Bitte führt den Klassen-Handy-Check durch! **2.** Erstellt eine Auswertung an der Tafel! **3.** Was kann man erkennen? Wie nutzt ihr eure Handys? Fasst die Ergebnisse – zunächst jeder für sich alleine – in Form von einigen kurzen Sätzen (sog. „Thesen") zusammen! **4.** Bitte vergleicht eure Ergebnisse mit Hilfe der Studien **JIM** und **KIM** (nachzulesen unter **www.mpfs.de**) und klärt die Frage, ob eure Klasse typisch ist für alle Kinder/Jugendlichen in Deutschland. **Zu Frage 11 des Fragebogens:** Wenn Sie mit Ihren Schülern das Handyfasten ausprobieren wollen, finden Sie auf der Webseite **www.handysektor.de** eine Anleitung.
AB 2: Du und dein Smartphone: Ständige Kontrolle garantiert!	Mit diesem Arbeitsblatt sollen sich die Schülerinnen und Schüler problematische Aspekte von Handys erarbeiten, die auf den ersten Blick für viele Anwendungen nützlich sind, wie Funkzellen, WLAN und GPS. Sie beinhalten aber auch Datenschutz-Aspekte, wie Handyortung oder die Übermittlung des Standortes o.ä. über die Jugendliche informiert sein sollten. Sie können hier gruppenteilig in fünf Gruppen (A bis E) arbeiten lassen und später in Form eines Gruppenpuzzles (jeweils ein Gruppenmitglied aus A, B, C, D und E) die Ergebnisse zusammenführen. Diese Methode erfordert eine gleiche Anzahl von Gruppenmitgliedern, die nicht immer vorhanden ist. Sie können hier mit „Joker" arbeiten, d. h. „überzählige" Schülerinnen/Schüler dürfen sich eine Gruppe auswählen, wo es dann eine doppelte Besetzung eines Themas während des Gruppenpuzzles gibt.

Lust auf mehr?

1. Auf den Seiten von Handysektor finden sich zahlreiche andere Erklärvideos zu Handy-Themen, die man in gleicher Weise erarbeiten lassen kann: **www.handysektor.de**
2. Wie wird die Entwicklung von Handys weitergehen? Die Schülerinnen und Schüler stellen sich die Welt in 20 Jahren vor und beschreiben sie z. B. in einem Zeitungsbericht über die Handynutzung im Jahr 2022.

Der Klassen-Handy-Check

Macht eure eigene Umfrage. Der Fragebogen wird zunächst von jedem einzelnen anonym ausgefüllt, die Auswertung für eure gesamte Klasse (oder Schule) erfolgt dann im Klassenverband an der Tafel o. ä. Danach seid ihr alle eingeladen zu diskutieren: Was fällt euch auf? Seid ihr überrascht?

Womit hättet ihr nicht gerechnet? Was findet ihr gut? Findet ihr etwas beängstigend? An welchen Punkten gibt es große Übereinstimmungen in eurer Klasse? An welchen Punkten gibt es große Unterschiede? Habt ihr von nun an Vorsätze in Bezug auf euer Handyverhalten? etc.

1. Wie viele Stunden nutzt du dein Handy am Tag im Durchschnitt?

☐ 0–0,5 Std. ☐ 0,5–1 Std. ☐ 1–2 Std. ☐ 2–3 Std. ☐ länger

2. Wofür nutzt du dein Handy hauptsächlich? (5 Kreuze möglich)

☐ Informationen (z. B. Wetter/ Bahn) abrufen
☐ Videos anschauen
☐ Games spielen
☐ Fotos machen
☐ Filme machen
☐ Wecker nutzen
☐ Social Communitys nutzen
☐ Im Internet surfen
☐ Musik hören
☐ Nachrichten schicken
☐ angerufen werden
☐ anrufen

3. Sprichst du oder schreibst du mehr mit deinen Freunden per Handy?

☐ sprechen ☐ schreiben

4. Wie viele Stunden am Tag bist du mit deinem Handy online?

☐ 0–0,5 Std. ☐ 0,5–1 Std. ☐ 1–2 Std. ☐ 2–3 Std. ☐ länger

5. Wie viele Apps hast du?

☐ 0–10 ☐ 10–25 ☐ 25–50 ☐ 50–70 ☐ mehr als 70

6. Welche Apps verwendest du am häufigsten?

❶ .....

❷ .....

❸ .....

7. Würdest du das Handy gerne (mehr) im Unterricht verwenden?

☐ ja ☐ nein

8. Wer bezahlt deine Rechnung?

☐ Ich ☐ Meine Eltern ☐ Ich teile die Rechnung mit meinen Eltern ☐ Andere

9. Wie hoch ist deine Rechnung monatlich im Durchschnitt?

☐ 0–20 Euro ☐ 20–40 Euro ☐ 40–60 Euro ☐ höher als 60 Euro ☐ Weiß nicht

10. In welchen Situationen kannst du auf keinen Fall auf dein Handy verzichten? (nenne 1–3 Situationen)

❶ .....

❷ .....

❸ .....

11. Würdest du an einem Experiment teilnehmen, bei dem du eine Woche lang ohne dein Handy leben müsstest?

☐ ja ☐ nein

Quelle: http://www.handysektor.de/fileadmin/user_upload/bilder/basisthemen/Paedagogenecke/HS-Unterrichtseinheiten/Klassen-Handycheck_klicksafe.pdf

Du und dein Smartphone: Ständige Kontrolle garantiert!

Bitte schaue dir folgendes Video an: **„Handysektor erklärt: Was ist eigentlich ein Bewegungsprofil?"** Hier werden drei technische Systeme erläutert, **Funkzellen, WLAN** und **GPS**, mittels derer der Standort eines Smartphones ermittelt werden kann.

Quelle: Video zu finden unter: http://www.handysektor.de/navigation-paedagogen/paedagogenecke/videos.html

Arbeitsaufträge:

1. Habt ihr alle Fachbegriffe verstanden? Bitte recherchiert folgende Begriffe und erläutert sie kurz, aber genau! Ihr dürft euch dazu in fünf Gruppen (A bis E) aufteilen:

1. Smartphone (im Unterschied zu einem „Handy")	
2. Funkzelle mit Funkmasten	
3. Netzanbieter	
4. WLAN	
5. GPS	

2. Erläutert diese Begriffe in Form eines Kurz-Referates den anderen!

3. Bleibt in euren Gruppen A bis E und beantwortet zunächst innerhalb der Gruppen folgende Fragen.

Gruppe A	Gruppe B	Gruppe C	Gruppe D	Gruppe E
Wieso ist jeder mit Smartphone unter „ständiger Beobachtung"?	Was ist im Film mit dem „Fingerabdruck" gemeint??	Was genau ist ein „Bewegungsprofil"?	Wie nutzen Apps die Standort-Daten von Funkzelle, WLAN und GPS?	Was ist an einem Bewegungsprofil so problematisch?

4. Setzt euch in Form eines Gruppen-Puzzles (mit jeweils einem Vertreter von A bis E) in neuen Gruppen zusammen. Beantwortet der Reihe nach eure Fragen und erläutertet eure Beispiele!

5. Wie kann die Geschichte von den Protagonisten des Films, Tom, Lisa und Tina weitergehen? Bleibt in den neuen Gruppen und – wer kann – gestaltet dazu eine Fotostory oder ein kurzes Erklär-Video (ähnlich dem von **Handysektor**).

Wer noch Zeit und Lust hat: Die Geschichte der Mobiltelefonie ist inzwischen eine lange und dabei sehr spannende! Erstellt einen Zeitstrahl auf einem Plakat und ergänzt ihn um wichtige Daten und Entwicklungen (vlt. auch mit Bildern?). Anregungen findet ihr hier:
www.handysektor.de/geraete-technik/detailansicht/article/happy-birthday-40-jahre-handy.html

Was wir lieben: Mobiles Internet, Kommunikation und Spiele
3_1 Mobiles Internet und Smartphones
3_2 Apps
3_3 WhatsApp und Co
3_4 Skype
3_5 Computerspiele

Apps

Was sind Apps?

App ist die Kurzform des englischen Begriffs „Application". Apps sind kleine Anwendungen, die auf ein Smartphone heruntergeladen werden können – wie Programme, die auf einen Computer aufgespielt werden. Auf einem Smartphone sind zwar bereits viele Standard-Programme vorinstalliert, jedoch stehen dem Nutzer viele weitere, mehr oder weniger nützliche Apps zum Download zur Verfügung. Diese finden sich in den sog. **App Stores**. Die Firma **Apple** eröffnete 2008 kurz nach der Markteinführung des **iPhones** den dazugehörigen **Apple App Store** und war damit der Erste auf dem Markt. In kurzer Folge wurden danach weitere App Stores für andere Betriebssysteme eröffnet: Für Android gibt es den **Google Play Store,** für Blackberry die **Blackberry World,** für Nokia, den **Nokia Store,** für Windows den **Windows Phone Store** etc. In diesen Stores können Apps bezogen werden, die Software-Entwickler kostenlos oder zum Verkauf anbieten. Eine App kostet dort durchschnittlich zwischen 1 und 4 Euro.

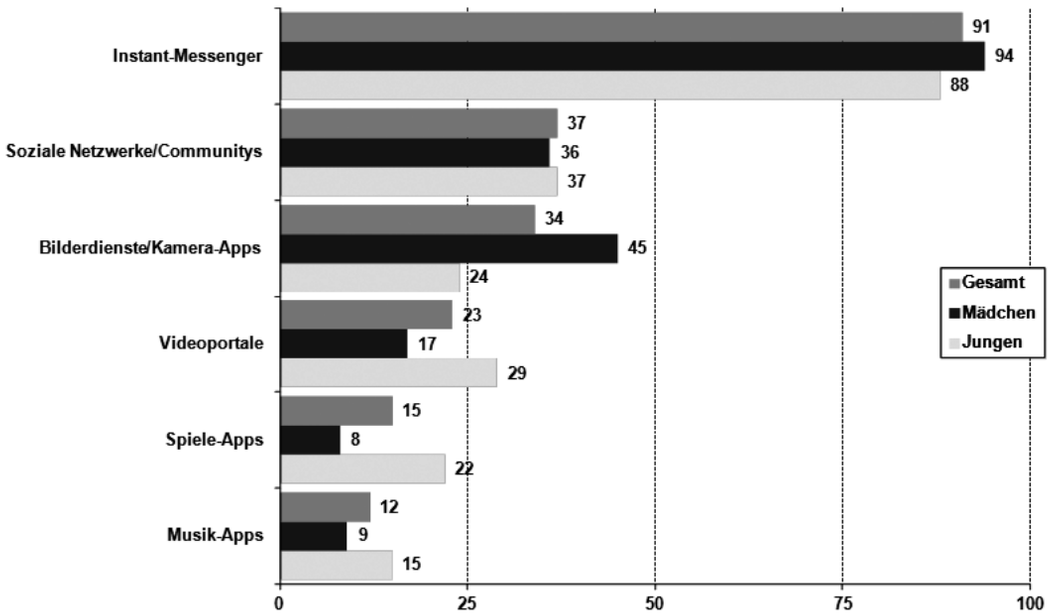
Apps – eine Goldgrube

In den USA war „App" nicht ohne Grund das Wort des Jahres 2010[1], denn das Geschäft mit den kleinen Programmen boomt weltweit. In Deutschland wurden 2012 1,7 Milliarden mobile Apps heruntergeladen; 2014 wird wohl die 3-Milliarden-Grenze überschritten. Zum Vergleich: 2010 waren es nur knapp 400 Millionen[2]. Alleine im App Store von **Apple** gaben die Nutzer 2013 rund 10 Milliarden US-Dollar aus[3]!

Beliebte Apps

Wenig überraschend gehören laut der **Jugend, Information, (Multi-)Media**-Studie (JIM-Studie) 2015 **WhatsApp** und die **Facebook-App** zu den beliebtesten Anwendungen der Jugendlichen:

Die wichtigsten Apps auf dem Smartphone* 2015
– bis zu drei Nennungen –



Quelle: MPFS (2015). JIM 2015, Angaben in Prozent. Basis: Befragte, die Apps auf dem handy installiert haben. n=1.044[4]

In allen Altersgruppen der App-Nutzer werden die sog. **Casual Games** immer beliebter. Unter den **Casual Games** sind Spiele-Apps zu verstehen, die einfach „zwischendurch" z. B. auf dem Weg zur Schule/Arbeit, beim Warten auf den Bus gespielt werden können. Sie sind recht intuitiv und erlauben daher einen schnellen Einstieg in das Spielvergnügen[5]. **Quizduell** ist eine solche App und erfreute sich 2014 in Deutschland einer großen Beliebtheit. Das Prinzip der App ist so einfach wie eingängig: Ähnlich wie bei **Wer wird Millionär?** erhält der Spieler Fragen zu verschiedenen Themenbereichen und muss aus verschiedenen Antwortmöglichkeiten die Richtige auswählen. Der Clou ist, dass der Spieler gegen andere Spieler antreten kann – gegen Bekannte ebenso wie gegen Fremde. Damit verbindet **Quizduell** das Casual Gaming mit dem Element des **Social Gaming,** also mit dem Spielen mit anderen. Gut möglich, dass in dieser Kombination das Erfolgsrezept begründet liegt, denn **Quizduell** wurde bis Mai 2014 10 Millionen Mal heruntergeladen – alleine in Deutschland[6].

Gibt es dafür nicht eine App?

In den App Stores steht ein breites Spektrum tausender unterschiedlicher Apps zum Download bereit. Augenscheinlich existiert für jede Lebenssituation eine App, ganz zu schweigen von den unzähligen Apps, die weniger sinnhaft, als vielmehr unterhaltsam sind: So gibt es eine **Bier-App,** die das Display in ein Bierglas verwandelt, dessen Füllhöhe beim Kippen des Smartphones beständig zurückgeht. Oder die **Sternenkarte-App**, die – hält man das Smartphone gen Himmel – die Sterne und Planeten anzeigt, die man sieht bzw. sehen könnte. Im Trend liegen derzeit Apps, die Körperfunktionen erfassen, auswerten und daraus individuelle Tipps generieren, um z. B. die Fitness oder den Schlaf zu verbessern oder die Ernährung gesünder zu gestalten. Diesen Trend nennt man **Quantified Self,** also das Bestreben, eigene Körperfunktionen mittels Apps und ggf. notwendiger Zusatzgeräte in Zahlen zu fassen und auszuwerten. Problematisch ist hier, dass diese sehr privaten Daten an die Server der Anbieter überspielt werden. Das alleine ist bereits kritisch. Man stelle sich nun aber vor, diese Daten gelangen in die Hände von Dritten, die an diesen Daten größtes Interesse haben: Im Falle der Daten über die körperliche Fitness wären das bspw. die Krankenkassen, die auf dieser Basis dann darüber entscheiden, wer zugelassen wird und wer lieber nicht. Noch ist das Zukunftsmusik – fragt sich jedoch, wie lange noch.

Apps und der Datenschutz

Auf einem Smartphone sind viele, teils sehr persönliche Daten gespeichert: Fotos, Videos, Kontakte, Nachrichten, Dokumente etc. Außerdem gibt ein Gerät in angeschaltetem Zustand viele Daten nach „außen", wie z. B. GPS, WLAN Schnittstelle, IP-Adresse etc. Einige Apps benötigen für ihr Funktionieren den Zugriff auf diese Daten, wie bspw. die Navigation über **Google Maps.** Andere Apps sind schlicht neugierig und verlangen Zugriff auf Daten oder Funktionen, die sie nicht benötigen, um zu funktionieren. Ein Beispiel ist die **Brightest Flashlight-App.** Diese fordert von den Nutzern die Berechtigung, u. a. auf ihren Standort zugreifen zu dürfen. Für den Nutzer ist oft unübersichtlich, welche App auf welche Daten zugreift. Ausgewählte Apps wie bspw. **Clueful Privacy Advisor** oder **SRT AppGuard** können diesbezüglich Abhilfe schaffen. Außerdem werden die Berechtigungen, die eine App einfordert, vor dem Download angezeigt.

Aus der Praxis

*Unter SchülerInnen ist der **App-Check** sehr beliebt: Zuerst werden Kriterien für den Check entwickelt. Dann werden diese auf die eigenen Lieblings-Apps angewendet. Bei dieser Aktivität kann man besonders gut die Diskussion um den Datenschutz anbringen, indem man die Frage erörtert, weshalb einige Apps (scheinbar) kostenlos zum Download angeboten werden. Wie verdienen diese Anbieter dennoch Geld?*

Die größten Herausforderungen bei Apps:

- **Datenschutzrisiken:** Einige Apps greifen auf viele Daten zu. Dieses Wissen über die Nutzer lässt sich gezielt für personalisierte Werbung einsetzen.
- **Unkontrollierter Datentransfer:** Für die Nutzer ist die Menge der gesendeten und empfangenen Daten kaum nachvollziehbar. Wer keine Internet-Flatrate besitzt, kann bei der monatlichen Smartphone-Rechnung böse überrascht werden.
- **Werbung & Abzocke:** Viele Apps sind kostenlos zu erwerben, wobei der Nutzer aber Werbeeinblendungen in Kauf nimmt. Tippt man auf Werbeeinblendungen unseriöser Anbieter, hat man schnell ein kostenpflichtiges Abo „abgeschlossen". Problematisch sind auch die sog. **In-App-Käufe** wie sie bei Spiele-Apps häufiger vorkommen: Apps sind allem Anschein nach kostenlos, bieten dann aber im Spiel mehr oder weniger offensichtlich die Möglichkeit z. B. gegen Bezahlung zusätzliche Funktionen freizuschalten.
- **Schadsoftware:** Da Smartphones nur handliche Computer sind, sind auch sie anfällig für Schadsoftware, die der Nutzer unbewusst oder von ihm unbemerkt auf sein Smartphone lädt, bzw. auf dieses geladen wird.
- **Akkuverbrauch:** Einige Apps sind in Betrieb wahre Stromfresser. Entsprechend oft muss das Smartphone an den Strom angeschlossen werden.
- **Speicherplatz:** Einige benötigen viel Speicherplatz. Dadurch wird das Smartphone u. U. sehr langsam.

Das **Bundesamt für Sicherheit in der Informationstechnik** (BSI) hat einige grundlegende Tipps für den sicheren Umgang mit Apps zusammengestellt[7]:

- *Nur aus vertrauenswürdigen Quellen (d. h. den offiziellen App Stores) installieren*
- *Vorsicht bei Schnäppchen*
- *Zugriffsrechte der Apps vor dem Download bzw. auf dem Smartphone kontrollieren*
- *Updates überprüfen und kontrollieren*
- *Statusmeldungen bei Gebrauch im Blick behalten*
- *Kontrollieren, welche App wann läuft*
- *Apps löschen, wenn sie nicht benötigt werden*

Endnoten

[1] SUEDDEUTSCHE.DE (2011, 11. Januar). *US-Wort des Jahres. App-laus, App-laus, App-laus.* Aufgerufen am 19.03.2015 unter http://www.sueddeutsche.de/digital/us-wort-des-jahres-app-laus-app-laus-app-laus-1.1044849

[2] STATISTA (2014, Mai). *Anzahl der Downloads mobiler Apps in Deutschland in den Jahren 2009 bis 2012 und Prognose für 2014* (in Millionen). Aufgerufen am 15.10.2014 unter http://de.statista.com/statistik/daten/studie/168038/umfrage/anzahl-der-downloads-mobiler-apps-in-deutschland-seit-2009/

[3] APPLE (2014, 7. Januar). *App Store Sales Top $10 Billion in 2013.* Aufgerufen am 15.10.2014 unter https://www.apple.com/pr/library/2014/01/07App Store-Sales-Top-10-Billion-in-2013.html

[4] MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.) (2015). JIM-Studie 2015, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland. Aufgerufen am 01.12.2015 unter http://www.mpfs.de/fileadmin/JIM-pdf15/JIM_2015.pdf

[5] ROLAND BERGER STRATEGY CONSULTANTS (2012, 28. September). *„Casual Gaming": Der Markt für Online-Gelegenheitsspiele wird in den nächsten Jahren weltweit wachsen.* Aufgerufen am 15.10.2014 unter http://www.rolandberger.de/pressemitteilungen/512-press_archive2012_sc_content/Casual_Gaming.html

[6] ULPTS, K. (2014, 28. Februar). *Faszination Quizduell: Warum es alle spielen. noz.de.* Aufgerufen am 20.10.2014 unter http://www.noz.de/deutschland-welt/gut-zu-wissen/artikel/454994/faszination-quizduell-warum-es-alle-spielen

[7] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI) (Hrsg.) (2015, März). *Basisschutz Apps.* Aufgerufen am 19.03.2015 unter https://www.bsi-fuer-buerger.de/BSIFB/DE/MobileSicherheit/BasisschutzApps/basisschutzApps_node.html

Arbeitsblatt	**AB 1**	**AB 2**
Titel	**Apps für jeden und alles!**	**Der App-Check für Fortgeschrittene**
Kompetenzen	Die Schülerinnen und Schüler beschreiben mit eigenen Beispielen die grundlegenden Funktionen von Handys im Alltag Heranwachsender	Die Schülerinnen und Schüler werten anhand eines vorgegeben „App-Checks" einzelne Apps aus und vergleichen die Ergebnisse miteinander.
Methoden	Internetrecherche	App-Check
Material	Arbeitsblatt	Arbeitsblatt, eigenes Handy
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Apps für jeden und alles!	Die Schülerinnen und Schüler sollen sich in einem ersten Schritt gegenseitig ihre Lieblings-Apps zeigen und dies begründen. Hier wird es sicherlich viele Überschneidungen geben, was ein Indiz dafür sein kann, dass die Handy-Nutzung auch starken Peer-Gruppen-Prozessen ausgesetzt ist bzw. davon bestimmt wird. In einem zweiten Schritt sollen sie die Funktionen von Handys kennenlernen und App-Beispiele dafür finden. Zum Schluss steht die Frage nach der Finanzierung, die im Einzelfall ohne tiefere Recherche nicht einfach zu beantworten ist. Grundsätzlich kann man unterscheiden zwischen „Bezahlung mit Werbung" oder „Bezahlung in der Währung Daten".
AB 2: Der App-Check für Fortgeschrittene	Die Schülerinnen und Schüler sollen mit Hilfe des „App-Checks" eine App analysieren im Hinblick auf Datensicherheit, Werbung, Berechtigungen. Auf dem Arbeitsblatt finden sich bereits technische Hinweise. Viele Funktionen sind gut im Internet zu finden und müssen für die Betriebssysteme und Modelle immer aktuell recherchiert werden, sind aber integriert (wie die Darstellung des Energieverbrauchs oder des Speicherbedarfs der App). Der anschließende Vergleich dient der Präsentation der Ergebnisse und nicht einem qualitativen Vergleich der Apps, der die Schülerinnen und Schüler für die genannten Problematiken sensibilisieren soll. Die Aufgaben h-j eignen sich auch als Hausaufgabe.

Lust auf mehr?

- In modernen Smartphones verstecken sich noch viele andere Funktionen, die missbraucht werden können, z. B. durch sogenannte „Spy-Apps", die unbemerkt Kamera oder Mikrofon aktivieren. Hier lohnt es sich, interessierte Schülerinnen und Schüler etwas tiefer eintauchen zu lassen.
- Ein Trend der Zukunft, oder eher der Gegenwart, wird als das „Internet der Dinge" bezeichnet. Darunter versteht man die Vernetzung von z. B. Haushaltsgeräten und Autos mit dem Internet, gesteuert über Apps auf dem Smartphone. Ein Arbeitsblatt dazu finden Sie auf:
  www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Ethik/Zusatz_AB_Internet_der_Dinge.pdf, Lösungen dazu im Bereich
  www.klicksafe.de/themen/medienethik/privatsphaere-und-big-data/

Apps für jeden und alles!

Es gibt eine **Biertrinker-App** und eine **Schlafüberwachungs-App** oder auch die **Helium-Stimme-App** und zahllose andere **mehr** oder **weniger sinnvolle Apps** für das Smartphone. Sicherlich hast du selbst viele Apps installiert und nutzt sie intensiv. Hier darfst du Beispiele für Apps finden und diese nach wissenschaftlichen Aspekten sortieren.

Arbeitsaufträge:

1. Bildet Gruppen von max. vier SchülerInnen. Stellt euch gegenseitig eure drei Lieblings-Apps vor und erklärt, warum ihr sie mögt/häufig benutzt! Gebt euch dann einen Gruppen-Namen, der etwas mit euren Lieblings-Apps zu tun hat!
2. Bitte findet Beispiel-Apps für folgende Funktionen, die Wissenschaftler zusammengestellt haben. Erklärt die Beispiele!

Funktion mit Erläuterung	Beispiel-App
Sicherheit, Freunde und Eltern benachrichtigen zu können.	
Organisation des Alltags: Zum Vereinbaren von Abholdiensten mit den Eltern bis hin zu Kontakten zu Freunden und Bekannten.	
Beziehung/Kommunikation mit Freunden und Freundinnen. Das Handy kann als **Schaltzentrale** des sozialen Netzwerkes verstanden werden.	
Identität. Das Handy wird dazu genutzt, sich selbst nach außen darzustellen..	
Unterhaltung durch die Nutzung von Video/Audio und Spielen.	
Information mittels Apps, die Informationen bereitstellen.	
Transaktion wie der Kauf von Kinokarten, Fahrkarten u.v.a.	
Sozialisation durch Fotos von FreundInnen, deren Weitergabe, Social Communities.	
Empowerment mit Anwendungen, die eine Erweiterung eigener Fähigkeiten bedeuten, bspw. Unterstützung körperlich eingeschränkter Kinder und Jugendlicher.	

Quelle: Verändert nach: Nicola Döring: „Handy-Kids: Wozu brauchen sie das Mobiltelefon" (2006)

3. Mit Apps lässt sich ein großes Geschäft machen. Recherchiert in der Gruppe wie sich kostenlose Apps finanzieren.

App-Alarm *Du bist dir nicht sicher, ob die App, die du dir herunterladen möchtest, wirklich sicher ist? Dann lasse die App vom Handysektor-Team testen und löse den App-Alarm aus! Auf* ***www.handysektor.de/apps-upps/app-alarm.html***

Der App-Check für Fortgeschrittene!

Apps sind eine tolle Sache, keine Frage. Nicht wenige haben auf ihrem Handy über 100 der kleinen (oder auch großen) Programme installiert. Hier kannst du mit deinen Mitschülerinnen und Mitschülern einen App-Check machen und ein echter App-Profi werden. Solltest du keines haben (oder es vergessen haben), dann dürft ihr zu zweit zusammenarbeiten!

Arbeitsaufträge:

1. Bitte ergänze im Folgenden zunächst die Angaben, die auf dich zutreffen:

Ich bin... ☐ ein Junge ☐ ein Mädchen:	Ich bin ..... Jahre alt	Ich habe: insg. ..... Apps installiert (Anzahl)	Meine drei Lieblings-Apps sind: 1..... 2..... 3.....

2. Wähle nun eine deiner Lieblings-Apps aus. **Name d. App:** .....

3. Nun wird es etwas technisch und vielleicht auch etwas schwierig. Es kann sein, dass du zu einigen der Fragen im Internet recherchieren musst. Versuche trotzdem, folgende Fragen möglichst genau zu beantworten:

   a) Ist diese App kostenlos? Wenn nein, wie teuer ist sie? Wenn ja, wird Werbung eingeblendet?

   b) Wenn Werbung eingeblendet wird? Wann und wo erscheint Werbung?

   c) Welche Werbung wird eingeblendet? (2-3 Beispiele)

   d) Welche Berechtigungen (z.B. Zugriff auf Kamera, Mikrofon, Fotos, Kontakte, Ortungsfunktion) verlangt diese App? In folgendem Video erfährst du, was eine App-Berechtigung ist:
   https://www.youtube.com/watch?v=E59crV5Auv0

   e) Welche Daten (z.B. Standort, Kontakte) gibt die App weiter?

   f) Gibt es sog. **In-App-Käufe**? D.h. kann man bspw. Zusatzfunktionen freischalten, wenn man Geld zahlt?

   g) Wenn ja, was genau kann ich kaufen und wie teuer ist es?

   Zusatzaufgaben für Technikbegeisterte:

   h) Wie hoch ist der Datentransfer? (Das ist nicht ganz einfach zu messen, ist aber möglich!)

   i) Verbraucht diese App viel Akku-Leistung? Macht dazu ein kleines Experiment!

   j) Wie viel Speicherplatz benötigt diese App auf meinem Handy?

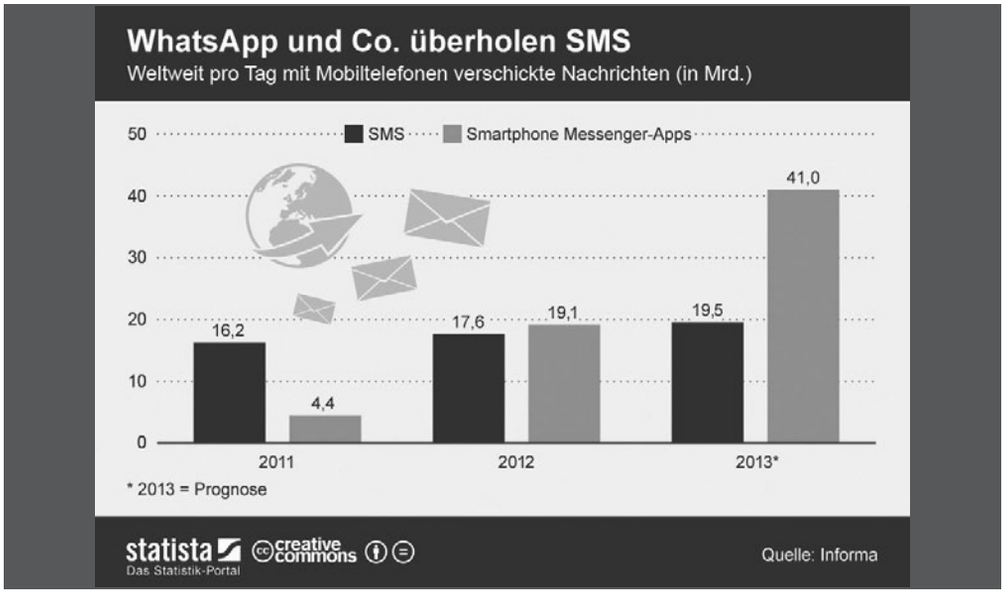
4. Schülerinnen und Schüler, die gleiche oder ähnliche Apps haben, finden sich nun in kleinen Gruppen (max.5 Personen) zusammen. Tauscht eure Ergebnisse aus und vergleicht sie miteinander.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt folgende Tipps:

- *Nur aus vertrauenswürdigen Quellen installieren/Vorsicht bei Schnäppchen*
- *Rechtevergabe der Apps innerhalb des Handys (Zugriff auf bspw. die Ortungsfunktion, Mikrofon etc.) kontrollieren*
- *Updates überprüfen und kontrollieren*
- *Statusmeldungen bei Gebrauch im Blick behalten/Kontrollieren, welche App wann läuft*
- *Apps bei Nicht-Gebrauch wieder löschen*

Von der SMS zu WhatsApp

Von der SMS zu WhatsApp
In der Zeit vor WhatsApp wurden Textnachrichten an Freunde und Bekannte fast ausschließlich über den **Short Message Service** (SMS) versendet. Eine Nachricht war begrenzt auf max. 160 Zeichen und das Versenden kostete je nach Anbieter einen Festbetrag von einigen Cent. 2009 kam dann der Instant-Messaging-Dienst **WhatsApp** auf den Markt und begann seinen steilen Aufstieg. Schon drei Jahre später wurden über Messenger-Dienste wie **WhatsApp** mehr Kurznachrichten versendet als SMS. Seit 2014 gehört WhatsApp dem US-amerikanischen Unternehmen Facebook Inc.



Quelle: Brandt (2013)[1]

WhatsApp ist eine Messenger-App, die für internetfähige Mobiltelefone ausgelegt ist und es den Nutzern ermöglicht, über verschiedene Betriebssysteme (z. B. für iPhone, Blackberry, Windows Phone, Android, etc.) hinweg, miteinander zu kommunizieren. Der Name ist ein Kofferwort aus dem englischen Ausdruck „What's up?" („Was ist los?"/„Was geht?") und „App" von dem englischen Wort „Application". Der Versand von WhatsApp-Nachrichten erfolgt über eine Internetverbindung. Neben Textnachrichten können auch Bilder, Video- und Audiodateien sowie Kontakte und der eigene Standort versendet werden. Eine beliebte Funktion von WhatsApp ist die Möglichkeit, Gruppen einzurichten. In diese Gruppen kann der Ersteller der Gruppe Personen einladen. Jede Nachricht, die in die Gruppe gepostet wird, geht automatisch an alle Gruppenmitglieder. WhatsApp ist derzeit im ersten Jahr kostenlos, ab dem zweiten Jahr wird eine Jahresgebühr von einem knappen Euro erhoben[2]. Im Frühjahr 2015 wurde den WhatsApp-Nutzern auch das internetbasierte Telefonieren möglich gemacht.

Datenschutz
In der Vergangenheit wurde WhatsApp immer wieder aufgrund gravierender Sicherheitsmängel kritisiert. So steht WhatsApp auch weiterhin v. a. aufgrund der Weitergabe von Namen und Telefonnummern in der öffentlichen Kritik. Datenschützer bemängeln, dass bei der Nutzung der App das vollständige Adressbuch des Nutzers an den amerikanischen Server weitergeleitet wird. Problematisch ist v. a., dass es sich dabei nicht nur um die eigenen Daten, sondern auch um die Daten von Personen handelt, die den WhatsApp-Messenger womöglich nicht einmal besitzen. WhatsApp verlangt aber nicht nur den Zugriff auf das Telefonbuch, sondern auch auf Standortdaten, Nachrichten oder Konten. Kritisch ist außerdem, dass die Nutzungsbedingungen von WhatsApp bislang nur auf Englisch verfügbar sind. Nutzer, die der englischen Sprache nicht oder nicht ausreichend mächtig sind, haben keine Möglichkeit, die Richtlinien, denen sie zustimmen sollen, überhaupt zu verstehen.

Wie kann man seine Daten schützen?
Wenn man WhatsApp nutzt, muss man sich im Klaren darüber sein, dass die Anwendung auf viele Daten der Nutzer zugreift: Standort, Kontakte, Bilder, Konten etc. Wirksam schützen kann man sich davor leider nicht, denn WhatsApp verlangt diese Berechtigungen, wenn man die App nutzen möchte. Es ist daher zu überlegen, ob man nicht auf alternative Dienste, wie **Threema, Telegram** etc. (s. u.) zurückgreift.

Aus der Praxis
*Das Thema **„WhatsApp"** eignet sich gut für **Peer-Education.** Medienscouts des Elsa-Brändström-Gymnasiums in Oberhausen veranstalten in allen 5. Klassen einen Parcours mit Stationen, an denen über verschiedene Aspekte von WhatsApp informiert wird. Diese Veranstaltung findet bei den (Klassen-) Lehrern, den Schüler und auch den Eltern großen Zuspruch.*

Ungewollte Kontaktaufnahme
Es ist nur möglich, mit einer Person über WhatsApp Kontakt aufzunehmen, wenn man über deren Mobilfunknummer verfügt. In der Regel betrifft das diejenigen Kontakte, die sich auch im eigenen Adressbuch wiederfinden. Es kann allerdings auch der Fall sein, dass eine dem Nutzer unbekannte Person den Kontakt aufnimmt. Das ist bspw. dann möglich, wenn die eigene Mobilfunknummer einer größeren Öffentlichkeit zugänglich ist, da sie z. B. in Sozialen Netzwerken eingestellt wurde.

Hinzufügen & Blockieren
Bei Erhalt einer Nachricht von einer unbekannten Nummer, erscheinen im Chatfenster die Schaltflächen „hinzufügen" und „blockieren". Klickt man auf „blockieren", erhält man von dem unbekannten Kontakt keine weiteren WhatsApp-Nachrichten mehr. Außerdem kann die blockierte Person nicht einsehen, wann man zuletzt online war oder ob man gerade online ist. Ebenso wenig werden der unbekannten Person Änderungen am eigenen Profil angezeigt. Gibt man einen Kontakt wieder frei, empfängt man keine Nachrichten, die dieser in der Zeit seiner Blockierung gesendet hat.

Es gibt jedoch zwei wichtige Dinge, die durch das Blockieren nicht verhindert werden können:

- Der Status ist weiterhin für die blockierte Person sichtbar, sofern die eigene Nummer unter ihren WhatsApp-Favoriten auftaucht.
- Durch das Blockieren entfernt man den Kontakt weder von seiner WhatsApp-Liste, noch entfernt man die eigene Nummer von dessen Liste. Um einen Kontakt aus der eigenen WhatsApp Liste zu löschen, muss man diesen aus dem Adressbuch löschen.

Problem mit Cyber-Mobbing
Junge WhatsApp-Nutzer nutzen die Anwendung nicht nur zum positiven Austausch untereinander. Immer öfter wird unter Jugendlichen auch über WhatsApp gemobbt. Mobbing findet - den Einträgen in Hilfeforen nach zu urteilen – v. a. über WhatsApp Gruppen statt. Es wird nicht nur per Text beleidigt, verletzt oder ausgegrenzt, sondern ebenfalls mit Bildern, Audiodateien oder Videos. WhatsApp ist deshalb problematisch, weil man einen Täter nicht „melden" kann und dieser somit keine Sanktionen seitens des Anbieters befürchten muss (s. auch: Kapitel **Cyber-Mobbing**).

Alternativen zu WhatsApp
Es gibt zahlreiche Alternativen zu WhatsApp, die ähnliche Funktionen bieten. Die folgende Auflistung ist nur eine beispielhafte Auswahl und Beschreibung und nicht vollständig. Unter dem Thema „WhatsApp" auf der klicksafe-Webseite finden sich weitere Alternativen:

- **Threema** bietet eine Ende-zu-Ende-Verschlüsselung und die Möglichkeit die Kontaktdaten gegenseitig per QR-Codes auszutauschen.
- **Telegram** bietet eine besondere Funktion: Man kann sich selbst löschende Nachrichten schicken und die Nachrichten so einstellen, dass der Chat-Partner vor dem Lesen einen Code zur Identifizierung eintippen muss.
- **Surespot** hat sich dem Datenschutz verschrieben und bietet einen starken Verschlüsselungsstandard und eine Lösch-Funktion, die auf dem eigenen Handy und ebenso auf dem Empfänger-Handy ausgelöst wird.
- **Viber** bietet neben den Text-Nachrichten auch die Möglichkeit (kostenlos über das Internet) zu Telefonieren, hat aber auch kaum Sicherheitseinstellungen.
- **Skype** ist bekannt als Anwendung zur Video-Telefonie, kann aber auch zum Chatten verwendet werden.

Links und weiterführende Informationen

Webseiten

www.klicksafe.de/themen/kommunizieren/whatsapp/
Im Themenbereich finden sich viele Informationen rund um WhatsApp u. v. m.

Endnoten

[1] BRANDT, M. (2013, 21. Juni). *WhatsApp und Co. überholen SMS.* Aufgerufen am 20.10.2014 unter http://de.statista.com/infografik/1085/weltweit-pro-tag-mit-mobiltelefonen-verschickte-nachrichten/

[2] WHATSAPP.COM (2014). Wie viel kostet das WhatsApp Abo? Aufgerufen am 19.03.2015 unter http://www.whatsapp.com/faq/de/general/23014681

Arbeitsblatt	**AB 1**	**AB 2**
Titel	**WhatsApp-Stress**	**WhatsApp mal ganz genau!**
Kompetenzen	Die Schülerinnen und Schüler erkennen die Probleme bei der Nutzung von WhatsApp anhand eines kurzen Erklärvideos und übertragen diese auf eigene Beispiele.	Die Schülerinnen und Schüler setzen Erkenntnisse über WhatsApp um indem sie an Stationen eigene Formen der Präsentation entwickeln.
Methoden	Video-Analyse, Blitzlicht	Tabelle, Stationenlernen (eigentl. Lernzirkel)
Material	Arbeitsblatt	Arbeitsblatt, eigenes Handy
Zeit (in Minuten)	90	90 (evtl. 135)
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: WhatsApp-Stress	Mit diesem Arbeitsblatt sollen die Schülerinnen und Schüler die problematischen Seiten von WhatsApp erkennen und mit eigenen Beispielen darstellen. Das Erklärvideo von Handysektor ist sehr anschaulich und auch für jüngere Schülerinnen und Schüler gut zu verstehen. Das Blitzlicht zu Beginn dient einer ersten Einschätzung/Stellungnahme, die – wie immer bei der Methode Blitzlicht – unkommentiert stehen gelassen werden sollte. Wenn die Schülerinnen und Schüler selbst (intensiv) WhatsApp nutzen, finden sie gewiss leicht Beispiele für eigene – ähnliche – Situationen. Sollten Sie Schülerinnen/Schüler haben, die kein Smartphone besitzen oder WhatsApp nicht nutzen, bilden Sie Teams mit einem „Experten"/einer „Expertin".
AB 2: WhatsApp mal ganz genau!	Die Schülerinnen und Schüler sollen sich zunächst nach Interesse auf eine der sechs Stationen (Themen s. Arbeitsblatt) in etwa gleicher Anzahl aufteilen (wobei eventuell nicht jedes Interesse berücksichtigt werden kann). Die Internet-Quellen sind relativ offen angegeben und dienen auch dem Üben einer Internet-Recherche. Hier müssen Sie ggf. etwas Hilfestellung geben. Insbesondere die letzte Station „Klassen-Chat" kann nicht recherchiert, sondern sollte im Gespräch innerhalb der Gruppe erarbeitet werden. Das Stationenlernen (eigentlich die Methode „Lernzirkel", da ALLE Stationen besucht werden müssen) dient der Präsentation und dem Austausch. Hier können Sie die kooperative Methode „one-stay-three-stray" benutzen. Darin verbleibt im Wechsel jeweils ein Schüler der Gruppe als Gastgeber bei der eigenen Station, die anderen (hier drei) gehen als Gäste zu anderen Stationen.

Lust auf mehr?
Regeln für einen Klassen-Chat beinhalten die Fragen nach einem respektvollen Umgang miteinander. Hier könnte man einen Werte-Diskurs anschließen, der viele Bereiche des Miteinanders und nicht nur die mediale Kommunikation einbezieht.

klicksafe hat unter dem Stichwort „Medienethik" Informationen dazu:
http://www.klicksafe.de/themen/medienethik/

WhatsApp-Stress

Wahrscheinlich benutzt du auf deinem Smartphone **WhatsApp,** um damit mit deinen FreundInnen zu schreiben. Vielleicht hat deine Klasse auch eine eigene WhatsApp-Gruppe, in der ihr euch oft Nachrichten postet. Erkennst du dich in dem folgenden Video über Lisa wieder?

Quelle: Video zu finden bei Handysektor unter: www.handysektor.de/navigation-paedagogen/paedagogenecke/videos.html

Arbeitsaufträge:

1. Bitte schaut euch gemeinsam in der Klasse den Erklärfilm, „WhatsApp-Stress" von **Handysektor** an.

2. Führt direkt danach ein sog. **Blitzlicht** durch, bei dem jeder kurz das sagen darf, was ihm zu dem Film aufgefallen ist!

3. Ergeht es euch wie Lisa? Erklärt – zunächst in Partnerarbeit – folgende Szenen aus dem Film und belegt sie mit eigenen Beispielen!
   - a) Lisa ist glücklich mit WhatsApp.
   - b) Lisa tritt dem Klassen-Gruppen-Chat bei.
   - c) Im Klassen-Chat gibt es zahlreiche Nachrichten.
   - d) In der Nacht schaut Lisa auf ihr Smartphone.
   - e) Alle anderen sehen, wann sie online ist.
   - f) Das Smartphone lenkt Lisa vom Lernen ab.
   - g) Im Straßenverkehr passt Lisa nicht auf.
   - h) Beim gemeinsamen Essen sitzt jeder mit seinem Smartphone, statt sich zu unterhalten
   - i) Lisa erhält eine Nachricht von Tom, obwohl er neben ihr sitzt.
   - j) Lisa hat eine Gruppe „stumm" geschaltet (wie geht das?).
   - k) Lisa hat die Funktion „zuletzt online" ausgeschaltet (wie geht das?).
   - l) Das Smartphone schaltet sie nachts aus.

4. Redet in der Klasse über eure Erlebnisse mit WhatsApp. Schreibt an die Tafel, was gut und was problematisch ist an WhatsApp!

5. Wie möchtest du WhatsApp nutzen? Finde – wiederum zunächst in Partnerarbeit – vier Regeln, die in der Klassen-WhatsApp-Gruppe gelten sollen. Diskutiert die Vorschläge mit allen und einigt euch – wenn möglich – auf Regeln, die ihr in Form eines „Vertrages" auf einem Plakat festhalten und von allen unterschreiben lassen solltet!

WhatsApp mal ganz genau!

Seid ihr WhatsApp-Profis?
Hier dürft ihr zeigen, wie gut ihr euch wirklich mit dieser App auskennt!

Arbeitsaufträge:

1. Bitte sucht euch eines der folgenden Themen 1–6 aus. Bildet Gruppen von max. 4 SchülerInnen (ihr dürft die Themen auch doppelt besetzen, aber jedes Thema muss erarbeitet werden!).
2. Erarbeitet das Thema in Form einer „Station", bei der ihr anderen das Thema in maximal 5 Minuten erklären könnt. Sicherlich müsst ihr einiges recherchieren. Z. B. auf **www.klicksafe.de/apps** und auf **www.handysektor.de.** Ihr dürft dazu Material suchen, Zeichnungen/Bilder erstellen oder verwenden oder auch Fragekärtchen oder ein Quiz machen oder ähnliches.
   Ihr dürft hier kreativ und witzig sein!
3. Benutzt danach folgenden **„Laufzettel"** und besucht alle anderen Stationen, wechselt euch dabei in der eigenen Station so ab, so dass sie immer besetzt ist.

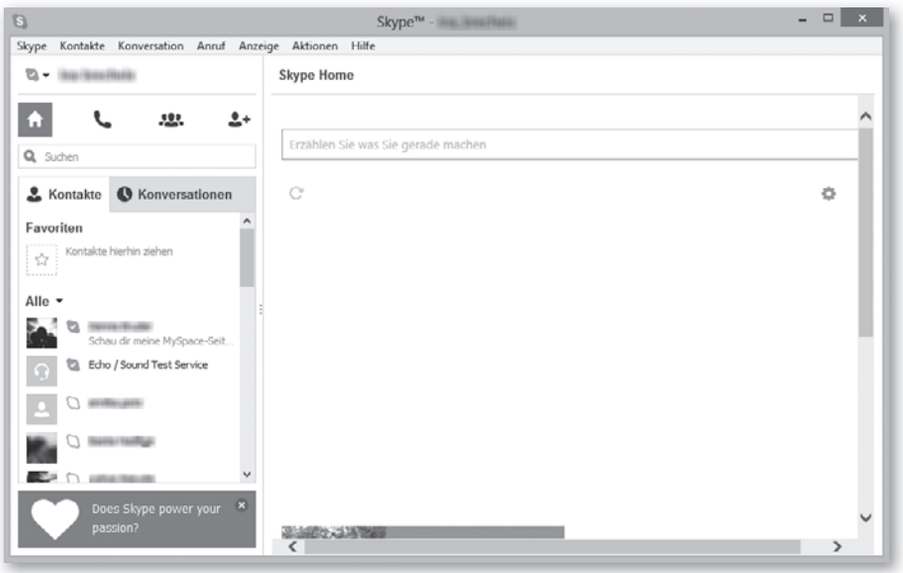
Laufzettel

Station	Leitfrage(n)	Notizen
1. Stress?!	Wann kann WhatsApp Stress bedeuten? Wie viele Nachrichten sind für mich o. k.? Wie kann ich Stress durch WhatsApp vermeiden?	
2. Datenschutz und WhatsApp	Was erfährt WhatsApp über mich? Welche Berechtigungen hat die App? Auf welche Daten greift WhatsApp zu? Wie kann ich meine Daten schützen?	
3. Die Firma WhatsApp	Was ist WhatsApp eigentlich? Womit verdient die Firma ihr Geld? Wann wurde sie gegründet? Wem gehört sie?	
4. Kettenbriefe und Sinnloses	Was wird Unsinniges geplaudert? Was ist wichtig und was ist unwichtig? Wie funktionieren Kettenbriefe?	
5. Erreichbarkeit?	Wann will ich für wen erreichbar sein? Und wann nicht? Wann kann ich WhatsApp mal ausschalten? oder wie kann ich es stummschalten?	
6. Klassen-Chat	So will ich behandelt werden! Regeln im Klassen-Chat	

Skype

Zahlen und Fakten

2002 entstand die Idee, eine Software für internetbasierte Telefonie zu entwickeln. Der ursprüngliche Name der Software war **Skyper** eine Abkürzung von „Sky peer-to-peer". Im August 2003 war dann die erste Version der **Skype**-Software öffentlich verfügbar. Skype wechselte in den letzten Jahren mehrmals den Besitzer, bevor 2011 **Microsoft** vorerst letzter Besitzer des Unternehmens wurde. 2013 verzeichnete Skype rund 660 Millionen Nutzer weltweit[1]. Jeden Tag wird über Skype 2 Milliarden Minuten gechattet und telefoniert[2]. Der Dienst ist so populär, dass er nicht nur in die deutsche Sprache Eingang gefunden hat: Das Verb **„skypen"** ist mittlerweile ein gängiges Wort, das lange nicht mehr nur für Skype selbst verwendet wird.



Quelle: eigener Screenshot Skype Benutzeroberfläche; Stand: 23.10.2014

Das Geschäftsmodell

Die Standard-Nutzung des Dienstes ist kostenlos. Für Zusatzdienste wie bspw.

- Anruf auf Handy oder Festnetz
- SMS
- Gruppen-Video-Gespräche
- Werbefreiheit etc.

werden Gebühren erhoben.

Die Funktionen

Die Internettelefonie nutzt die gleiche Technik zur Datenübertragung wie das Surfen im Internet: Sprache und ggf. Videobild werden in Datenpakete verpackt und über das Internet versendet. Aus diesem Grund schwankt die Datenübertragung mit der Qualität der Internetverbindung. Die Ein- und Ausgabe der Sprache erfolgt am Laptop/PC bestenfalls über ein sog. „Headset". Ein Headset ist eine Kombination aus Kopfhörer und Mikrofon. Die Bilder liefert eine Kamera, die bei Laptops/Smartphones integriert ist oder die als Zusatzgerät an PCs angeschlossen werden kann.

Skype-Teilnehmer erhalten keine Rufnummer, sondern wählen einen Benutzernamen, der an die zukünftigen Gesprächspartner weitergeben werden muss. Nach dem Start des Programms wird in der Kontaktliste auf der linken Seite angezeigt, wer gerade online erreichbar ist.

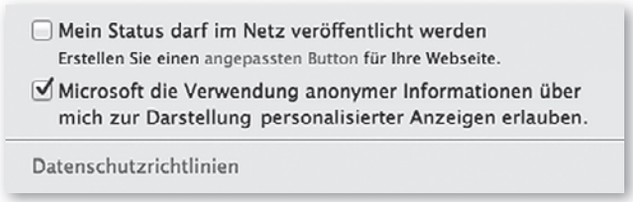
Skypen bietet vielfältige Möglichkeiten. Dazu gehören:

- Sprachtelefonie
- Gruppenanrufe (max. 25 Teilnehmer)
- Videoanrufe: Einzelvideoanrufe, Gruppenvideoanrufe
- Videonachrichten
- SMS (auch als Gruppen-SMS)
- Sprachnachrichten
- Versenden von Dateien, Bildschirminhalten oder auch Kontaktlisten

Aus der Praxis
*Das Thema **„Skype"** spielt im Schulalltag üblicherweise keine große Rolle, dabei kann es im Unterricht durchaus reizvoll eingesetzt werden: Erstaunlich viele Experten, Zeitzeugen oder Prominente sind bereit, sich für eine halbe Stunde den Fragen von SchülerInnen zu stellen, da sie das mittels **Skype** bequem von zu Hause aus tun können. Einfach mal anfragen!*
Ebenso interessant kann es sein, einen Schüler/eine Schülerin zu sprechen, der/die gerade für ein Jahr im Ausland weilt.
***Wichtig:** Beim Skypen in der Schule vorher die Technik ausprobieren!*

Datenschutz und Spionagevorwürfe
Wenn man Skype nutzt, d. h. Nachrichten versendet, telefoniert etc., werden Daten durch Skype ausgelesen. Meldet man sich bei dem Dienst an, räumt man Skype das Recht ein, auf Daten zuzugreifen. Hier ein Auszug aus den Allgemeinen Geschäftsbedingungen:

„Skype nutzt gegebenenfalls innerhalb von Sofortnachrichten und SMS automatisiertes Scannen zur Bestimmung von (a) vermutlichem Spam und/oder (b) URLs, die bereits als Spam-, Betrugs- oder Phishing-Links identifiziert wurden (…)."[3]



Quelle: eigener Screenshot Skype Datenschutzrichtlinien; Stand: 14.10.2014

Problematisch ist auch die Skype-Version, die in China zum Einsatz kommt. Dort existiert der Dienst **TOM-Skype**[4]**.** Dieser ermöglicht staatlichen Behörden eine Suche nach Schlüsselbegriffen und damit eine Kontrolle der Skype-Kommunikation. Neben diesen Spitzelvorwürfen muss auch ganz generell darauf hingewiesen werden, dass trotz der Verschlüsselungstechnik, die Skype verwendet, Gespräche nicht abhörgeschützt sind. Aus diesem Grund stellt eine Studie des **Fraunhofer-Institut** für **Eingebettete Systeme und Kommunikationstechnik** (ESK) aus München im November 2013 fest: „Die Nutzung von Skype wird […] derzeit nicht empfohlen!"[5] (S. 19).

Endnoten

[1] TAGESSCHAU.DE (2013, 23. April). *Wie ein Gratis-Dienst Milliarden brachte.* Aufgerufen am 21.10.2014 unter http://www.tagesschau.de/wirtschaft/skype116.html

[2] Ebd.

[3] MICROSOFT.COM (2014, März). *Datenschutzerklärung von Skype: Sonstige Informationen* (Abs. 7). Abgerufen am 19.03.2015 unter https://www.microsoft.com/privacystatement/de-de/skype/default.aspx#accessingPersonalData

[4] HEISE.DE. (2008, 2. Oktober). *Skype in China filtert und speichert politische Mitteilungen.* Aufgerufen am 21.10.2014 unter http://www.heise.de/newsticker/meldung/Skype-in-China-filtert-und-speichert-politische-Mitteilungen-209292.html

[5] MESSERER, T. & Eickhoff, B. (2013). *Einsatz von Skype in Unternehmen. Chancen, Risiken und Policy-Empfehlungen* (S. 19). Fraunhofer ESK. Aufgerufen am 21.10.2014 unter http://www.esk.fraunhofer.de/content/dam/esk/de/documents/Skype_im-Unternehmen.pdf

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Chatregeln – kennst du welche?**	**Skypen – praktisch und doch problematisch!**
Kompetenzen	Die Schülerinnen und Schüler übertragen die Chat-Regeln durch eine Zuordnungs-Übung und übertragen sie auf Erfahrungen.	Die Schülerinnen und Schüler erklären Funktionen der Software Skype anhand einer Internet-Recherche und beurteilen die Datenschutzrichtlinien des Unternehmens.
Methoden	Zuordnungs-Übung, Gesprächskreis	Tabelle, Partnerarbeit
Material	Arbeitsblatt	Arbeitsblatt, Skype Zugänge
Zeit (in Minuten)	45	90
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Chatregeln – kennst du welche?

Hier sollen die Schülerinnen und Schüler die Chat-Regeln zum sicheren Chatten kennen lernen. Dies geschieht spielerisch in Form eines Textpuzzles. Ob Sie den letzten Arbeitsauftrag tatsächlich durchführen wollen und können, bleibt Ihnen überlassen. Aber das Thema „Chatten" ist wichtig und kann schlimme Folgen, gerade für Jüngere, haben, so dass man an das Chatten heranführen sollte – allerdings in sicheren, moderierten Chatrooms. Diese Chatrooms, hier die Beispiele des SWR und ZDF, verlangen aus bekannten Gründen eine kurze Anmeldung, die evtl. mit den Eltern abgesprochen werden sollte. Wenn Sie die Aufgabe als Hausaufgabe geben, weisen Sie ausdrücklich darauf hin, dass die Eltern informiert sein müssen.

Lösung Textpuzzle
Chat-Tipps für Kinder – Sicher Chatten!

1. Chatte am Anfang nicht allein!
   Frag deine Eltern…
2. Such dir einen kleinen Chat, in dem jemand aufpasst!
   Die Aufpasser (Moderatoren) achten darauf, dass…
3. Geh nicht in Chats für Erwachsene!
   Oft werden dort unangenehme Sachen geschrieben…
4. Denk dir einen guten Spitznamen aus!
   Der Nickname sollte reine Fantasie sein: z. B. …
5. Verrate nie deine Adresse, Telefonnummer und deinen Nachnamen.
   Janine (12 Jahre) hat erlebt, was dann passieren kann: …
6. Sei freundlich, aber bleib auch misstrauisch!
   Verhalte dich so freundlich, wie du auch im richtigen Leben bist…
7. Triff dich nicht mit Leuten aus dem Chat!
   Man kann nie wissen, wer sich dahinter versteckt. …

Quelle: Broschüre: Chatten ohne Risiko? Zwischen fettem Grinsen und Cybersex; www.jugendschutz.net

Hinweise für die Durchführung

AB 2: Skypen – praktisch und doch problematisch!

Den Schülerinnen und Schülern ist das „Skypen" sicherlich geläufig. Die vielen zusätzlichen Funktionen, die Skype bietet, sind wahrscheinlich aber nicht allen bekannt. Die Schülerinnen und Schüler können hier die Software etwas genauer kennenlernen, vor allem unter dem technischen und finanziellen Aspekt (was kostet diese Funktion?). Ein Impuls dahingehend, wieso die Grundfunktionen kostenlos sein können, hilft vielleicht beim Einstieg in das Thema.
Hilfen: **www.skype.com/de/features/**
Wie so oft spielt das Thema Datenschutz eine große Rolle. Hier sollen die Schülerinnen und Schüler dafür sensibilisiert werden, indem sie sich die Datenschutzrichtlinien (ein anspruchsvoller Lesestoff) genauer anschauen. Als kleine Motivationshilfe dient vielleicht der Hinweis, dass JEDER, der bereits Skype nutzt, diesen Datenschutzrichtlinien zugestimmt hat, also auch zumindest ein Teil Ihrer Schülerinnen und Schüler! Die Aufteilung und Partnerarbeit in einzelne Punkte der Richtlinien soll die große Aufgabe handhabbar machen. Vielleicht achten Sie auf eine gleichmäßige Verteilung im Umfang.

Lust auf mehr?

- Zur Weiterarbeit bietet sich eine Dokumentation der Ergebnisse in Form eines Plakates, Merkzettels oder einer Info-Broschüre an. Vielleicht können Sie sogar eine Chateinführung für eine andere, jüngere Klasse veranstalten lassen.

  Auf der Seite **http://www.chatten-ohne-risiko.net/** gibt es einen Lehrerbereich mit Unterrichtsmaterialien sowie einen „Chat Atlas" zur Gefahreneinschätzung aktueller Chats, Messengers und Sozialer Netzwerke.
- WhatsApp bietet mit Whats App calls ebenfalls Telefonie über Messenger. Lassen Sie die SuS hier zu Vorteilen aber auch Problemen recherchieren. Sammlung in einer Mindmap +/–

Chatregeln – kennst du welche? (1/2)

Wenn du dich mit deinen Freunden triffst, machst du das vielleicht bei dir zu Hause in deinem Zimmer. Auch im Internet kannst du dich mit anderen treffen: In einem so genannten „Chat". Um zu chatten, musst du dir also zunächst einen Chatroom suchen. Im Internet gibt es viele Seiten, auf denen du chatten kannst.

„(to) chat" [tschet] ist das englische Wort für plaudern oder schwatzen, „room" [ruum] heißt Raum.
*In **Chatrooms** geht es um unterschiedliche Themen wie zum Beispiel Sport oder Tiere! Zum Chatten brauchst du einen Nickname (= Spitznamen), den können die anderen Kinder auf ihrem Bildschirm auch sehen.*

Nun brauchst du nur noch einen Nicknamen und los geht's!

… **Aber Vorsicht!!!**

Arbeitsaufträge

1. Ordne die Tipps und die Beispiele auf der Folgeseite einander zu und schreibe die passende Zahl in das vorgesehene Feld. Vergleicht eure Anordnung in der Klasse!

2. Ist dir schon einmal etwas Ähnliches passiert? Rede im Sitzkreis mit deinen Klassenkameraden darüber!

3. Weißt du, warum die einzelnen Regeln wichtig sind? Findet zu zweit weitere Beispiele und spielt sie der Klasse vor!

4. Hier findest du Chats für Kinder:

   www.kindernetz.de/netztreff

   www.tivi.de/tivi/tivitreff/rubrik/01057

Tipp:
Probiere die Chat-Tipps doch selbst mal aus. Klebe das Blatt gut sichtbar an deinen Computerbildschirm!

!!! Bei ihnen musst du dich vorher anmelden!
Also frage erst deine Eltern, ob du es überhaupt darfst!

Chatregeln – kennst du welche? (2/2)

Hier noch ein paar Tipps, damit dir das Chatten auch Spaß macht.
Ups … die Tipps und die Beispiele dazu sind durcheinander geraten.

Chat-Tipps für Kinder – Sicher Chatten!

1 Chatte am Anfang nicht allein!

Man kann nie wissen, wer sich dahinter versteckt. Darauf ist Cora (11 Jahre) reingefallen: „Ich habe mich mit einem Mädchen aus dem Chat verabredet, das Pferde auch sehr liebte. Es kam aber ein Junge, der schon über 20 war. Zum Glück war meine Mutter dabei. Ich rate allen: Dass sie sich nie mit jemandem treffen, den sie aus dem Chat kennen. Das ist ein großer FEHLER."

2 Suche dir einen kleinen Chat, in dem jemand aufpasst!

Verhalte dich so freundlich, wie du auch im richtigen Leben bist. Aber glaube nicht alles, was jemand im Chat über sich erzählt. Das ist manchmal geflunkert.

3 Geh nicht in Chats für Erwachsene!

Janine (12 Jahre) hat erlebt, was dann passieren kann: „Ich habe jemandem gesagt, wie ich heiße und in welchem Ort ich wohne! Er wohnte auch dort und fragte mich immer: „Wo wohnst du genau?" Ich habe ihm aber nichts gesagt. Ich hatte ziemliche Angst, dass er plötzlich vor der Tür steht."

4 Denke dir einen guten Spitznamen aus!

Der Nickname (=Spitzname) sollte reine Fantasie sein: z. B. ein Name aus deinem Lieblingsbuch, Lieblingsfilm oder ein lustiges Wort. Dein richtiger Name ist dein Geheimnis.

5 Verrate nie deine Adresse, Telefonnummer und deinen Nachnamen.

Die Aufpasser (Moderatoren) achten darauf, dass alle freundlich sind. Sie helfen dir, wenn du nicht zurechtkommst.

6 Sei freundlich, aber bleib auch misstrauisch!

Oft werden dort unangenehme Sachen geschrieben. Katrin (14 Jahre) hat Folgendes erlebt: „Einmal hat einer mich mit blöde Kuh und Nutte beschimpft. Da bin ich sofort aus dem Chat. Und obwohl ich schon 14 bin, gehe ich lieber in Kinder-Chats, weil ich dort nie dumm angemacht werde."

7 Triff dich nicht mit Leuten aus dem Chat!

Frag deine Eltern oder älteren Geschwister, ob sie dir helfen.

Skypen – praktisch und doch problematisch!

Das **„Skypen"**, also das Telefonieren mit Videoübertragung über das Internet ist wirklich eine praktische Erfindung und wird überdies kostenlos angeboten! Es gibt allerdings einige Firmen, die ihren Mitarbeitern das **„Skypen"** verbieten. Sie haben Bedenken, dass sie so leicht ausspioniert und abgehört werden können.

Arbeitsaufträge:

1. Nutzt du selbst Skype? Berichte in der Klasse von deinen Erfahrungen damit.

2. Unten findest du eine Tabelle mit Funktionen, die die Software „Skype" von Microsoft bietet. Bitte recherchiert in Partnerarbeit und erklärt jede Funktion kurz. Findet dabei heraus, ob die Funktion kostenlos ist oder wie viel sie kostet!

a) Anrufe an andere Skype-Nutzer	b) Anrufe auf Handy oder Festnetz	c) Gruppen-Anrufe	d) Eigene Skype-Nummer
e) Skype-to-go	f) Click-to-call-Anrufe	g) Einzel-Video-Anrufe	h) Gruppen-Video-Anrufe
i) SMS senden	j) Sprach-Nachrichten	k) Video-Nachrichten	l) Anrufe weiterleiten
m) Sofort-Nachrichten	n) Rufnummern-Anzeige	o) Kontakt-Übertragung	p) Gruppen-Bildschirm-Übertragung
q) Group-Me	r) Datei-Übertragung	s) Bildschirm-Übertragung	

3. Die Kritik an Skype richtet sich vor allem gegen die mangelnde Datensicherheit bei der Übertragung. Recherchiert in Partnerarbeit zu diesem Problem und stellt kurz dar, mit welcher Begründung einige Firmen Skype verbieten.

4. Auch für Privatpersonen kann der Datenschutz bei Skype wichtig sein. So speichert die Software viele Informationen. Unter folgender Adresse stehen die Datenschutzrichtlinien von Skype (in Englisch):

   http://www.skype.com/de/legal/privacy

   Sucht euch in Partnerarbeit bitte daraus zwei Punkte, die ihr besonders wichtig findet. Stellt sie den anderen vor.

Computerspiele

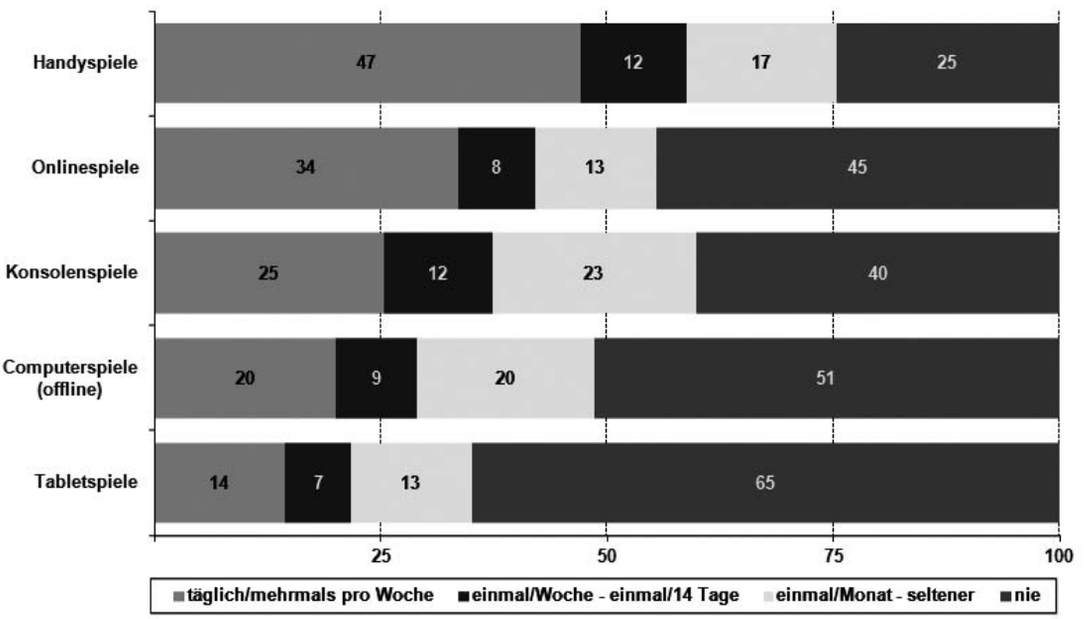
Computerspiele – ein eigenes Universum
Das Thema „Computerspiele" ist facettenreich und wird nicht selten in der medialen Öffentlichkeit heiß diskutiert. Dieses Kapitel bietet einen Überblick der wichtigsten Aspekte zum Thema. Unter dem Begriff „Computerspiele" werden alle Bildschirm-Spiele zusammengefasst:
Das klassische Computer-Spiel (mit PC offline wie online), die Konsolen-Spiele (z. B. X-Box – Microsoft, Playstation – Sony, Wii – Nintendo), die Spiele auf portablen Geräten auch „Handhelds" genannt (Nintendo DS, Gameboy, PSP) und auch die Spiele für das Smartphone.

Computerspiele sind ein milliardenschweres Geschäft. Die deutsche Computerspiele-Branche hat nach Angaben ihres Interessenverbandes, **Bundesverband Interaktive Unterhaltungssoftware** e. V. (BIU), alleine im 1. Halbjahr 2014 einen Umsatz von 798 Milliarden Euro erzielt[1]. Besonders der Markt für mobile Spiele (Spiele-Apps) und Onlinespiele verzeichnet große Zuwachsraten: Wurden im 1. Halbjahr 2013 nur 49 Millionen Euro mit Spiele-Apps und In-App-Käufen umgesetzt, waren es im 1. Halbjahr 2014 bereits 114 Millionen. Das entspricht einem Zuwachs von 133 %[2].

Faszination: Computerspiele

Computerspiele und ihre jugendlichen Nutzer
Die Studie **Jugend, Information, (Multi-) Media** (JIM-Studie) 2015 unterscheidet zwischen Handyspielen, Onlinespielen, Konsolenspielen und Offline-Computerspielen. 59 % der befragten Jugendlichen spielen täglich/mehrmals pro Woche oder einmal pro Woche am Handy. 42 % spielen online, 37 % an der Konsole und knapp 30 % spielen die klassischen offline Computer-Spiele:

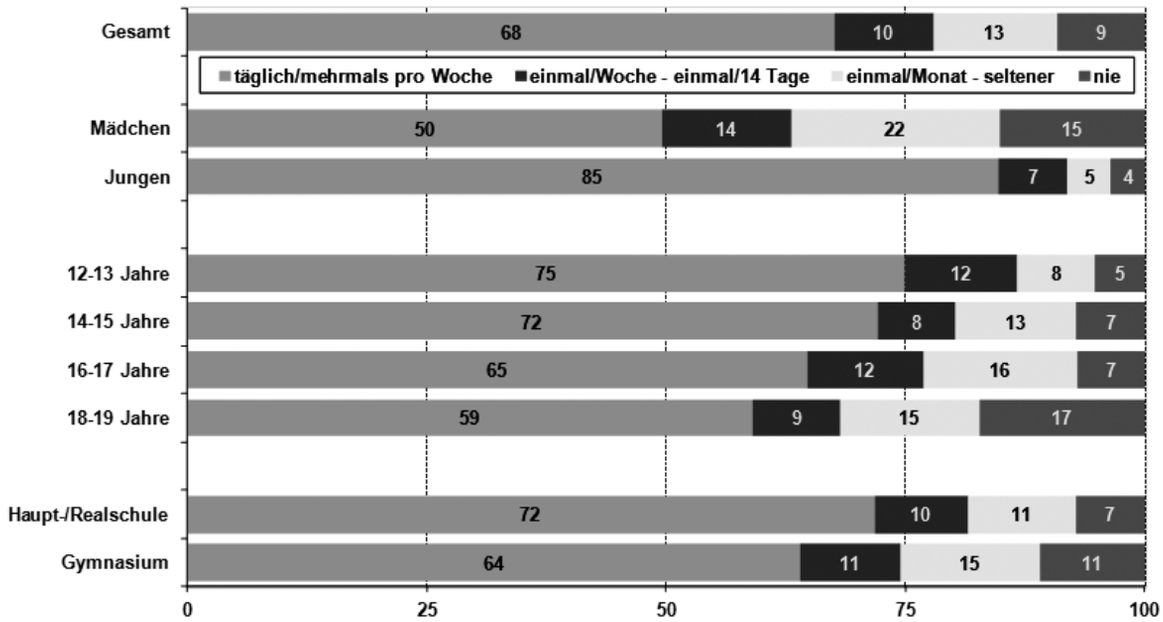
Computer-, Konsolen-, Online-, Tablet- und Handyspiele: Nutzungsfrequenz 2015



Quelle: MPFS (2015). Angaben in Prozent. Basis: alle Befragten, n= 1.200[3]

Während bei der Nutzung anderer digitaler Medien kaum Gender-Unterschiede auszumachen sind, ist das bei Computerspielen anders: 85 % der Jungen spielen täglich/mehrmals pro Woche. Ihre Zahl liegt damit deutlich höher als die der spielenden Mädchen mit 50 %:

Computer-, Konsolen-, Online- und Handyspiele (netto): Nutzungsfrequenz 2015

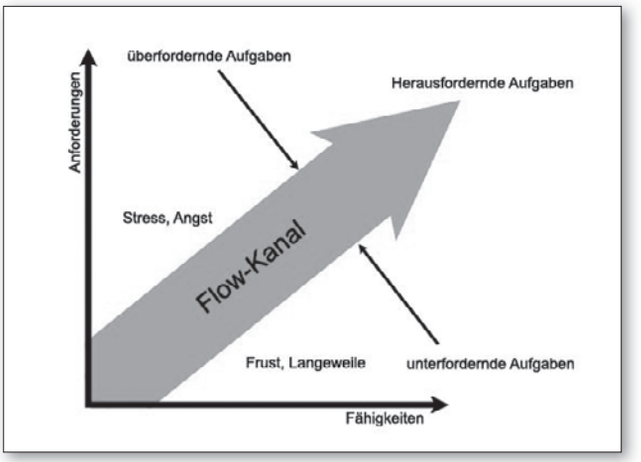


Quelle: MPFS (2015). Angaben in Prozent. Basis: alle Befragten, n= 1.200[4]

Aus der Praxis
Selbstverständlich steht in der Schule die kritische Auseinandersetzung mit Computerspielen im Vordergrund. Nicht minder wichtig ist es aber für den Lehrer, sich auf die Welt der Computerspiele einzulassen. Möglich ist das bspw. in sog. LAN-Partys – Computerspiele-Events – für Lehrer und Eltern.

Computerspiele üben offensichtlich eine große Faszination auf Kinder und Jugendliche aus. Dafür gibt es verschiedene Gründe:

- **Interaktives Erlebnis:** Die Spieler nehmen aktiv gestaltend am Spielverlauf teil, denn ihre Aktionen haben unmittelbare Konsequenzen auf den Spielverlauf.
- **Erfolgserlebnis:** Computerspiele bescheren den Spielenden viele Erfolgserlebnisse. Das Besondere ist, dass die Spieler sich sowohl Spielinhalt als auch den Schwierigkeitsgrad des Spiels selbst wählen. Somit können sie die Spielwelt beherrschen – anders als die reale Lebenswelt.
- **Soziales Erlebnis:** Das Spiel mit und gegen Gleichgesinnte schafft ein Gefühl der Zusammengehörigkeit. Auf dieser Basis entstehen Freundschaften und intime Beziehungen.
- **Flow-Erlebnis:** Ein Flow-Erlebnis bezeichnet einen Zustand der völligen Versunkenheit in eine Tätigkeit, den auch Computerspieler erleben. Voraussetzung für ein solches Erlebnis ist, dass sich überfordernde und unterfordernde Aufgaben die Balance halten, dann ist der sog. **Flow-Kanal** bereitet.[5]



Quelle: klicksafe.de (2015)[6]

Aus der Praxis
Vertretungsstunden können dazu genutzt werden, den Flow-Kanal mit SchülerInnen zu erarbeiten: 30 Minuten dürfen sie nutzen, um auf ihrem Smartphone zu spielen, dann wird 15 Minuten darüber reflektiert.

Genres

In der öffentlichen Diskussion ist oft von „den" Computerspielen die Rede. Das verstellt den Blick darauf, wie vielfältig und unterschiedlich Computerspiele tatsächlich sind. Analog zu Filmen können Computerspiele in verschiedenste Genres unterteilt werden, deren Grenzen mitunter fließend sind[7, 8]:

Actionspiele
Bei diesen Spielen ist Reaktionsschnelligkeit und Geschicklichkeit gefragt, denn das Spielgeschehen ist temporeich. Der Spieler bewegt sich entweder in der **Ich-Perspektive** oder in der **Dritte-Person-Ansicht** durch die Spielwelt und wird ständig vor neue Handlungsmöglichleiten gestellt. Zu Actionspielen gehören auch **Jump & Run** sowie **Shooter** s. u. Beispiele für dieses Genre sind: Tomb Raider, Zelda, Grand Theft Auto u. v. m.

Adventure
Ein klassisches **Adventure** (Abenteuerspiel) ist gekennzeichnet durch eine in sich geschlossene Spielgeschichte, bei welcher der Spieler eine Spielfigur oder abwechselnd verschiedene Figuren durch eine festgelegte Spielgeschichte steuert. Ziel ist es, zumeist ohne Zeitdruck, Rätsel und Aufgaben zu lösen. Im Rahmen dessen müssen Umgebungen erkundet, Gegenstände gesammelt und Gespräche mit Spielcharakteren geführt werden. Beispiele für dieses Genre sind: Skyrim, Oblivion u. v. m.

Denk- und Geschicklichkeitsspiele
Denkspiele und Geschicklichkeitsspiele werden meist in einem Genre zusammengefasst, da die Übergänge recht fließend sind. Bei beiden Formen steht das eigentliche Spielprinzip im Vordergrund, eher weniger eine Geschichte. Bei Denkspielen bestimmen Logik, das Erkennen von Zusammenhängen und Kombinationsgabe über den Spielerfolg, während in Geschicklichkeitsspielen Reaktionsschnelligkeit, feinmotorischen Umgang mit den jeweiligen Eingabegeräten und eine gute Hand-Augen-Koordination gefordert werden. Beispiele für dieses Genre sind: Crazy Machines, Bejeweled u. v. m.

Gesellschaftsspiele
Dieses Genre umfasst grundlegend alle Bildschirmspiele, denen ein Brett-, Karten- oder Würfelspielprinzip als Vorlage dient. Darüber hinaus gehören auch Musikspiele zu diesem Genre. Zentrales Merkmal des Genres ist die Möglichkeit, gemeinsam auf unterhaltsame Weise virtuell spielen zu können. Vertreter dieses Genres sind: Monopoly, Guitar Hero u. v. m.

Lernspiele & Serious Games
Spiele dieses Genres sind durch Anspruch gekennzeichnet, Erziehung, Lernen und Unterhaltung ansprechend miteinander verknüpfen zu wollen. Ziel ist es v. a., die Lernmotivation zu steigern. Vertreter dieses Genres sind: The Migrant Trail, Gone Home u. v. m.

Rennspiele
Spiele dieses Genres sind insbesondere bei männlichen Jugendlichen beliebt. Ziel der Spiele ist es, sich auf einer vordefinierten Strecke mit einem Fahrzeug gegen andere Spieler oder computergesteuerte Gegner durchzusetzen. Die Siegoptionen variieren dabei von Spiel zu Spiel teils stark. Traditionell geht es allerdings darum, ähnlich des realen Rennsports, das Ziel in möglichst kurzer Zeit bzw. vor den Gegnern zu erreichen. Vertreter dieses Genres sind: Burnout Paradise, Need for Speed u. v. m.

Rollenspiele
Spiele dieses Genres sind dadurch gekennzeichnet, dass ein Spieler die Kontrolle über eine heroische Figur (Charakter) oder eine Heldengruppe hat. Zu Beginn ist die Figur in der Regel eher schwach und schlecht ausgestattet. Durch das Erledigen von Aufgaben (sog. Quests) und/oder das Besiegen von Gegnern wird die Heldenfigur zunehmend mächtiger und der Spieler kann bestimmte Fähigkeiten wie z. B. mächtige Zauber oder effektive Kampftechniken erlernen.
Es obliegt oftmals der Entscheidung des jeweiligen Spielers, welchen Held er in der virtuellen Welt verkörpern möchte. Beispiele für dieses Genre sind: Oblivion, Mass Effect 2 u. v. m.

(Ego)Shooter
In diesen Spielen bewegt der Spieler eine menschliche oder menschenähnliche Figur aus der Ich-Perspektive durch ein dargestelltes Szenario. Das Besiegen von Gegnern durch Waffengewalt ist meist eine zentrale Spielaufgabe, wenngleich der Spieler in manchen Genrevertretern möglichst ohne Einsatz von Gewalt verschiedene Aufgaben lösen muss. Beispiele für dieses Genre sind: Counter Strike, Call of Duty u. v. m.

Sportspiele
Spiele dieses Genres simulieren reale und fiktive Sportarten. Ähnlich wie im realen Vorbild gilt es, die eigenen Fähigkeiten zu trainieren und im Wettkampf das eigene Können unter Beweis zu stellen. Kennzeichen des Sports ist der Wettstreit gegen Gleichgesinnte – so ist es kaum verwunderlich, dass die meisten virtuellen Genrevertreter einen Mehrspielermodus anbieten, in dem Kinder und Jugendliche ihr Können unter Beweis stellen können. Vertreter dieses Genres sind: Fifa, Wii Sports u. v. m.

Strategiespiele
In diesem Genre steuert der Spieler keine einzelne Spielfigur. Er ist vielmehr für die Geschicke einer gesamten Fraktion oder eines Volkes verantwortlich. Ihm obliegt dabei unter anderem die Kontrolle über verschiedene Wirkungsbereiche, wie z. B. dem Aufbau einer florierenden Wirtschaft, der Ausdehnung des eigenen Wirkungsbereiches durch Erkundung und Eroberung, das Treffen politischer/diplomatischer Entscheidungen etc. Vertreter dieses Genres sind:
Die Siedler, Anno u. v. m.

Speziell für **Online-Spiele** lassen sich folgende Genres unterscheiden:

Browsergames
Wie der Name bereits verrät, benötigt der Spieler einen Internet-Browser, um spielen zu können. Die Spiele stehen meist direkt auf der Webseite des Anbieters bereit, Software muss zum Spielen nicht auf dem eigenen Rechner installiert werden, das gesamte Spiel wird online gespielt und gespeichert.

Online-Rollenspiele
Online-Rollenspiele oder auch **Massively Multiplayer Online Role-Playing Games** (MMORPGs) genannt, kennzeichnen sich durch ähnliche Handlungsanforderungen wie herkömmliche Computer-Rollenspiele. So muss auch hier eine eigene Spielfigur (Charakter) gestaltet werden, die dann im Spielverlauf an Fähigkeiten und Fertigkeiten hinzugewinnt. Diese Online-Variante bietet aber im Unterschied zu herkömmlichen Computer-Rollenspielen eine virtuelle Welt für Tausende von Spielern und deren Interaktionen. Da ab einem gewissen Fortschritt Spielerfolge nur noch im Verbund möglich sind, fördern Online-Rollenspiele das gemeinschaftliche Spiel mit Gleichgesinnten. Sie bilden Gilden oder Clans und ziehen zusammen in epische virtuelle Schlachten.

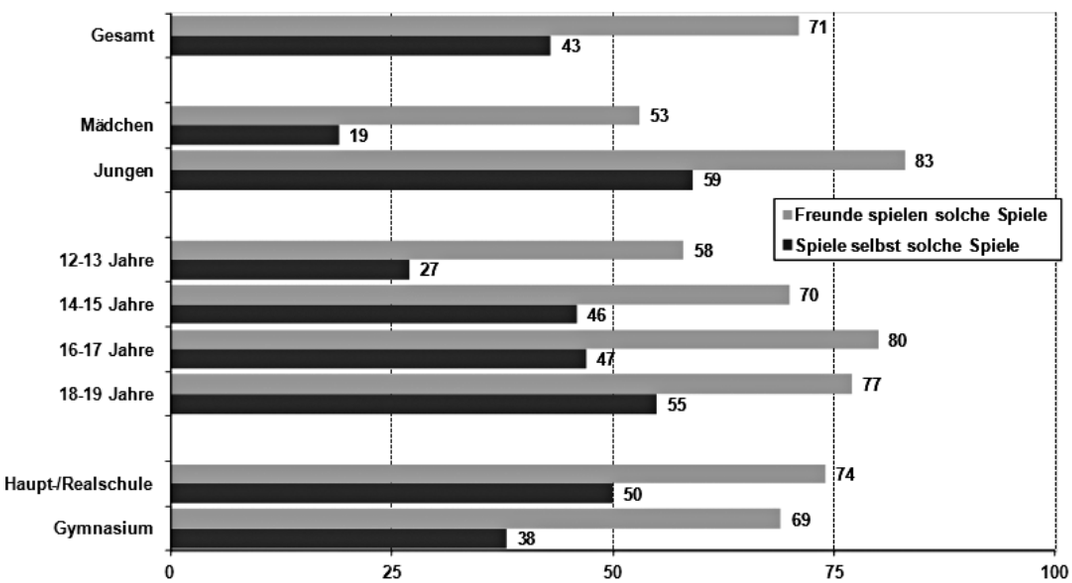
Social Games
Social Games sind ein noch relativ junges Genre. Die Spiele dieses Genres sind zumeist kleine, kostenlose Programme, die über den Internetbrowser gespielt werden können und dabei in soziale Netzwerke wie z. B. Facebook eingebunden sind. Für die Teilnahme an diesen Spielen ist eine Mitgliedschaft im jeweiligen Sozialen Netzwerk notwendig. Spielerfolge werden anderen Teilnehmern des Netzwerkes auf deren Startseite mitgeteilt und über die Kommunikationsmöglichkeiten der sozialen Plattform kann schnell Kontakt zu anderen Spielern aufgebaut werden.

Problematik von Computerspielen

Problematische Inhalte

Gewalt in Computerspielen ist in der öffentlichen Diskussion ein großes Streitthema. Von den Kritikern wird auf deren vermeintlich verrohendes Potenzial hingewiesen, Befürworter hingegen betonen die Lust am reinen Spiel. Die Diskussion wird vielleicht auch deshalb teils hitzig geführt, weil in ihr Generationenunterschiede deutlich werden: Junge, enthusiastische Spieler treffen auf Erwachsene, die in einer anderen Medienumgebung groß geworden sind. Für Letztere ist daher nur schwer verständlich, weshalb viele (meist männliche) Jugendliche viel Zeit mit ihrem Hobby verbringen und als Gangster mit Waffe in der Hand durch eine moralisch verdorbene Welt laufen (Grand Theft Auto IV), an einem Krieg gegen russische Ultranationalisten teilnehmen (Call of Duty – Modern Warfare 2), gegen Drachen kämpfen (Dragon Age) oder sich gegen Zombies zur Wehr setzen (Resident Evil 5). Laut der Studie **Jugend, Information, (Multi-)Media** (JIM-Studie) 2015 spielen immerhin 43 % der jugendlichen Computerspieler brutale bzw. besonders gewalthaltige Computer-, Konsolen- oder Onlinespiele. 71% geben an, dass ihre Freunde solche Spiele spielen. Der Anteil von Jungen (59 %), die gewalthaltige Computerspiele spielen, ist deutlich höher als der Anteil der Mädchen (19 %):

Nutzung von brutalen bzw. besonders gewalthaltigen Computer-, Konsolen-, Onlinespielen 2015



Quelle: MPSF (2015); Angaben in %; Basis: Nutzer von Computer-, Konsolen-, Onlinespielen, n=970[9]

Die These, dass gewalthaltige, brutale Computerspiele ihre Nutzer aggressiv machen würden, konnte bisher nicht eindeutig bestätigt werden. Breit diskutiert wurde diese Ansicht v. a. in der medialen Öffentlichkeit nach den Amokläufen in Erfurt (2002) und Winnenden (2009). Damals wurde in der Auseinandersetzung über die Beweggründe der Täter neben einem laxen Gesetz zum Waffenbesitz v. a. sog. **Killerspiele** verantwortlich gemacht. An sich ist der Begriff „Killerspiel" alt und wurde früher für Nicht-Computerspiele wie z. B. **Paintball** und **Laser Tag** verwendet. Nach den Amokläufen wurden Killerspiele vorwiegend in Zusammenhang mit Computerspielen genannt, in denen die Spieler in der **Ich-Perspektive** auf andere Charaktere schießen. Auf diese Weise, so eine verbreitete Meinung, wären die Amokläufer zu ihrer Tat angeregt worden und hätten bereits im Spiel das Töten von Menschen geübt. Es gibt allerdings keinen erwiesenen direkten Zusammenhang zwischen der Nutzung von

Gewaltspielen und der Ausübung von realer Gewalt. Viel eher sind die Zusammenhänge multifaktoriell zu sehen. Beeinflusst wird Gewaltbereitschaft in einem Zusammenspiel von individuellen Merkmalen und Umwelteinflüssen. Und dennoch: Computerspiele stellen einen von vielen Faktoren da, die auf Kinder und Jugendliche Einfluss nehmen.

In Zusammenhang mit stereotypen Rollenbildern wird der Einfluss von Computerspielen wohl deshalb ebenfalls diskutiert: Eine deutliche Mehrheit der Computerspiele setzt auf eine stereotype Darstellung von Männlichkeit und Weiblichkeit. Männer werden folglich als stark handelnd mitunter auch gewalttätig porträtiert. Frauen hingegen bekleiden eher Nebenrollen oder sind Trophäe der männlichen Figur. Spiele, in denen Frauen der handelnde Charakter sind, wie **Tomb Raider**, zeigen den weiblichen Körper hypersexualisiert[10]. Mehrheitlich sind die Charaktere jedoch männlich, was der vorwiegend männlichen Nutzerschaft geschuldet sein mag.

Computerspiele-Sucht

Neben der Gewaltdebatte prägt die Diskussion mit Eltern vor allem die Frage nach der zeitlichen Nutzung von Computerspielen und die damit zusammenhängenden Ängste, ihre Kinder könnten in die Abhängigkeit abgleiten. Eltern von spielenden Kindern beklagen oft den hohen Zeitaufwand, den ihre K inder für das Hobby aufbringen. Jedoch ist nicht jeder Samstag, an dem ein Teenie 6 Stunden vor dem Rechner zubringt, um ein Spiel zu spielen Indiz für eine Computer-spiele-Abhängigkeit. Kritisch wird es erst, wenn die folgenden Kriterien erfüllt sind[11]:

- Das Kind hat ein unwiderstehliches Verlangen, am Computer zu spielen. Nur unter großen Kraftanstrengung oder Androhung von Konsequenzen seitens der Eltern, kann es sich vom Bildschirm lösen.
- Das Kind hat keinen Überblick über seinen Spielkonsum – auch nachts werden Stunden vor dem Computer zugebracht.
- Versuche, den Konsum einzuschränken, scheitern.
- Das Kind möchte immer häufiger spielen; auch, um auf diese Weise Konflikten, Frustration und Misserfolgen des Alltags zu entfliehen.
- Wenn das Kind nicht spielt, fühlt es sich psychisch und körperlich unwohl.
- Die schulischen Leistungen des Kindes leiden, Freundschaften werden vernachlässigt.
- Wenngleich Konflikte und Schwierigkeiten, die durch das exzessive Spielen verursacht werden, zunehmen, spielt das Kind weiterhin.
- Das Spielen dominiert Gedanken, Gefühle und Verhalten des Kindes und beherrscht seinen Tagesablauf.

Die Computersucht ist eine Unterform der Verhaltenssüchte. Computersucht ist als Krankheit (noch) nicht anerkannt. Oft sind es Zweitdiagnosen wie Depression, die eine Therapie ermöglichen. Wichtig ist es frühzeitig Rat und Hilfe einzuholen.

Computerspiele & Jugendmedienschutz

Die vorgestellte Problematik der Computerspiele verdeutlicht, dass es aus Perspektive des Jugendschutzes wichtig ist, die Nutzung von Computerspielen – gerade für jüngere Kinder – zu reglementieren.

Grundsätzlich ist der Schutz der Minderjährigen und Jugendlichen vor problematischen Medieninhalten in zwei verschiedenen rechtlichen Grundlagen verankert:

- Jugendschutzgesetz (JuSchG): Das JuSchG regelt den Umgang mit Trägermedien. Der juristische Begriff „Trägermedien“ umfasst alle materiell greifbaren Medien, wie z. B. DVDs, CDs etc.
- Jugendmedienschutz-Staatsvertrag der Länder (JMStV): JMStV regelt den Jugendschutz im Rundfunk und in den Telemedien. Unter den Begriff „Telemedien“ werden materiell nicht greifbare Medien gefasst, wie bspw. eine Radiosendung oder eine Internetseite.

Für Computerspiele bedeutet dies, dass alle Spiele, die auf Datenträgern angeboten werden, auf Basis des Jugendschutzgesetzes geprüft werden.
Diese Prüfung übernimmt die Selbstkontrolleinrichtung **Unterhaltungssoftware Selbstkontrolle** (USK). Sie sichtet die Trägermedien und versieht sie mit einer Alterskennzeichnung:

Quelle: bundespruefstelle.de (2015)[12]

Auf europäischer Ebene werden Trägermedien zusätzlich durch das **Pan European Game Information-System** (PEGI) gekennzeichnet. Die Kriterien, die dieser Einschätzung zugrunde liegen, weichen von den USK-Kriterien ab.

Spiele, die als Telemedien vorliegen, wie bspw. **Browserspiele** unterliegen den Bestimmungen des Jugendmedienschutz-Staatsvertrages. Für diese Spiele existieren keine verbindlichen Alterskennzeichen[13]. Es sei denn, es ist eine Online-Version eines auch als Datenträger (Trägermedium) vorliegenden Spiels. Dann greift die Alterskennzeichnung der USK. Für Eltern und deren Kinder ist es daher nicht einfach, die Inhalte der Online-Spiele nach der Eignung für das Alter ihres Kindes einzuschätzen.

Kritisch ist auch die Einschätzung der Spiele-Apps. Zwar finden sich in den großen App Stores (Apple App Store, Google Play etc.) Alterseinschätzungen oder inhaltliche Einschätzungen der Apps. Nach welchen Kriterien hier allerdings bewertet wird, ist nicht offen gelegt – sicher ist nur, dass es keine deutschen Rechtsgrundlagen sind. Außerdem überprüft niemand, wie alt der Nutzer tatsächlich ist, der auf eine +17-App zugreifen möchte.

Tipps für den Umgang mit SchülerInnen, die Computerspiele nutzen:

- *Sprechen Sie mit den SchülerInnen über Computerspiele*
- *Machen Sie Gewalt in Spielen zum Thema*
- *Geben sie reale Orientierung*
- *Begegnen Sie Computerspielen offen*
- *Machen Sie sich schlau und spielen Sie selbst einmal*
- *Achten Sie auf die Altersfreigabe*

Endnoten

[1] BUNDESVERBAND INTERAKTIVE UNTERHALTUNGSSOFTWARE E.V. (BIU) (2015, März). *Gesamtmarkt digitale Spiele im ersten Halbjahr 2014.* Aufgerufen am 19.03.2015 unter http://www.biu-online.de/de/fakten/marktzahlen.html

[2] BUNDESVERBAND INTERAKTIVE UNTERHALTUNGSSOFTWARE E.V. (BIU) (2015, März). *Umsatzentwicklung mit Spiele-Apps.* Aufgerufen am 19.03.2015 unter http://www.biu-online.de/de/fakten/marktzahlen-1-halbjahr-2014/online-browser-und-app-spiele/umsatzentwicklung-mit-spiele-apps.html

[3] MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.) (2015). *JIM-Studie 2015, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland.* (S. 42). Aufgerufen am 01.12.2015 unter http://www.mpfs.de/fileadmin/JIM-pdf15/JIM_2015.pdf

[4] S. 43, ebd.

[5] SPIELBAR.DE (2015). *Faszination & Erlebnis.* Aufgerufen am 19.03.2015 unter http://www.spielbar.de/neu/praxiswissen-computerspiele/1x1/faszination-erlebnis/

[6] KLICKSAFE.DE (2015, März). *Spieler zwischen Frust und Flow* (Abs. 12). Aufgerufen am 19.03.2015 unter http://www.klicksafe.de/themen/spielen/computerspiele/faszination/spieler-zwischen-frust-und-flow/

[7] SPIELBAR.DE (2015, März). *Genres und Spielweisen.* Aufgerufen am 19.03.2015 unter http://www.spielbar.de/neu/praxiswissen-computerspiele/1x1/genres-spielweisen/

[8] KLICKSAFE.DE (2015, März). *Genres.* Aufgerufen am 19.03.2015 unter http://www.klicksafe.de/themen/spielen/computerspiele/genres/s/genres/

[9] MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.) (2015). *JIM-Studie 2015, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland.* (S. 45). Aufgerufen am 01.12.2015 unter http://www.mpfs.de/fileadmin/JIM-pdf15/JIM_2015.pdf

[10] V. ORDE, H. (2013). *Geschlechterbilder in den Medien. Eine Zusammenfassung ausgewählter Forschungsergebnisse. TeleviZion* (2013/2) (S.11-15). Aufgerufen am 23.10.2014 unter http://www.br-online.de/jugend/izi/deutsch/publikation/televizion/26-2013-2/vomOrde_Geschlechterbilder_Medien.pdf

[11] UNIVERSITÄTSMEDIZIN MAINZ. (2015, März). *Computerspielsüchtig? Checkliste für Eltern.* Aufgerufen am 19.03.2015 unter http://www.unimedizin-mainz.de/psychosomatik/patienten/behandlungsangebote/ambulanz-fuer-spielsucht/checkliste-computerspiel.html

[12] BUNDESPRUEFSTELLE.DE (2015, März). *Jugendmedienschutz – wer ist für was zuständig? Games* (Abs. 3). Aufgerufen am 19.03.2015 unter http://www.bundespruefstelle.de/bpjm/Jugendmedienschutz/games.html

[13] BUNDESPRUEFSTELLE.DE (2015, März). *Onlinespiele.* Aufgerufen am 19.03.2015 unter http://www.bundespruefstelle.de/bpjm/Jugendmedienschutz/Games/onlinespiele.html

Arbeitsblatt	**AB 1**	**AB 2**
Titel	**Was ist so schön an Handy-Spielen?**	**Online-Spiele – was hältst du von diesen Tipps?**
Kompetenzen	Die Schülerinnen und Schüler fassen ihre Erfahrungen mit Handy-Spielen zusammen und setzen ein gemeinsames Spielen, auch mit den Eltern, um.	Die Schülerinnen und Schüler beurteilen die klicksafe-Tipps für Eltern zum Thema Computerspiele.
Methoden	Tabelle, Partnerarbeit	Stufenleiter, Tabelle
Material	Arbeitsblatt, eigenes Handy, evtl. Elternbrief	Arbeitsblatt
Zeit (in Minuten)	90 (plus Hausaufgabe)	90
Zugang Internet/PC	nein	nein

Hinweise für die Durchführung

AB 1: Was ist so schön an Handy-Spielen?

Über Handy-Spiele zu reden ohne sie zu spielen ist nicht wirklich sinnvoll. Sicherlich finden sich zahlreiche Spiele auf den Handys Ihrer Schülerinnen und Schüler. Sie sollen darüber nachdenken, was ihnen an dieser Art der Spiele gefällt und was nicht. Im zweiten Schritt sollen sie sich untereinander **und** mit Erwachsenen austauschen. Diesen Schritt sollten Sie vielleicht im Vorfeld den Eltern kommunizieren (Per Elternbrief Bescheid geben, was auf die Eltern zukommt!). Kinder haben einen großen Spaß daran und genießen ihre Rolle als „Experten", wenn sie Erwachsenen etwas am Computer, Tablet oder Handy vorführen können. Viele der Reaktionen werden typisch sein. Kinder gehen sehr viel selbstverständlicher, unbefangener damit um, Eltern sehen oft vor allem die Risiken.

Hier eine Formulierungshilfe für einen Elternbrief:

> Liebe Eltern der Klasse x,
> das Spielen am Handy gehört sicherlich auch für Ihr Kind inzwischen zum Alltag. Wir wollen in der Schule dieses Phänomen thematisieren. Dazu betrachten wir kleine Handy-Spiele, die die Kinder üblicherweise spielen und die für die Altersgruppe geeignet sind. In einem zweiten Schritt sollen die Schülerinnen und Schüler diese Spiele (zu Hause) mit Ihnen, den Großeltern oder anderen Erwachsenen spielen und darüber sprechen. Bitte unterstützen Sie Ihr Kind dabei. Danke.

AB 2: Online-Spiele – was hältst du von diesen Tipps?

Mit dem kleinen Fallbeispiel zum Einstieg sollen die Schülerinnen und Schüler die Tipps von klicksafe zu dem Thema kennen lernen. Dabei sollen sie in die Rolle des Vaters schlüpfen und so einen Rollentausch erleben. Mithilfe der **„Stufenleiter"** können die Schüler eine Bewertung der Tipps vornehmen, die als wichtigstes Kriterium die Teilhabe haben wird. Vielleicht können Sie Ihre Schülerinnen und Schüler anregen, die Tipps auch zu Hause weiterzugeben. Die letzte Phase, die Diskussion des Problems, könnte in Form eines Rollenspiels geschehen oder auch in einem Klassengespräch oder einer Podiumsdiskussion. Vielleicht bietet sich die Methode der „Talking Chips" an, wo jede Schülerin/jeder Schüler zwei „Talking Chips" erhält und für eine Meldung einsetzen muss. Sind alle Chips verbraucht, gibt es eventuell neue. Auf diese Weise erreichen Sie, dass sich alle Schülerinnen und Schüler genau zweimal beteiligen (müssen).
Flyer: **www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_Allgemein/Flyer_ComSpiel_Eltern_klicksafe.pdf**

Lust auf mehr?

- Die Online-Spiele boomen und sind, auch wegen ihrer schlechten rechtlichen Fassbarkeit, manchmal problematisch. Gerade die Bereiche „Datenschutz" und „Kostenfallen" bieten sich für eine Vertiefung an, evtl. auch das Problem „Spielsucht".
- Anhand des Flyers „Social Games – Online spielen in Communitys" oder der Webseite **www.klicksafe.de/themen/spielen/computerspiele/social-gaming-im-griff-behalten-tipps-fuer-kinder/** können Sie die Schüler Tipps für Jugendliche erarbeiten lassen:

  Flyer: **www.klicksafe.de/service/materialien/broschueren-ratgeber/social-games-online-spielen-in-communitys/s/spiele/**

Was ist so schön an Handy-Spielen?

Nilays Lieblingsspiel auf ihrem Smartphone ist **Flappy Bird.** Immer wenn ihr langweilig ist, z. B. auf der Busfahrt zur Schule, dann lässt Nilay auf ihrem Handy den kleinen Vogel durch die Hindernisse fliegen. Aber **Flappy Bird** ist nur eines von vielen Spielen, die sie auf ihrem Smartphone hat. Je nach Lust, Laune und Zeit spielt sie das eine oder das andere.

Arbeitsaufträge

1. Findet euch zu dritt zusammen, wenn möglich mit verschiedenen Handy-Spielen.

2. Spielt zunächst das eigene Spiel und danach – wenn möglich – reihum die Spiele der anderen.

3. Füllt danach für eines der Spiele diese Tabelle aus:

Dieses Spiel habe ich gespielt:

.....

Das gefiel mir an dem Spiel gut:

+

−

Das gefiel mir an dem Spiel nicht so gut:

Ich zeige dieses Spiel:

.....

4. Nun darfst du dieses Spiel einem Erwachsenen zeigen! Lasse ihn unbedingt selbst spielen und frage ihn, was ihm an dem Spiel gefällt und was nicht!

5. Sprecht in der Klasse über eure Erfahrungen mit den Erwachsenen!

Nilays Eltern haben ein wenig Sorge, wenn sie zu viel mit ihrem Handy spielt. Kannst du verstehen warum? Redet in der Klasse darüber, wie Erwachsene Handy-Spiele bei Jugendlichen sehen.

Online-Spiele – was hältst du von diesen Tipps? (1/3)

Der Vater von Anna (14 Jahre) ist schier verzweifelt. Er weiß nicht mehr, was er tun soll, denn Anna sitzt jede freie Minute vor Handy, Computer und Tablet und spielt. Der Vater hat ihr schon das Taschengeld gestrichen, aber Anna spielt immer noch Online-Spiele, die angeblich kostenlos sind. Er hat überhaupt keinen Überblick mehr darüber, was genau Anna spielt und steht kurz davor, ihr die Geräte ganz wegzunehmen.

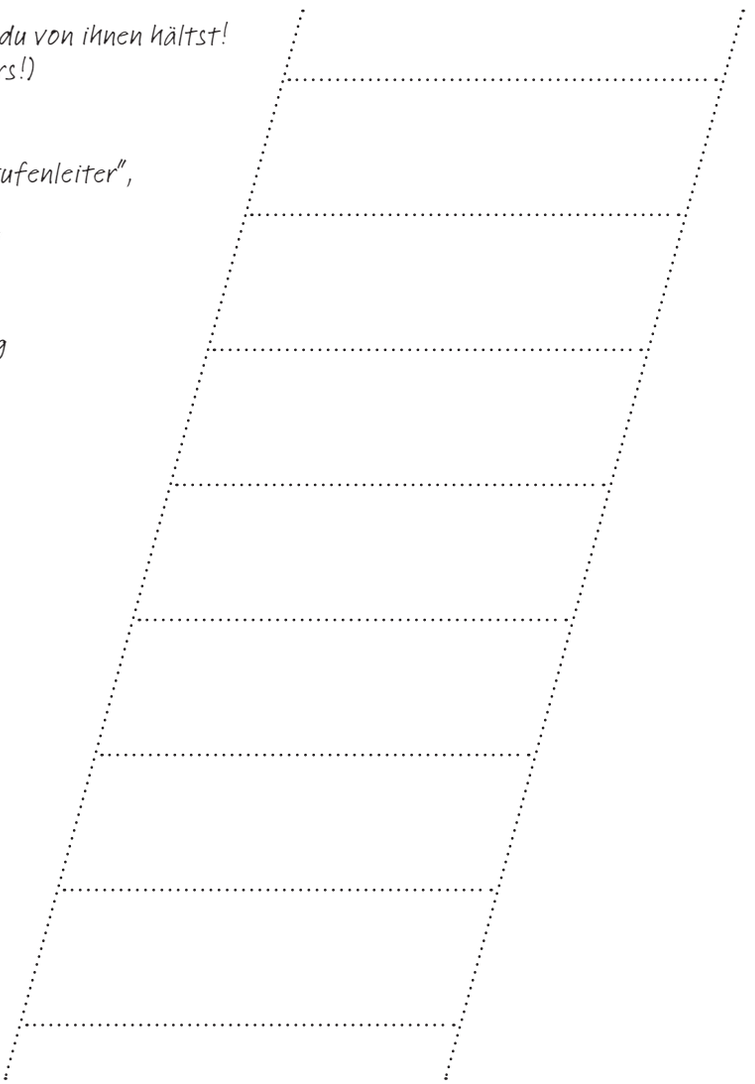
Da stößt Annas Vater auf das Internetangebot von klicksafe.de und liest folgende Tipps:
(siehe nächste Seite)

Arbeitsaufträge

1. Lies die Tipps sorgfältig und notiere kurz, was du von ihnen hältst! (Denke daran, du bist in der Situation des Vaters!)

2. Welche der Tipps hältst du für wichtiger? Sortiere die Tipps nach Wichtigkeit in einer „Stufenleiter", den wichtigsten Tipp nach oben. Tausche dich mit deinen Klassenkameraden darüber aus und zeigt euch gegenseitig eure Einschätzungen.

3. Diskutiert mit der gesamten Klasse eine Lösung für Anna und ihren Vater!



Online-Spiele – was hältst du von diesen Tipps? (2/3)

Tipp	**Erklärung**	**Das halte ich davon:** (in der Rolle des Vaters)
klicksafe.de-Tipp 1: Zeigen Sie Interesse!	Informieren Sie sich über die unterschiedlichen Plattformen, Spielarten (Genres) und die momentan angesagten Spiele. Pädagogische Angebote (z. B. **www.Spieleratgeber-NRW.de, www.spielbar.de, www.usk.de**) bieten weitreichende Informationen zu Inhalten, Altersfreigaben, Chancen und Risiken der gängigen Spiele.	
klicksafe.de-Tipp 2: Beachten Sie Spiele auf mobilen Geräten!	Smartphones und Tablets werden auch als Spielgeräte immer beliebter. Das Angebot ist groß und unübersichtlich. Sie sollten daher gemeinsam geeignete Spiele aussuchen, um z. B. Kostenfallen und problematische Inhalte zu umgehen.	
klicksafe.de-Tipp 3: Sprechen und spielen Sie mit Ihrem Kind!	Interesse, Austausch und gemeinsame Medienerlebnisse ermöglichen eine vertrauensvolle Basis zwischen Ihnen und Ihrem Kind. Suchen Sie daher das offene Gespräch und begegnen Sie dem Freizeitinteresse mit einer grundlegend unvoreingenommenen Haltung. Durch gemeinsame Spielerlebnisse können Sie mitreden, die Faszination nachvollziehen und viel eher erkennen, ob es für Ihr Kind geeignet ist.	
klicksafe.de-Tipp 4: Vereinbaren Sie gemeinsam Regeln!	Erstellen Sie gemeinsam mit Ihrem Kind verbindliche und nachvollziehbare Regelungen zum Medienkonsum. Dazu zählen neben der Nutzung des Computers auch Fernsehen, Smartphones und Spielkonsolen. Achten Sie bei der Vereinbarung auf regelmäßige Bildschirmpausen.	
klicksafe.de-Tipp 5: Orientieren Sie sich an Zeitvorgaben!	Zur Orientierung können folgende Zeitvorgaben hilfreich sein: **4–6 Jahre:** ca. 20 bis 30 Minuten pro Tag in Begleitung der Eltern **7–10 Jahre:** ca. 45 Minuten pro Tag **11–13 Jahre:** ca. 60 Minuten pro Tag (Suchen Sie gezielt nach empfehlenswerten Spielen für Ihr Kind, z. B. auf **www.Spieleratgeber-NRW.de, www.internet-abc.de/eltern**). Für ältere Heranwachsende eignet sich in der Regel ein gemeinsam vereinbartes Medienbudget pro Woche viel eher als eine tägliche Höchstgrenze.	
klicksafe.de-Tipp 6: Achten Sie unbedingt auf die Alterskennzeichnung!	Prüfen Sie unter **www.usk.de**, ob ein Spiel für die Altersgruppe Ihres Kindes freigegeben ist und somit ein entsprechendes Alterskennzeichen der Unterhaltungssoftware Selbstkontrolle (USK) trägt. Diese bieten Ihnen eine wichtige Orientierungshilfe, stellen dabei allerdings keine pädagogische Empfehlung dar. Auch unterliegen viele Spiele im Internet keiner Kennzeichnungspflicht. Nutzen Sie hierzu ergänzende Beratungsangebote (z. B. **www.Spieleratgeber-NRW.de**).	

Online-Spiele – was hältst du von diesen Tipps? (3/3)

Tipp	**Erklärung**	**Das halte ich davon:** (in der Rolle des Vaters)
klicksafe.de-Tipp 7: Seien Sie Vorbild!	Erklären Sie lhrem Kind, weshalb es wichtig ist, dass es Gesetze zum Jugendschutz und zum Urheberrecht gibt. Hinterfragen Sie auch lhre eigenen Mediengewohnheiten und gehen Sie mit gutem Beispiel voran.	
klicksafe.de-Tipp 8: Bieten Sie Alternativen!	Viele Kinder sitzen aus reiner Langeweile vor dem Computer oder der Konsole. Bieten Sie lhrem Kind zum Ausgleich gemeinsame Unternehmungen an. Vermeiden Sie es, Computerspiele als „Babysitter" einzusetzen.	
klicksafe.de-Tipp 9: Tauschen Sie sich aus!	Fragen Sie andere Eltern, wie sie mit dem Medienkonsum ihrer Kinder umgehen. lnformieren und unterstützen Sie sich gegenseitig. Das gibt lhnen Sicherheit und fördert die eigene Kompetenz.	
klicksafe.de-Tipp 10: Nutzen Sie Spiele nicht als erzieherisches Druckmittel!	Computerspiele sollten weder zur Belohnung noch als Bestrafung eingesetzt werden. Dadurch erhalten sie einen ungewollt hohen Stellenwert im Alltag lhrer Kinder. Halten Sie lieber an einer verbindlichen Regelung fest: Zuerst die Hausaufgaben, dann eine Pause, dann Computerspielen.	
klicksafe.de-Tipp 11: Handeln Sie, wenn Sie sich um das Spielverhalten lhres Kindes Sorgen machen!	Auskünfte und Hilfsangebote bieten Computerspielsucht-Hotlines und Beratungsstellen, wie bspw. das Berliner Universitätsklinikum Charité, die Uniklinik Mainz sowie die Nummer gegen Kummer. Werden Sie aktiv, wenn lhr Kind (über einen längeren Zeitraum): ■ tägliche Pflichten wie Hausaufgaben vernachlässigt. ■ alle Zeitabsprachen ignoriert. ■ seine Kontakte zu Gleichaltrigen verliert. ■ das lnteresse an anderen Aktivitäten stark zurückgeht.	
klicksafe.de-Tipp 12: Sensibilisieren Sie Ihr Kind bzgl. der Weitergabe persönlicher Daten bei der Nutzung von Online-Spielen.	Geben Sie folgende Tipps weiter: ■ Lege Dir eine E-Mail Adresse an, die Du nur für die Anmeldung bei unbekannten Anbietern benutzt! ■ Nutze einen Nickname (Spitznamen) und eine E-Mail-Adresse, die keine Rückschlüsse auf Dich zulassen! ■ Gib Deinen Nickname (Spitzname) und persönliche Daten nur an Bekannte weiter! ■ Nutze als Avatar (virtuelle Spielfigur) kein Foto von Dir! ■ Lies in den AGBs bzw. der Datenschutzerklärung nach, was der Anbieter mit Deinen Daten macht!	

Quelle: www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_Allgemein/Flyer_ComSpiel_Eltern_klicksafe.pdf

4

Wie wir uns vernetzen: Communitys, Nutzerkonten und Mikroblogging

4|1 Soziale Netzwerke: Facebook und Trends

4|2 YouTube: Ein Nutzerkonto für alles

4|3 Mikroblog: Twitter

Soziale Netzwerke

Was sie ausmacht und weshalb sie faszinieren

Online Communitys
Überall dort, wo sich Menschen online zu Gruppen zusammenfinden oder gemeinsam einen bestimmten Online-Dienst nutzen, spricht man von **Online Communitys**[1].

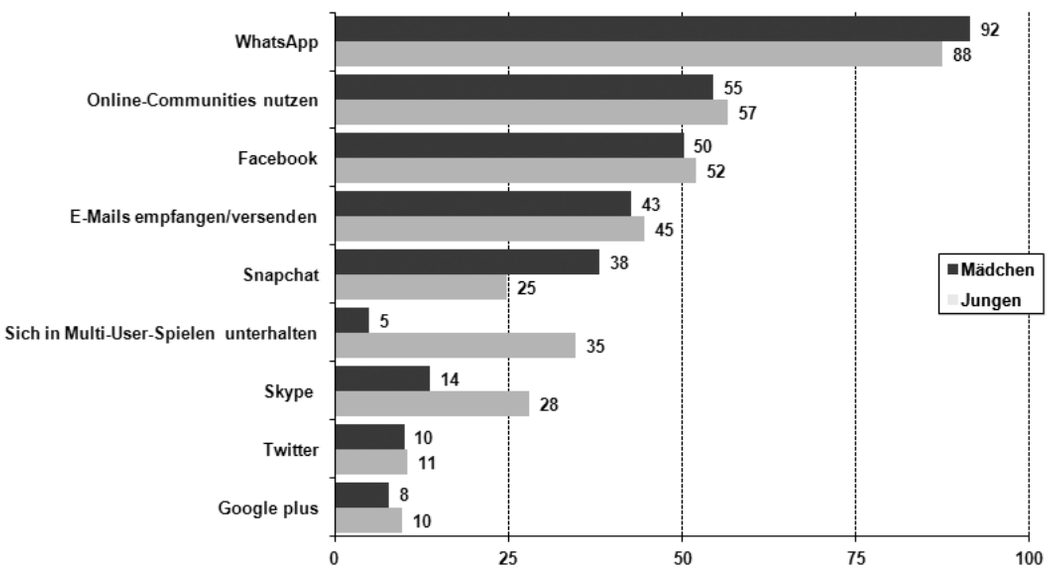
Online Communitys liegen im Trend: Es gibt immer mehr Dienste und Apps, mit deren Hilfe Menschen sich verabreden, sich unterhalten, miteinander spielen, handeln, diskutieren, sich gegenseitig helfen, flirten u. v. m. Nicht nur privat werden die Online Communitys häufig genutzt, auch in politischer und wirtschaftlicher Hinsicht spielen sie eine wichtige Rolle. Erinnert sei an dieser Stelle an den Arabischen Frühling 2011: In vielen muslimisch geprägten Ländern gingen Menschen auf die Straße, um für mehr Rechte zu demonstrieren. „Facebook war anfänglich das wichtigste Medium zur Mobilisierung der Bevölkerung. Über Twitter und YouTube sendeten junge Araberinnen und Araber Informationen über Massenproteste um die Welt"[2].

Genannt sei an dieser Stelle auch der Trend **„Crowdfunding"**, der über Online Communitys verbreitet wird. Crowdfunding ist eine Möglichkeit, finanzielle Mittel für ein Projekt zu akquirieren. Wie der Name verrät, geht es darum, viele Personen von einem Projekt zu überzeugen und sie dazu zu motivieren, kleine Beträge für ein Projekt zu spenden. Auf diese Weise wurde bspw. der Film Stromberg 2011 realisiert: Innerhalb einer Woche gingen insg. 1 Million Euro an sog. Mikro-Spenden ein.

Online Social Communitys
Von einer Online **Social Community** (deutsch: Soziales Netzwerk) spricht man dann, wenn bei einer Online Community wie sie oben beschrieben wurde, das soziale Miteinander und der soziale Austausch im Vordergrund steht.

Soziale Netzwerke im Internet haben für Jugendliche eine große Bedeutung. Hier kommunizieren sie mit ihren Freunden, mit der Familie und mit Bekannten. Es verwundert daher nicht, dass die meisten der Jugendlichen Communitys wie z. B. WhatsApp regelmäßig nutzen:

Aktivitäten im Internet – Schwerpunkt: Kommunikation 2015
– Täglich / mehrmals pro Woche –



Quelle: MPFS (2015). JIM 2015. Angaben in Prozent. Basis: Befragte, n=1.200 [3]

So funktionieren Soziale Netzwerke

Das Konzept Sozialer Netzwerke wird erklärt mit den Aspekten Selbstdarstellung, Teilhabe und Beziehungspflege durch Vernetzung[4] sowie mit dem „Nutzen- und Belohnungsansatz“[5]. Medien werden zur Befriedigung von Wünschen und Bedürfnissen genutzt, nach:

- Unterhaltung
- Orientierung, Identitätsbildung
- Teilhabe, Zugehörigkeit und Soziale Unterstützung
- Selbstdarstellung und Anerkennung

Selbstdarstellung

Die (positive) Darstellung der eigenen Person, des eigenen Lebens, der Hobbys, Erlebnisse etc. ist ein Kernelement der Sozialen Netzwerke. In einem Facebook-Profil können u. a. Angaben zu Alter, Wohnort, Arbeitsplatz, Kontaktinfos, Beziehungsstatus, Lebensereignissen, Hobbys, Lieblingsmusik, Lieblingsbüchern oder -filmen gemacht werden. Hinzu kommen Fotos, die Nutzer selbst einstellen oder auf denen sie durch andere Nutzer markiert werden, Textbeiträge oder Filmclips, die sie (re)posten, **Gefällt-mir-**Angaben, die sie machen etc. Die Nutzer präsentieren sich mit diesen Mitteln so, wie sie von anderen Nutzern gesehen werden möchten.

Vernetzung

Die Vernetzung mit anderen Mitgliedern eines Sozialen Netzwerks ist einfach: Über einen Button auf der Profilseite können Nutzer einer anderen Person eine Kontaktanfrage schicken. Bestätigt diese Person die Anfrage, ist sie der eigenen Kontaktliste hinzugefügt – sie wurde **geaddet**.
Die Kontakte werden je nach Netzwerk etwas anders benannt: In **Facebook** heißen sie bspw. **Freunde**, in **Twitter Follower** etc. Die Kontakte können in **Gruppen** (Facebook) oder **Kreise** (Google+) entsprechend gleicher Interessen, Hobbys etc. eingeteilt werden. Die Anzahl der Kontakte wird unter Jugendlichen als sichtbares Zeichen der Beliebtheit einer Person gewertet. Entsprechend finden sich bei einigen Nutzern mehrere hunderte Kontakte. Nicht zu allen Kontakten wird ein enges persönliches Verhältnis gepflegt. Oft sind auch Personen verknüpft, die sich nur über eine dritte Person „kennen“: Jana ist z. B. mit Carina befreundet, diese kennt wiederum Helena und Jana added nun Helena, ohne diese jemals getroffen zu haben.

Kommunikation

In medientheoretischem Sinne ist jede soziale Handlung in einem Sozialen Netzwerk, bspw. das Posten von Beiträgen oder das Liken bestimmter Beiträge ebenso als „Kommunikation“ zu verstehen wie der Nachrichtenaustausch über die integrierten Tools wie Chats, Nachrichten, Tweets, Posts usw. Sehr wichtig für die Kommunikation unter Facebook-Nutzern ist die Möglichkeit, die Posts (Texte/Fotos/Videos) anderer Nutzer zu kommentieren und sich so miteinander über einen Beitrag auszutauschen. Mit dem hinlänglich bekannten **Like-** bzw. **Gefällt-mir-Button** wird Anerkennung und Gefallen bekundet.

Faszination Sozialer Netzwerke

Angesichts der Millionen Nutzer, die die Sozialen Netzwerke verzeichnen, scheint es fast so, als hätte die Menschheit auf diese Möglichkeit des sozialen Miteinanders gewartet. Der Philosoph Peter Sloterdijk formulierte diesbezüglich treffend: „Der Rückzug von den anderen, das Alleinseindürfen, das ist die große Errungenschaft des Individualismus. Aber der Mensch ist auch ein Stammeswesen. Diese Netzwerke können beides glücklich vereinen: Man bleibt vom lästigen, vom aufsässigen anderen verschont, und doch ist der ganze Stamm immer anwesend“[6]. Es geht also im weitesten Sinn um das menschliche Bedürfnis, mit anderen in Kontakt zu sein, das durch die Teilhabe in Sozialen Netzwerken befriedigt wird.

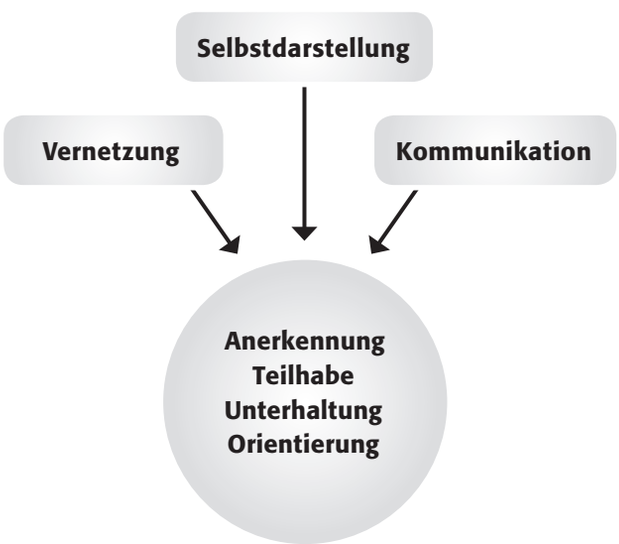
Konkret bedienen die Möglichkeiten Sozialer Netzwerke wie Vernetzung, Selbstdarstellung und Kommunikation wichtige Bedürfnisse nach **Anerkennung, Teilhabe, Unterhaltung** und **Orientierung:**

Anerkennung
Ein wichtiges Bedürfnis ist die Anerkennung durch andere. In Sozialen Netzwerken wird diese durch Beiträge ausgedrückt oder etwa in Facebook direkt durch das „Liken” mittels des „Gefällt mir“-Buttons bspw. eines eingestellten Fotos. Auch die bloße Wahrnehmung durch andere ist eine Form der Anerkennung.

Teilhabe
Teil einer Gruppe zu sein ist für jeden Menschen bedeutsam. Soziale Netzwerke bieten Gruppenzugehörigkeit, ohne größere Anstrengung: Man „liked“ die Seite einer Musikgruppe, einer Marke etc. oder man tritt einer bestimmten Gruppe bei. Hier hat man die Möglichkeit, auf Gleichgesinnte zu treffen und mit ihnen ins Gespräch zu kommen.

Unterhaltung
Unser Zeitalter ist durch das (mobile) Internet geprägt. Von beinahe überall und zu jeder Zeit hat man Zugriff auf private und redaktionelle Nachrichten, auf Zeitungen und Zeitschriften, auf Videos, Blog-Inhalte etc. In Sozialen Netzwerken findet der Nutzer ein buntes Potpourri unterschiedlicher, unterhaltsamer und informativer Beiträge. Dieser Informationsstrom gehört zur Alltagswelt vieler Jugendlicher, auf den sie ungern verzichten.

Orientierung
Zu den Entwicklungsaufgaben von Jugendlichen gehört u. a. die Entwicklung des Selbst-Konzeptes (Wer bin ich?) und die Herausbildung von Selbstvertrauen in die eigenen Fähigkeiten und Fertigkeiten[7]. In dieser Phase der Selbstfindung spielen Familie, Gleichaltrige und mediale Vorbilder wie Musik-, TV-, YouTube-, oder Kinostars eine entscheidende Rolle. Sie geben den Jugendlichen Orientierung, indem sie vorgeben, was angesagt und folglich gesellschaftlich akzeptiert ist. Auch Soziale Netzwerke bieten diese Orientierung: In der Kommunikation miteinander verhandeln hier Jugendliche – ohne Bewertung durch Erwachsene – ihre Themen und formen Meinungen und Haltungen.



Quelle: klicksafe

Sicher in Sozialen Netzwerken unterwegs

Melden und Ignorieren

Die meisten Sozialen Netzwerke bieten die Möglichkeit, sich vor unerwünschten Kontakten und Beiträgen folgendermaßen zu schützen:

- **Integriertes Meldesystem:** Anstößige Inhalte können dem Betreiber gemeldet werden.
- **Ignorieren-, oder Blockieren-Funktion:** Kontaktpersonen können ignoriert, oder blockiert werden. Dadurch können diese keine Beiträge mehr posten sowie Bilder und Beiträge kommentieren, oder persönliche Nachrichten verschicken.

Privatsphäre und Datenschutz

Manche Kinder und Jugendliche, aber auch Erwachsene geben in den Sozialen Netzwerken unbedacht sehr persönliche Informationen preis. Oft sind sich diese Personen über die Folgen ihres Tuns nicht im Klaren – das liegt nicht zuletzt daran, dass sie meist keine direkten (negativen) Konsequenzen erfahren. Problematisch ist das v. a. dann, wenn das eigene Profil nicht nur den Freunden, sondern allen Nutzern eines Sozialen Netzwerks zugänglich ist. Hier gilt es, die Sichtbarkeit der eigenen Informationen einzuschränken und diese nur für ausgewählte Personengruppen zu ermöglichen.

Es ist wichtig und richtig, die eigenen Daten vor dem Missbrauch durch andere Nutzer zu schützen. Gleichzeitig ist es aber ebenso relevant, die Verwendung und Verwertung der eigenen Daten durch den Anbieter selbst im Blick zu haben. Facebook und Co. verdienen durch die Daten ihrer Nutzer viel Geld: Auf dieser Basis können sie Werbetreibenden eine passgenaue Auslieferung ihrer Werbebotschaften ermöglichen – ein Dienst, den sie sich gut bezahlen lassen. Facebook und Co. sammeln dabei nicht nur über ihr originäres Angebot, dem Sozialen Netzwerk, ihre Daten. Auch über Seiten, die mit Facebook verknüpft sind, bspw. durch den Like-Button, können Daten auf vielen Internetseiten gesammelt werden[8].

*Tipp: Facebook bietet z. B. die Funktion **Meine Seite für Andere:** Das eigene Profil kann aus der Perspektive eines beliebigen anderen Nutzers betrachtet werden. So weiß man, welche Infos den anderen Nutzern zugänglich sind und kann gegebenenfalls Einstellungen anpassen.*

Adressbuch-Abgleich

Mit dem Adressbuch-Abgleich werden alle Adressen aus dem persönlichen E-Mail-Konto oder dem Adressbuch an das jeweilige Netzwerk übermittelt – das gilt für Laptop oder PC ebenso wie für das Smartphone. Bei Zugriff auf das Mail-Konto ist allerdings das Passwort für das E-Mail-Konto erforderlich. Bei manchen Netzwerken werden die Adressdaten dann dazu genutzt, Freunde und Bekannte anzuwerben. Vorsicht: Freunde und Bekannte werden nicht über diese Verwendung ihrer persönlichen Daten informiert!

Ortungsdienste

Einige Netzwerke bieten die Funktion, zu jedem veröffentlichten Post den Ort anzugeben, an dem man sich gerade befindet (z. B. Facebooks „Orte"). Nutzt man diese Funktion, legt die Anwendung ein Bewegungsprofil an, auf das andere Nutzer Zugriff haben. Die ständige Auffindbarkeit ist ein großer Eingriff nicht nur in die Privatsphäre, sondern auch in die Sicherheit. Funktionen wie „Orte" auf Facebook sollten allerhöchstens für gute Freunde sichtbar sein.

Aus der Praxis

Viele SchülerInnen haben ein emotionales Verhältnis zu „ihrem" Sozialen Netzwerk. Trotzdem oder gerade deshalb sollte man mit ihnen über folgende Punkte kritisch diskutieren:

- *Besprechen Sie das Konzept „Freunde"!*
- *Sensibilisieren Sie für die Weitergabe persönlicher Daten!*
- *Thematisieren Sie die Verantwortung bezüglich der Daten von anderen (Stichwort: Adressbuch-Abgleich)!*
- *Weisen Sie auf Informations- und Hilfsangebote hin!*

Facebook

Zahlen, Daten und Fakten

Ein 20-jähriger Student der Harvard University in Cambridge, Massachusetts, stellte 2004 eine Seite ins Netz, die er **The Facebook** nannte. Der Name ist angelehnt an die Tradition vieler Schulen und Universitäten, ein Jahrbuch mit Namen und Bilder der SchülerInnen oder StudentInnen zu veröffentlichen. Das hinderliche „The" wurde fallen gelassen und innerhalb von 10 Jahren erreichte **Facebook** eine Nutzerzahl von weltweit über 1,1 Milliarden Nutzer. Um sich diese Zahl besser vorstellen zu können hier ein Beispiel: Im vergangenen Jahrzehnt meldete sich täglich eine Großstadt mit der Einwohnerzahl Augsburgs – rund 270.000 Menschen – in Facebook an. Auch in Deutschland erfreut sich das Soziale Netzwerk einer großen Beliebtheit und gehört laut der **Studie Jugend, Information, (Multi-)Media** (JIM-Studie) 2015 zu den beliebtesten Online Communitys der Zwölf bis 19-jährigen[9]. Was als kleines Projekt begann ist heute ein millionenschweres Unternehmen und der junge Erfinder Mark Zuckerberg ist heute ein reicher Mann.

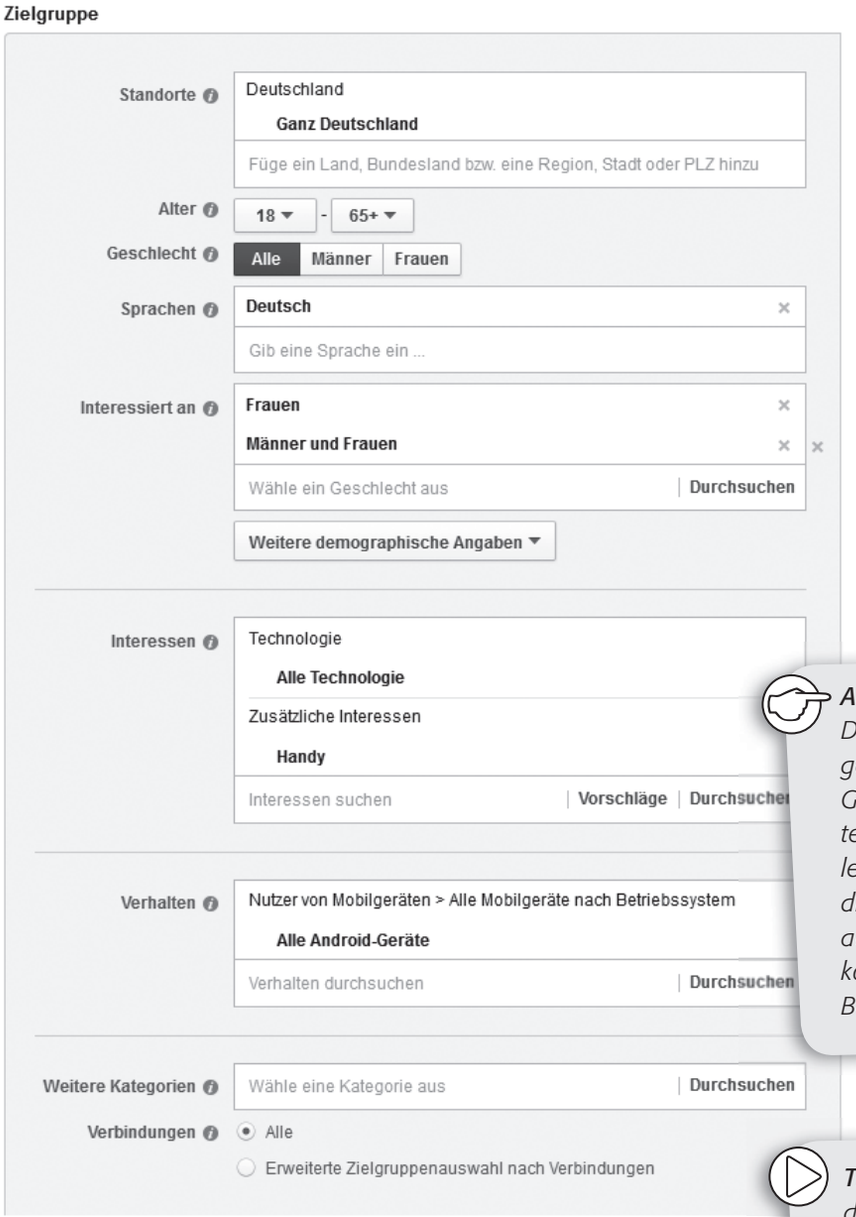
Funktionen von Facebook

Jeder Facebook-Nutzer verfügt über ein Profil (genannt **Chronik**), in dem er sich mit Namen, Wohnort, Hobbys, Lieblingsfilmen, -büchern, -musik, Fotos etc. vorstellen kann. Alle Aktivitäten des Nutzers werden hier (sofern nicht anders eingestellt) chronologisch entlang eines Zeitstrahl dargestellt. Auf der **Pinnwand** kann der Nutzer Texte, Bilder oder Videos veröffentlichen, Beiträge anderer posten und kommentieren. Andere Nutzer können an der eigenen Pinnwand ebenfalls öffentlich Beiträge hinterlassen. Neben diesem öffentlichen – also tatsächlich für alle anderen Nutzer einsehbaren – Nachrichtenaustausch gibt es auch die Möglichkeit, sich private Nachrichten zu schicken oder sich im Chat auszutauschen.

Nutzer können sich in sog. **Gruppen** organisieren, Veranstaltungen erstellen und diese teilen, Seiten oder Beiträge liken, Apps nutzen u. v. m. Laut den Allgemeinen Geschäftsbedingungen ist die Nutzung des Netzwerks erst ab dem Alter von 13 Jahren erlaubt. Es findet allerdings keine Altersverifikation bei der Anmeldung statt: d. h. der Nutzer kann das Geburtsdatum frei eingeben und das Alter wird nicht überprüft.

Geschäftsmodell

Seit dem Börsengang im Sommer 2012 gehört das Unternehmen Facebook Inc. einem Konglomerat von Anteilseignern. Als Gründer und **Chief Executive Officer** (CEO) nimmt Mark Zuckerberg auch weiter hin eine besondere Stellung im Unternehmen ein, das seinen Hauptsitz in Menlo Park (Kalifornien) hat. Weitere größere Zweigstellen unterhält das Unternehmen u. a. in New York, Tokio, Stockholm und Dublin. Facebook ist ein kommerzielles Unternehmen, dessen Haupteinnahmequelle Werbeanzeigen sind. Werbung in Facebook gibt es in verschiedenen Formen, z. B. werden Werbeanzeigen am rechten Rand der eigenen Facebook-Seite oder auch direkt im Nachrichtenstrom angezeigt. Diese „Werbeplätze" verkauft Facebook an Werbekunden. Für Werbetreibende ist der große Vorteil von Facebook gegenüber anderen Seitenbetreibern, dass das Unternehmen seine Nutzer sehr genau kennt, denn diese teilen freiwillig viele persönliche Informationen auf ihrem Profil mit. Auf dieser Datenbasis kann Facebook seinen Werbekunden anbieten, ihre Werbung passgenau ohne große Streuverluste an eine Zielgruppe auszuliefern:



Quelle: eigener Screenshot, Facebook Zielgruppe;
Stand: 30.10.2014

Die Daten der Nutzer lassen sich so in bares Geld umwandeln. Anfang 2013 verzeichnete Facebook Werbeeinnahmen von 1,33 Milliarden Euro. 23 % davon entfielen auf Mobil-Werbung d. h. Werbeeinblendungen für mobile Endgeräte, denn ein Großteil der Facebook-Nutzer greift von ihrem Smartphone oder Tablet auf das Netzwerk zu[10]. Zusatzprogramme, wie Spiele oder Umfragen, werden in der Regel von Drittanbietern zur Verfügung gestellt, die im Falle der Nutzung auf das Profil zugreifen können. Deshalb ist es wichtig, bei der Auswahl der Spiele und Anwendungen vorsichtig zu sein.

Aus der Praxis
Die SchülerInnen der älteren Jahrgangsstufen am Elsa-Brändström Gymnasium in Oberhausen veranstalten als „Medienscouts" ein Stationenlernen zu Facebook. Zielgruppe sind die jüngeren MitschülerInnen, aber auch im Rahmen von Elternabenden kommt diese Methode bei alle Beteiligten gut an.

Tipp: *Für Spiele und andere Anwendungen, die über Facebook aktiviert werden, kann eingesehen werden, auf welche persönlichen Informationen die ausgewählte Anwendung Zugriff verlangt. Dies ist direkt vor, aber auch noch nach der Installation bzw. Aktivierung möglich. Anwendungen, die zu neugierig sind, sollten gelöscht oder erst gar nicht aktiviert werden.*

Kritik an Facebook und Co

In einem Interview 2010 sagte Mark Zuckerberg: „People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time."[11] Damit trat der Chef von Facebook eine breite Diskussion über das Konzept des Schutzes persönlicher Daten im digitalen Zeitalter los, die bis heute nicht an Brisanz verloren hat. Nach wie vor steht auch Facebooks unzureichende Datenschutz-Politik in der Kritik. Das Thema ist heikel, denn eine aktive Nutzung des Sozialen Netzwerks setzt ein gewisses Maß an Freigiebigkeit bezüglich persönlicher Daten voraus. Dennoch ist das Ausmaß der Berechtigungen, die sich Facebook über die Daten seiner Nutzer bei der Registrierung einräumt, aus datenschutzrechtlicher Perspektive problematisch:

> *„Für Inhalte wie Fotos und Videos, die unter die Rechte an geistigem Eigentum (sog. ‚IP-Inhalte') fallen, erteilst du uns durch deine Privatsphäre- und App-Einstellungen die folgende Erlaubnis: Du gibst uns eine nicht-exklusive, übertragbare, unterlizenzierbare, gebührenfreie, weltweite Lizenz zur Nutzung jeglicher IP-Inhalte, die du auf oder im Zusammenhang mit Facebook postest (‚IP-Lizenz'). Diese IP-Lizenz endet, wenn du deine IP-Inhalte oder dein Konto löschst, außer deine Inhalte wurden mit anderen Nutzern geteilt und diese haben die Inhalte nicht gelöscht."*[12]

Damit räumen die Nutzer Facebook weitgehende Zugriffsrechte ein: Auf Inhalte von Posts, Fotos, Videos, Profilinformationen etc.

Trends

Soziale Netzwerke und Anwendungen wie **Facebook** oder **WhatsApp** erfreuen sich bei Jugendlichen und Erwachsenen großer Beliebtheit. Abgesehen von den etablierten Diensten kommen in immer kürzeren Abständen neue Dienste auf den Markt (z. B. Snapchat), während andere verschwinden (z. B. schülerVZ, werkenntwen). So hatte schülerVZ 2010 noch über 6 Millionen jugendliche Nutzer, musste aber drei Jahre später eingestellt werden, da die Nutzer zu Facebook abwanderten[13]. Man kann feststellen, dass der Trend weg von Angeboten führt, die eine große Bandbreite an Funktionen für ihre Nutzer bereitstellen (s. werkenntwen) hin zu kleinen, simplen Anwendungen, die einen speziellen Zweck erfüllen, wie z. B. Snapchat, Instagram etc. Facebook hat diesen Trend erkannt und mit dem Kauf von Instagram (2012) und WhatsApp (2014) darauf reagiert.

Beliebte Dienste/Tools 2015
Diese Dienste und Tools waren 2015 bei Jugendlichen besonders beliebt:

- **Instagram:** Eine kostenlose Foto- und Video-Anwendung für Smartphones, mit der man Bilder nicht nur bearbeiten, sondern auch umgehend für andere im Internet veröffentlichen kann.
- **Snapchat:** Ein Instant-Messenger, mittels dem Fotos an **Freunde** versendet werden können. Das Besondere bei Snapchat: Diese Fotos sind für den Adressaten max. 10 Sekunden sichtbar und werden dann – laut dem Anbieter – automatisch gelöscht. Allerdings gibt es technische Möglichkeiten, die Fotos dennoch zu speichern!
- **Tumblr:** Eine Blogging-Plattform, auf der Texte, Bilder, Zitate, Links und Videos veröffentlicht werden können. Andere Nutzer dürfen die Inhalte auf ihrer Seite dann nochmals bloggen.
- **Pinterest:** Ein Soziales Netzwerk, das das Veröffentlichen von Bildern zum Inhalt hat. Die Nutzer können ihre Bilder „pinnen" d. h. veröffentlichen. Andere Nutzer können diese dann teilen, kommentieren oder ihr Gefallen ausdrücken.
- **Ask.fm:** Eine Website, auf der Nutzer sich gegenseitig Fragen stellen – auch anonym – und darauf antworten. Die Profile bei angemeldeten Nutzern sind immer für alle (auch nicht-angemeldete Nutzer) sichtbar! Immer wieder gab es Fälle von Cyber-Mobbing und auch sexueller Belästigung durch anonyme Kommentare.
- **Quizduell:** Ein kleines Quiz-Spiel, bei dem der Spieler zu einer Frage vier Antwortmöglichkeiten erhält und daraus die Richtige wählen muss. Es besteht außerdem die Möglichkeit, gegen andere Personen – Freunde und Fremde – spielen zu können.
- Andere **Casual Games: Angry Birds, Paper Toss, Doodle Jump, Plants vs. Zombies, Fruit Ninja** oder **Jewels** sind nur einige Beispiele beliebter Spiele-Apps, die sich bei vielen Jugendlichen auf dem Smartphone finden.
- **Smileys waren gestern :-(** Beliebt für die verschiedensten Kommunikationsmöglichkeiten, wie z. B. WhatsApp und Facebook sind die kleinen Bilder, die **Emoji** genannt werden. Diese gibt es in allen erdenklichen Formen und Farben und können in jeden Text integriert werden. Hier dienen sie als zusätzlicher Zeichensatz:

Quelle: eigener Screenshot, Facebook-Emoji; Stand: 30.10.2014

Links und weiterführende Informationen

Webseite

www.lfm-nrw.de/fileadmin/lfm-nrw/Forschung/LfM-Band-62.pdf
Studie zur Rolle des Web 2.0 im Alltag von Jugendlichen und jungen Erwachsenen.

Endnoten

[1] ONLINE COMMUNITY (2015). *Aus Cambridge University Press. Dictionaries Online.* Aufgerufen am 26.03.2015 unter http://dictionary.cambridge.org/dictionary/business-english/online-community?q=online-communityimm

[2] EL DIFRAOUI, A. (2011, 3. November). *Die Rolle der neuen Medien im Arabischen Frühling* (Abs. 5). Aufgerufen am 21.10.2014 unter http://www.bpb.de/internationales/afrika/arabischer-fruehling/52420/die-rolle-der-neuen-medien

[3] MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.) (2015). *JIM-Studie 2015, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland* (S. 32). Aufgerufen am 04.01.2016. http://www.mpfs.de/fileadmin/JIM-pdf15/JIM_2015.pdf

[4] SCHMIDT, J.-H., Paus-Hasebrink, I. & Hasebrink, U. (2011). *Heranwachsen mit dem Social Web.* Aufgerufen am 21.10.2014 unter http://www.lfm-nrw.de/fileadmin/lfm-nrw/Forschung/LfM-Band-62.pdf

[5] MEKONET KOMPAKT (2010) *Intimität im Netz auf einen Blick,* Grimme-Institut Marl Aufgerufen am 12.05.2015 unter http://www.grimme-institut.de/handreichungen/pdf/mekonet_kompakt_intimitaet.pdf

[6] BLECH, J. et al. (2009, 02. März). *Nackt unter Freunden.* Der Spiegel 2009 (10) (S. 126)

[7] SCHMIDT, J.-H., Paus-Hasebrink, I. & Hasebrink, U. (2011). *Heranwachsen mit dem Social Web. Zur Rolle von Web 2.0-Angebote im Alltag von Jugendlichen und jungen Erwachsenen.* Aufgerufen am 21.10.2014 unter http://www.lfm-nrw.de/fileadmin/lfm-nrw/Forschung/LfM-Band-62.pdf

[8] SCHMIDT, J. (2011, 20. April). *Das Like-Problem. Was Facebooks Gefällt-Mir-Buttons verraten.* Aufgerufen am 21.10.2014 unter http://www.heise.de/security/artikel/Das-verraet-Facebooks-Like-Button-1230906.html

[9] MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.) (2015). *JIM-Studie 2015, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland.* Aufgerufen am 12.01.2016 unter http://www.mpfs.de/fileadmin/JIM-pdf15/JIM_2015.pdf

[10] FOCUS.DE. (2013, 31. Januar). *Facebook schafft den Weg aus der mobilen Falle.* Aufgerufen am 29.10.2014 unter http://www.focus.de/finanzen/news/unternehmen/deutlich-mehr-werbeeinnahmen-facebook-schafft-den-weg-aus-der-mobilen-falle_aid_909522.html

[11] MATYSZCZYK, C. (2010, 10. Januar). *Zuckerberg: I know that people don't want privacy.* (Abs. 4). *CNET.* Aufgerufen am 26.03.2015 unter http://www.cnet.com/news/zuckerberg-i-know-that-people-dont-want-privacy/

[12] FACEBOOK (2015, 30. Januar). *Erklärung der Rechte und Pflichten* (Abs. 10). Aufgerufen am 26.03.2015 unter https://www.facebook.com/legal/terms?locale=de_DE

[13] RÄTH, G. (2013, 9. April). *SchülerVZ ist endgültig tot. gruenderszene.de.* Aufgerufen am 30.10.2014 unter http://www.gruenderszene.de/news/schulervz-offline-bildervz

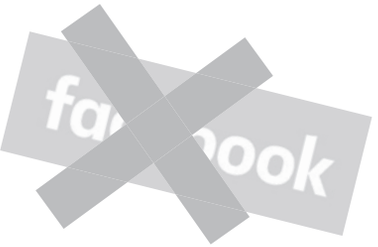
Arbeitsblatt	**AB 1**	**AB 2**
Titel	**Facebook-Verbot für Laura**	**Welche Nutzungsmotive gibt es für Facebook?**
Kompetenzen	Die Schülerinnen und Schüler setzen sich in einem Rollenspiel mit den Vor- und Nachteilen von Social Communitys auseinander.	Die Schülerinnen und Schüler vergleichen Zitate zur Beschreibung von Facebook-Nutzungsmotiven und setzen sie in Bezug zu ihren eigenen Erfahrungen.
Methoden	Rollenspiel	Textarbeit, Stufenleiter
Material	Arbeitsblatt, Kärtchen	Arbeitsblatt
Zeit (in Minuten)	90 (evtl. länger)	45
Zugang Internet/PC	ja	nein

Hinweise für die Durchführung

AB 1: Facebook-Verbot für Laura	Die Schülerinnen und Schüler sollen in Form eines Rollenspiels die Vor- und Nachteile von Social Communitys wie Facebook diskutieren. Dazu nutzen sie in einem ersten Schritt die Stichworte aus der Tabelle, die einige Nutzungsmotive und Herausforderungen darstellen. Die fünf Rollen sollten etwa gleich groß besetzt sein. Wenn es innerhalb der Gruppe keine Einigung auf den „Rollenspieler" bzw. die „Rollenspielerin" gibt, sollten Sie den Zufall entscheiden lassen (dies aber vorher kommuniziert haben!). Wichtig bei dieser Methode ist die Reflexion im Anschluss, bei der alle Beteiligten ein methodisches und inhaltliches Feedback geben dürfen, aber auch die Distanzierung der Spieler von ihren Rollen ist enorm wichtig. Achten Sie darauf, dass die Spielerinnen und Spieler nicht „Ich" sagen, sondern „Die Mutter war der Meinung..." o. ä.
AB 2: Welche Nutzungsmotive gibt es für Facebook?	Einige Begriffe wie „Teilhabe" oder „Identitätsbildung" werden Sie erläutern müssen. Trotzdem bietet das Arbeitsblatt mit diesen sechs Zitaten einen guten und knappen Überblick über die Nutzungsmotive einer Social Community wie Facebook. Die Stufenleiter dient der eigenen Beurteilung der Motive und ihrer Gewichtung, der Zeitungsartikel im letzten Arbeitsauftrag soll eine kreative Form der Darstellung ermöglichen. Schülerinnen und Schüler, die selbst kein Facebook nutzen, übertragen die Aufgabe auf WhatsApp oder stellen sich vor, sie würden Facebook nutzen! **Quellenangaben:** [1] Schmidt, J-H. et al. (2010). *Heranwachsen mit dem Social Web.* Aufgerufen am 30.10.2014 unter http://www.hans-bredow-institut.de/de/node/2482 [2] mekonet kompakt. (2010). *Intimität im Netz auf einen Blick.* Aufgerufen am 30.10.2014 unter http:/www.mekonet.de/t3/uploads/media/mekonet_kompakt_intimitaet-im-netz2012.pdf [3] Sloterdijk, P. (2009). *Fremde Freunde – Vom zweifelhaften Wert digitaler Beziehungen.* Der Spiegel, 10 [4] Wippermann, P. im Interview (k. A.). (2012, 1. Februar). *heute-Journal* [Nachrichtenmagazin]. Mainz: Zweites Deutsches Fernsehen. [5] Laird, S. (2012). *Why do People use Facebook?* [6] Bauer, J. (2010). *Interview-Titel „Lob der Schule"*

Lust auf mehr?
Beide Arbeitsblätter lassen sich mit wenigen Anpassungen auf weitere Angebote anwenden, so zum Beispiel auf Dienste wie Instagram, Snapchat, Ask.fm usw.

Facebook-Verbot für Laura!



„Oh je! Jetzt ist es passiert!“ stöhnt Laura morgens in der Schule in Richtung ihrer besten Freundin Zehra. „Meine Mutter verbietet mir Facebook! Die ist total unter schlechten Einfluss geraten und hat gestern so eine Fernsehsendung gesehen, wo Jugendliche als Kommunikationszombies auf Droge ‚Internet‘ dargestellt wurden! Dazu kam noch mein Onkel – der ist so voll der Datenschützer! Zehra tippt weiter auf ihrem Handy herum, während sie sagt: „So ein Unsinn! Mache ihr klar, wie sehr unser Bewusstsein erweitert und unsere Freundschaft durch Facebook vertieft wird!“ und muss dabei laut lachen.

Stelle dir vor, es kommt am Nachmittag zu einem Gespräch zwischen Laura, ihren Eltern, Zehra und dem Onkel.

Arbeitsaufträge:

1. Bitte teilt euch in etwa gleich große Gruppen auf:

Laura	Zehra	Mutter	Vater	Onkel

2. Überlegt euch innerhalb der Rollen, wie ihr sie spielen wollt.
   Erstellt euch eine kurze Rollenkarte, auf die ihr die grundlegende Meinung zur Facebook-Nutzung von Jugendlichen schreibt.
   Bei Mutter, Vater und Onkel dürft ihr euch Vornamen und Berufe ausdenken, bei Laura und Zehra könnt ihr Hobbies / Lieblingsbeschäftigungen notieren.

3. Erstellt euch neun Kärtchen zu folgenden Stichworten. Notiert darauf, was es bei jedem Stichwort Positives und Negatives zu sagen gibt (nur so könnt ihr in der Diskussion auf diese Argumente reagieren!). Dazu müsst ihr vielleicht einige der Themen noch genau im Internet nachschauen.

Dabei sein wollen / Gruppenzwang	Der LIKE-Button und Kommentare	Cyber-Mobbing (zum Beispiel Beleidigungen)
Weitergabe persönlicher Daten / Sicherheitseinstellungen	Freunde und Freundschaften	Unterhaltung und Freizeitbeschäftigungen
Chronik mit privaten Fotos	Kommunikation mit den Klassenkameraden	Werbung auf Facebook

4. Wählt in der Gruppe eine Person aus, die die Rolle spielt (dabei ist es egal, ob Junge oder Mädchen). Führt das Rollenspiel durch!

5. Bitte macht danach unbedingt eine Runde, bei der jede Rolle sagen darf, wie sie sich gefühlt hat und das Publikum sagen kann, ob das Spiel realistisch war.

6. Wertet das Spiel danach aus: Welche Argumente wurden gebracht?
   Wie wurde Facebook dargestellt? Was ist das Schöne daran?
   Was ist problematisch für Jugendliche an Facebook?

Welche Nutzungsmotive gibt es für facebook?

Jan-Hinrik Schmidt[1]:
Soziale Netzwerke werden vor allem aus folgenden Gründen genutzt:
- Selbstdarstellung
- Teilhabe und Beziehungspflege durch Vernetzung

Mekonet[2]:
Der „Nutzen- und Belohnungsansatz": Medien werden zur Befriedigung von Wünschen und Bedürfnissen genutzt, nach:
- Unterhaltung
- Orientierung, Identitätsbildung
- Teilhabe, Zugehörigkeit und Soziale Unterstützung
- Selbstdarstellung und Anerkennung

Sam Laird[5]:
Wir alle wollen ein Teil von etwas sein!

Peter Sloterdijk[3]:
„Der Rückzug von den anderen, das Alleinseindürfen, das ist eine große Errungenschaft. Aber der Mensch ist auch ein Stammeswesen. Diese Netzwerke können beides glücklich vereinen: Man bleibt vom lästigen, vom aufsässigen anderen verschont, und doch ist der ganze Stamm immer anwesend."

Peter Wippermann[4]:
„Es dreht sich um mediales „Kraulen". Nicht was ich jemandem erzähle ist wichtig, sondern dass ich etwas erzähle ... dass ich noch wahrgenommen werde von meiner Umwelt"

Joachim Bauer[6]:
Menschen haben Bedeutungshunger.

Arbeitsaufträge:

1. Ihr dürft in Partnerarbeit arbeiten. Bitte erklärt euch gegenseitig kurz die sechs Aussagen der sechs Autoren. Belegt sie mit eigenen Beispielen!

2. Übertrage – zunächst alleine – die drei (für dich!) wichtigsten Aussagen in eine Stufenleiter, wobei das Wichtigste oben steht. Erklärt euch dann gegenseitig warum diese Nutzungsmotive so wichtig sind!

3. Macht eine kurze Umfrage in der Klasse und erstellt eine Übersicht an der Tafel: Welches der Motive ist für die meisten am wichtigsten / am unwichtigsten?

4. Diskutiert diese Übersicht in der Klasse!

5. Weshalb nutzen über eine Milliarde Menschen Facebook? Kläre das Phänomen mit eigenen Worten in Form eines Zeitungsartikels über Facebook und baue (wenn es passt) die Nutzungsmotive der Autoren ein.
   Hast du noch eigene Gründe (= Nutzungsmotive), die noch nicht genannt wurden? Wenn ja, erkläre sie bitte!

YouTube: Ein Nutzerkonto für alles

Das Google-Universum
Bei dem Wort „Google" denken wohl die meisten sofort an die beliebte Suchmaschine. Google ist jedoch weit mehr als das: Das Unternehmen bietet zahlreiche weitere Anwendungen – meist kostenlos – an, darunter auch YouTube:

- Suchmaschine Google
- Google Chrome (Browser)
- Google Maps
- Gmail
- YouTube
- Google+
- Google Books
- Google Earth
- Google Alerts
- Google Kalender
- Google Docs
- Google Übersetzer
- Hangouts
- Google Groups
- Google Keep
- u.w.m

Aus datenschutzrechtlicher Sicht ist problematisch, dass alle Anwendungen mit einem einzigen Benutzerkonto verknüpft sind: Mit ein und demselben Konto werden in YouTube Filme eingestellt, andere Filme kommentiert, über Gmail E-Mails erstellt, versendet und empfangen, Kalendereinträge erstellt, mittels der Suchmaschine gesurft etc. All diese Daten können durch das eine Konto mit einem bestimmten Nutzer verknüpft werden. Google weiß demnach viel über die Nutzer seiner Anwendungen. Dieses Wissen ist geldwert, denn auf dieser Basis lässt sich Werbung an eine sehr genau definierte Zielgruppe richten. Nicht umsonst verzeichnete Google 2013 50,58 Milliarden US $ Werbeumsätze[1].

Tipp: Um zu vermeiden, dass die Daten der unterschiedlichen Anwendungen nutzerspezifisch miteinander verknüpft werden können, sollten Anwendungen unterschiedlicher Anwender genutzt werden – also nicht alles aus nur einer Hand.
Werden vorwiegend Google-Anwendungen genutzt, hat man unter **www.google.com/dashboard** *die Möglichkeit, die Daten, die man durch die Nutzung der Anwendungen generiert, zu überblicken.*

YouTube

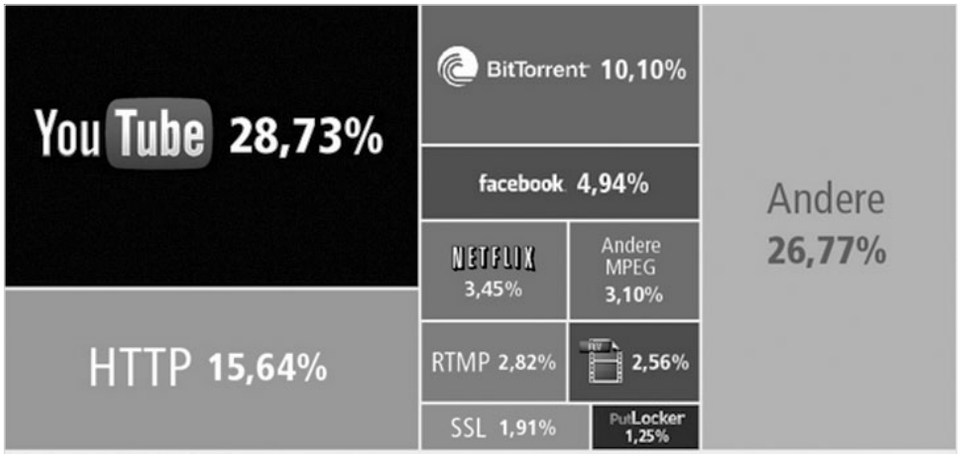
Von Null auf eine Milliarde
YouTube wurde im Februar 2005 von drei ehemaligen PayPal-Mitarbeitern, Chad Hurley, Steve Chen und Jawed Karim, gegründet. Das erste YouTube-Video wurde im April 2005 eingestellt und zeigt Jawed Karim 18 Sekunden lang vor einem Elefantengehege. Rund anderthalb Jahre später, im Oktober 2006, verkauften sie den Dienst für 1,65 Milliarden Euro an den Google-Konzern[2].

Der Begriff „Tube" bezeichnet in den U.S.A. den Fernseher, vergleichbar mit dem deutschen Begriff der „Röhre". Mit dem vorangestellten „You" bedeutet YouTube sinngemäß „Du sendest". Der Name des Dienstes ist Programm und mittlerweile ist YouTube „die" Video-Plattform schlechthin, auf der Tausende Nutzer Videos ansehen, kommentieren und eigene Videos veröffentlichen. Hier einige Zahlen aus dem Frühjahr 2015[3]:

- YouTube verzeichnet mehr als eine Milliarde Nutzer.
- Pro Minute werden durchschnittlich 300 Stunden neues Videomaterial hochgeladen.
- Jeden Tag werden auf YouTube Videos mit einer Gesamtdauer von mehreren hundert Millionen Stunden wiedergegeben.
- YouTube gibt es in 75 Ländern und in 61 Sprachen.
- Die Hälfte der Videoaufrufe wird über mobile Geräte generiert.

Aufgrund der hohen Nutzer- und Nutzungszahlen verwundert es nicht, dass YouTube Spitzenreiter der europäischen Download-Traffics ist:

YouTube ist der größte Traffic-Fresser Europas
Zusammensetzung des europäischen Download-Traffics bei maximaler Auslastung, nach Anwendung*



* Stand: September 2013. Nur Festnetz-Internet.

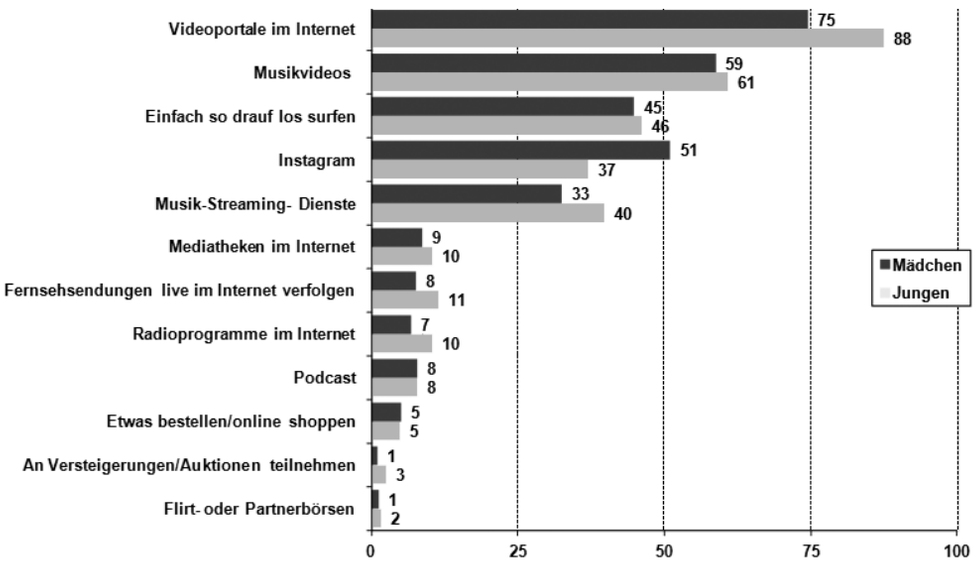
Quelle: Richter (2013)[4]

Das Geschäftsmodell
Mit dem Motto „Erst Masse, dann Kasse" waren und sind viele Internet-Firmen kommerziell erfolgreich. Dahinter steckt die Idee, das Angebot zunächst kostenlos und eventuell sogar werbefrei zu halten, bis eine kritische Masse an Nutzern erreicht wird. Erst dann beginnt die Kommerzialisierung – oft zunächst behutsam, um die Nutzer daran zu gewöhnen.
In Deutschland blendet YouTube seit Mitte 2008 Werbung auf sog. **Partner-Seiten** ein. Diese „Partner" sind prozentual an den Werbeeinnahmen beteiligt, weshalb sich einige Nutzer erfolgreich über ihre Filme finanzieren können. Seit der Einführung dieses Models gibt es kurze Werbeeinblendungen vor dem Start eines Videos und außerdem Bannerwerbung. Seit Mai 2013 ist YouTube – zunächst nur in den U.S.A. – in das klassische Geschäft des Pay-TV eingestiegen und bietet bestimmte Kanäle gegen eine monatliche Gebühr zwischen 1 und 8 Dollar an. Der Unterschied zum klassischen Fernsehen besteht darin, Sendungen zu jeder Zeit, also „on demand" sehen zu können. Sendungen von **National Geographic Kids** sind bspw. nur noch über diesen Weg zu sehen. Abgerechnet wird über das Google-eigene Bezahlsystem **Google Wallet**.

Das YouTube-Konto
Wer sich Videos auf YouTube ansehen möchte, kann dies ohne eine Anmeldung tun. Ein Konto ist jedoch dann erforderlich, wenn ein Nutzer Videos auf YouTube veröffentlichen, Videos kommentieren oder Videos mit Altersbeschränkung ansehen möchte. Durch die Registrierung bei YouTube, erhält der Nutzer ein Konto, das bei YouTube **Kanal** heißt, und hat nun zugleich ein Google-Konto. Eine Anmeldung bei YouTube ist deshalb natürlich auch mit einem bereits bestehenden Google-Konto möglich. Es gibt zahlreiche Kanäle von Personen, Firmen, Gruppen, Institutionen etc. auf YouTube. Schon längst haben Unternehmen die „Röhre" als Werbemedium entdeckt und nutzen sie intensiv. Die Kanäle können von anderen (angemeldeten) Nutzern kostenlos abonniert werden. Dann werden beim Log-in auf YouTube sofort die neuesten Videos und Benachrichtigungen angezeigt.

YouTube und Co – beliebt bei jugendlichen Nutzern
Bei Jugendlichen stehen Videoportale wie YouTube, Clipfish, MyVideo, Sevenload, vimeo oder dailymotion hoch im Kurs: Laut JIM-Studie 2015 nutzten drei Viertel der befragten Jugendlichen Videoportale zur Unterhaltung:

Tätigkeit im Internet/am Computer – Schwerpunkt: Unterhaltung 2015
– Täglich / mehrmals pro Woche –



Quelle: MPFS (2015). JIM 2015, Angaben in Prozent, Basis: alle Befragten, n=1.200[5]

Mit YouTube haben sich neue, einfache Möglichkeiten aufgetan, Videos an ein großes Publikum zu verbreiten. Manche aktive YouTube-Nutzer, die regelmäßig eigene Beiträge einstellen – sog. **YouTuber** – genießen einen regelrechten Kultstatus und haben Tausende jugendliche Fans, die sehnsüchtig auf das nächste Video warten. Dieses wird dann innerhalb weniger Stunden oft hunderttausendfach aufgerufen. Zu den unter Jugendlichen beliebten YouTubern gehören z. B.:

- **Y-Titty:** Comedy-Trio, das Stars aus Musik- und Filmbusiness auf die Schippe nimmt.
  Zu finden unter:
  https://www.youtube.com/user/YTITTY/featured
- **Gronkh:** Ein YouTuber, der v. a. mit Erklärungen und Kommentaren zu Videospielen erfolgreich ist.
  Zu finden unter:
  www.youtube.com/user/gronkh
- **LeFloid:** YouTuber, der aktuelle Ereignisse aufgreift und in seinen Videos diskutiert. Zu finden unter:
  www.youtube.com/user/lefloid
- **Die Aussenseiter:** Comedy-Duo, das sich humorvoll mit sehr unterschiedlichen Themen auseinandersetzt. Zu finden unter:
  www.youtube.com/user/DieAussenseiter
- **PietSmiet:** Ein Team mehrerer YouTuber, die mit Erklärungen und Kommentaren zu Videospielen sehr erfolgreich sind. Zu finden unter:
  www.youtube.com/user/PietSmittie
- **BibisBeautyPalace:** Ihre Fans begeistert Bianca Heinicke mit ihren Tutorials über Make-up und Trendfrisuren, Lifestyle und die neuesten Modetrends.
  https://www.youtube.com/user/BibisBeautyPalace
- **Dagi Bee:** DagiBee, deren Kanal neben Tutorials, Haul-Videos, Mode und Lifestyle auch Parodien über alltägliche Probleme beinhaltet.
  https://www.youtube.com/user/Dagibeee

Quelle: eigener Screenshot, YouTube/LeFloid, Stand: 01.05.2014

Erklärvideos zum Lernen

Neben einer Plattform für unterhaltsame Videos hat sich YouTube auch als Plattform für Erklärvideos etabliert. Zu vielen schulischen, aber auch anderen Themen finden sich teils hochprofessionell erstellte Videos. Nicht wenige SchülerInnen nutzen YouTube, um für die Schule zu lernen. Berühmt geworden ist die **Kahn Academy** des Amerikaners Salman Khan. Diese Akademie ist eine gemeinnützige Organisation, die Videos zu Themen der Mathematik, Biologie, Physik, Chemie etc. im Internet frei verfügbar macht. Zu finden unter:
www.youtube.com/user/KhanAcademyDeutsch

Aus der Praxis

Als Alternative zu einem klassischen Referat ist ein Erklärvideo gut geeignet. Diese Videos können, sofern der Urheber damit einverstanden ist bzw. keine Rechte verletzt werden, veröffentlicht werden. Das ist im Einzelfall schwierig zu beurteilen und sicher ist man eigentlich nur, wenn die Arbeit komplett auf die Darstellung anderer Personen verzichtet, sowie Bild und Musik sicher legal verwendet werden dürfen. Das abzuklären ist aber auch ein wichtiges Lernziel!

Problematik bei YouTube

Problematische Inhalte

Es ist unmöglich, alle Inhalte zu kontrollieren, die von den Millionen von YouTube-Nutzern tagtäglich hochgeladen werden. Aus diesem Grund kommt es immer mal wieder vor, dass sich auch problematische Inhalte in Videos finden lassen, wenngleich in den Community-Richtlinien festgehalten ist, keine unangemessenen Inhalte einzustellen. Diese Inhalte können direkt bei YouTube gemeldet und letztlich auch entfernt werden. Es ist dennoch wichtig, Kinder und Jugendliche im Umgang mit YouTube für diese Problematik zu sensibilisieren.

Problematisch sind u. a. folgende Inhalte[6]:

- pornografisch oder sexuell eindeutig
- rassistisch oder anders diskriminierend
- Misshandlungen von Tieren
- Drogenmissbrauch
- Anleitung zum Bau einer Bombe
- drastische oder grundlose Gewalt
- Videos / Bilder mit Unfällen und Leichen oder
- Stalking, Drohungen, Verletzung der Privatsphäre

Nutzungsrechte

Mit dem Upload eines Videos räumt der Nutzer YouTube weitreichende Rechte an den Inhalten ein:

„10. Rechte, die Sie einräumen
10.1 Indem Sie Nutzerübermittlungen bei YouTube hochladen oder posten, räumen Sie

A. *YouTube eine weltweite, nicht-exklusive und gebührenfreie Lizenz ein (mit dem Recht der Unterlizenzierung) bezüglich der Nutzung, der Reproduktion, dem Vertrieb, der Herstellung derivativer Werke, der Ausstellung und der Aufführung der Nutzerübermittlung im Zusammenhang mit dem Zur-Verfügung-Stellen der Dienste und anderweitig im Zusammenhang mit dem Zur-Verfügung-Stellen der Webseite und YouTubes Geschäften, einschließlich, aber ohne Beschränkung auf Werbung für und den Weitervertrieb der ganzen oder von Teilen der Webseite (und auf ihr basierender derivativer Werke) in gleich welchem Medienformat und gleich über welche Verbreitungswege;*

B. *jedem Nutzer der Webseite eine weltweite, nicht-exklusive und gebührenfreie Lizenz ein bezüglich des Zugangs zu Ihren Nutzerübermittlungen über die Webseite sowie bezüglich der Nutzung, der Reproduktion, dem Vertrieb, der Herstellung derivativer Werke, der Ausstellung und der Aufführung solcher Nutzerübermittlung in dem durch die Funktionalität der Webseite und nach diesen Bestimmungen erlaubten Umfang.“*[7]

Unter den sog. **Nutzerübermittlungen** sind alle nutzergenerierten Inhalte zu verstehen. Das umfasst sowohl das Videomaterial (Nutzervideos) als auch die Nutzerkommentare. YouTube und damit Google Inc. darf all das somit ohne Rückfrage und Honorar anderweitig nutzen.

Urheberrecht
Web 2.0-Angebote, also Angebote, die Nutzern die Veröffentlichung eigener Inhalte ermöglichen, sind aus Perspektive des Urheberrechts nicht ganz unproblematisch: Aufgrund der Menge der eingestellten Inhalte ist es für den Anbieter nicht möglich, gänzlich alle Inhalte auf Urheberrechtsverletzungen hin zu kontrollieren. Aus diesem Grund kommt es immer wieder vor, dass sich YouTube mit Urheberrechtsverletzungen konfrontiert sieht, wenngleich das Unternehmen in seinen Nutzungsbedingungen die Achtung des Urheberrechts vorsieht. So waren die Medienkonzerne Viacom und Warner Music Group in langjährige Rechtsstreitigkeiten mit YouTube verwickelt. In beiden Fällen ging es um Urheberrecht verletzende Nutzeruploads auf die Videoplattform[8,9].

Vor diesem Hintergrund wurde und wird die Frage diskutiert, inwieweit der Betreiber eines Internet-Portals für die Inhalte haftbar gemacht werden kann, die nicht er selbst, sondern Nutzer veröffentlichen. Das Landgericht Hamburg entschied 2012, dass YouTube nicht hauptverantwortlich für Inhalte seiner Nutzer sei, aber stärker darauf achten müsse, welche Videos eingestellt würden. Diese Maßgabe sei z. B. durch technische Maßnahmen, wie Wortfilter, erfüllt. Mit diesen Filtern sollen Lieder durchsucht werden, die von der **Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte** (GEMA) als urheberrechtlich geschützt markiert wurden.

Derzeit setzt YouTube, wie viele andere Netzwerke auch, vorwiegend auf Kontrolle durch die Nutzer selbst – sozus. auf die Selbstreinigung. Videos, die z. B. das Urheberrecht verletzen, können von Nutzern gemeldet werden. Daraufhin erfolgt eine Prüfung durch Mitarbeiter von YouTube, die einige Tage in Anspruch nehmen kann, bevor eine Reaktion erfolgt.

Tipp:
YouTube bietet eine umfangreiche Infoseite über die Sicherheit auf der Video-Plattform an. Das sog. ***Sicherheitscenter*** *ist zu finden unter:*
www.youtube.com/yt/policyandsafety/de/safety.html

Politische Relevanz von YouTube
Die Möglichkeit der Nutzer, sich über ein selbst erstelltes YouTube-Video an gesellschaftspolitischen Diskussionen zu beteiligen und die eigene Meinung kundzutun, ist nicht in allen Ländern gern gesehen. YouTube wurde und wird – wie auch Twitter und Facebook – in einigen Ländern zensiert.

Links und weiterführende Informationen

Webseiten

http://www.klicksafe.de/themen/kommunizieren/youtube/
Hintergrundinfos zum Thema YouTube bei klicksafe.

http://www.klicksafe.de/themen/kommunizieren/youtube/youtube-szene-die-wichtigsten-youtuberinnen/
Infos über die wichtigsten YouTuberInnen bei klicksafe

https://www.youtube.com/playlist?list=PL3VDIS0fyb0nEGqRsVnKyaDhqXrTVGVrf
Youtube-Kanal des ServiceBureau Jugendinformation Bremen YouTube - Expedition in eine fremde Welt (für Erwachsene)

http://www.scoop.it/t/youtube-by-servicebureau
Viele interessante Artikel zu YouTube.

www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Suchmaschine/Zusatz_AB_Suchmaschinen.pdf
Unterrichtsmaterialien zum Thema Suchmaschinen mit umfassendem Infoteil.

www.google.de/intl/de/safetycenter/families/start/
Google stellt für Eltern eine Reihe von Informationen zum Google-Konto bereit, die auch die Aspekte Jugendschutz, bewusstes Surfen und das eigene Identitätsmanagement umfassen.

Endnoten

[1] STATISTA. (2014, k. A.). *Höhe der Werbeumsätze von Google von 2001 bis 2013* (in Milliarden US-Dollar). Aufgerufen am 03.11.2014 unter http://de.statista.com/statistik/daten/studie/75188/umfrage/werbeumsatz-von-google-seit-2001/

[2] KRÖGER, M. (2006, 10. Oktober). *YouTube-Verkauf: Der Club der Millionäre.* Spiegel Online. Aufgerufen am 03.11.2014 unter http://www.spiegel.de/wirtschaft/youtube-verkauf-der-club-der-millionaere-a-441871.html

[3] YOUTUBE (2014, k. A.). *Statistiken.* Aufgerufen am 26.03.2015 unter http://www.youtube.com/yt/press/de/statistics.html

[4] RICHTER, F. (2013, 15. November). *YouTube ist der größte Traffic-Fresser Europas* (Abs. 5). Aufgerufen am 26.03.2015 unter http://de.statista.com/infografik/1628/die-groessten-trafficfresser-europas/

[5] MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.) (2015). *JIM-Studie 2015, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland* (S. 34). Aufgerufen am 04.01.2016. http://www.mpfs.de/fileadmin/JIM-pdf15/JIM_2015.pdf

[6] YOUTUBE (2014). *YouTube-Community-Richtlinien.* Aufgerufen am 03.11.2014 unter https://www.youtube.com/t/community_guidelines

[7] YOUTUBE (2015). *Nutzungsbedingungen* (Abs. 48). Aufgerufen am 26.03.2015 unter https://www.youtube.com/t/terms

[8] MARTINSON, J. (2006, 13. Oktober). *Google faces copyright fight over YouTube.* theguardian. Aufgerufen am 10.11.2014 unter http://www.theguardian.com/business/2006/oct/13/digitalmedia.citynews

[9] RUSHE, D. (2014, 18. März). *Google and Viacom settle major copyright case after years of litigation.* theguardian. Aufgerufen am 10.11.2014 unter http://www.theguardian.com/technology/2014/mar/18/google-viacom-settle-copyright-case-years-of-litigation

[10] KUHN, J. (2014). *YouTube in der Filter-Falle.* Sueddeutsche.de. Aufgerufen am 26.03.2015 unter http://www.sueddeutsche.de/digital/urteil-im-gema-streit-youtube-in-der-filter-falle-1.1338111

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Broadcast yourself**	**Google, Google, Google**
Kompetenzen	Die Schülerinnen und Schüler erkennen die Möglichkeiten von YouTube für das schulische Lernen.	Die Schülerinnen und Schüler ermitteln die kostenlosen Angebote des Google-Konzerns und hinterfragen sie kritisch auf Finanzierung und Datenschutz.
Methoden	Video-Analyse, Präsentation	Internet-Recherche
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Broadcast yourself	YouTube ist eine unter Pädagogen manchmal unterschätzte Möglichkeit für das schulische Lernen. Zu sehr vielen Unterrichtsthemen gibt es sehr gute Erklär-Videos, die von engagierten Menschen, oftmals auch Lehrerinnen und Lehrern, hergestellt und (kostenlos) veröffentlicht werden. Ein Blick lohnt sich also. Aber… wie immer bei der Fülle im Netz, muss hier der kritische Blick bleiben und eine Video-Analyse, vor allem auch inhaltlich zur Überprüfung der Richtigkeit der Informationen, ist notwendig. Nach der Pflicht könnten Sie eine Kür einbauen und die Schülerinnen und Schüler selbst ein Erklär-Video erstellen lassen. Die Technik ist über die Kameras und Schnitt-Möglichkeiten in den Schüler-Handys sowie YouTube-interne Schnittmöglichkeiten vorhanden.
AB 2: Google, Google, Google	Mit diesem Arbeitsblatt sollen die Schülerinnen und Schüler einen Blick hinter die Kulissen von Google werfen. Vielleicht aktualisieren Sie die vorhandene Liste mit einem Blick auf die Google-Seiten, denn der Konzern ist eine dynamische Technologie-Firma mit immer neuen Ideen. Über all diesen Angeboten steht immer wieder die Frage, wie sie kostenlos sein können und gleichzeitig für Google so gewinnbringend. Dazu dienen die Fragen, die in der Präsentation beantwortet werden sollen. Gleichzeitig sollen die Fragen eine rein technische und vielleicht allzu unkritische Darstellung verhindern.

Lust auf mehr?

- YouTuber als Berufsmodell? Wie man mit YouTube Geld verdienen kann erfahren die Schüler in dem Video des hauptberuflichen TechChanel-YouTubers Felix Bahlinger (Chanel Felixba):
  www.youtube.com/watch?v=eCLvx-KfVZw
  Sammlung: Welche problematischen Aspekte werden genannt?
- Themenspecial über YouTube und Kommerzialisierung unter
  www.klicksafe.de/themen/kommunizieren/youtube/
- Google arbeitet ständig an neuen Produkten und gibt dies auf der Seite
  http://research.google.com/ bekannt. Hier könnten die Schülerinnen und Schüler weiterarbeiten und einen Blick in die Zukunft werfen.

Broadcast yourself

Bestimmt kennt ihr das Videoportal YouTube und andere Portale wie MyVideo, Daily Motion, Vimeo oder Clipfish. Aber wusstet ihr, dass ihr diese Videoportale auch für die Schule nutzen könnt?

Arbeitsaufträge:

1. Partnerarbeit: Sucht euch zwei Videos aus, die euch interessieren, und schaut sie euch an.

- Geschichte/Kleinstaaten in Europa:
  http://tinyurl.com/7cup9lc
- Biologie/Mendelsche Regeln:
  http://tinyurl.com/nqua5xj
- Sport/Parcours im Sportunterricht:
  http://tinyurl.com/cjq62rl
- Hauswirtschaft/Stricken lernen:
  http://tinyurl.com/yz467rl
- Mathe/Winkel messen und zeichnen:
  http://tinyurl.com/ck65l4d
- Musik/Gitarre lernen:
  http://tinyurl.com/cjxncsj
- Erste Hilfe:
  http://tinyurl.com/nmzkn25
- ITG/Computer: Einrichten von Lesezeichen am Beispiel des Browsers Mozilla Firefox:
  http://tinyurl.com/c2fywg3
- Und noch etwas Witziges:
  http://tinyurl.com/cfucxhr
  http://tinyurl.com/63427z

2. Sucht nach folgenden Fragen. Findet ihr Erklärungen auf YouTube?
   a) Was ist der Satz des Pythagoras?
   b) Wie ist das Herz des Menschen aufgebaut?
   c) Wie wird das Past Perfect Simple im Englischen gebildet?
   d) Wie wird das Komma bei Aufzählungen gesetzt?

Projektvorschlag:
Produziert selbst in Gruppen ein Lernvideo und stellt es den anderen Schülern zur Verfügung. Ihr könnt es auch bei YouTube online stellen. Dann müsst ihr aber auf folgende Dinge achten:

- die Bildrechte der Beteiligten (haben alle, die im Video vorkommen, ihr Einverständnis gegeben?)
- ein sinnvolles Tagging (die Auswahl von Begriffen, die den Inhalt eurer Videos beschreiben, damit sie über die Suchfunktion zu finden sind)
- überlegt euch, ob ihr das Video unter Creative-Commons-Lizenz veröffentlichen wollt – Informationen über Creative Commons: **http://de.creativecommons.org/was-ist-cc/**

Google, Google, Google

Schon längst ist Google viel mehr als eine einfache Suchmaschine. Der Konzern **Google Incorporated** mit Sitz in Kalifornien wurde 1998 von Larry Page und Sergey Brin gegründet und hat sich seitdem zu einem weltweiten Motor für Internet-Technologien entwickelt.

Hier kannst du Google etwas besser kennenlernen … und auch einen kritischen Blick auf das Unternehmen werfen.

Arbeitsaufträge:

1. Google hat zahllose Anwendungen entwickelt, die in der Regel kostenlos für den Nutzer sind. Bitte sucht euch jeweils zu zweit eine Google-Anwendung aus und recherchiert dazu.

Suchmaschine Google	Google Chrome	Google Maps	Gmail
YouTube	Google+	Google Books	Google Earth
Google Alerts	Google Kalender	Google Docs	Google Übersetzer
Hangouts	Google Groups	Google Keep	?
?	?	?	?

Bei den Fragezeichen in der Liste könnt ihr ein Produkt auswählen, das noch nicht genannt wurde. Die Produkte findet ihr unter: **www.google.de/intl/de/about/products**

2. Erstellt eine kurze Präsentation für die anderen und beantwortet darin folgende Fragen: Ist diese Anwendung kostenlos? Wenn nein, wie teuer ist sie? Wenn ja, wird Werbung eingeblendet?
   - a) Wozu dient die Anwendung?
   - b) Ist sie kostenlos? (Wenn nein, wie teuer ist sie?)
   - c) Wie wird sie finanziert?
   - d) Ist eine Anmeldung mit persönlichen Daten notwendig? (Wenn ja, mit welchen?)
   - e) Was erfährt Google über mich bei der Nutzung?

3. Google verlangt von seinen Nutzern, ein Konto einzurichten, das dann für alle Anwendungen genutzt werden kann. Macht folgendes Gedankenexperiment: Willi ist ein Google-Fan und nutzt fast ausschließlich Google-Anwendungen. Erstellt – zunächst in Partnerarbeit, dann an der Tafel – eine Liste mit Daten, die Google möglicherweise über Willi erfahren kann.

4. Diskutiert in der Klasse die Frage, welche Macht Google dadurch erlangt und inwieweit dies problematisch sein könnte.

Tipp:
Es gibt Alternativen zu Suchmaschinen mit Datenhunger: Zum Beispiel Startpage:
https://startpage.com/deu/
und DuckDuckGo
https://duckduckgo.com/

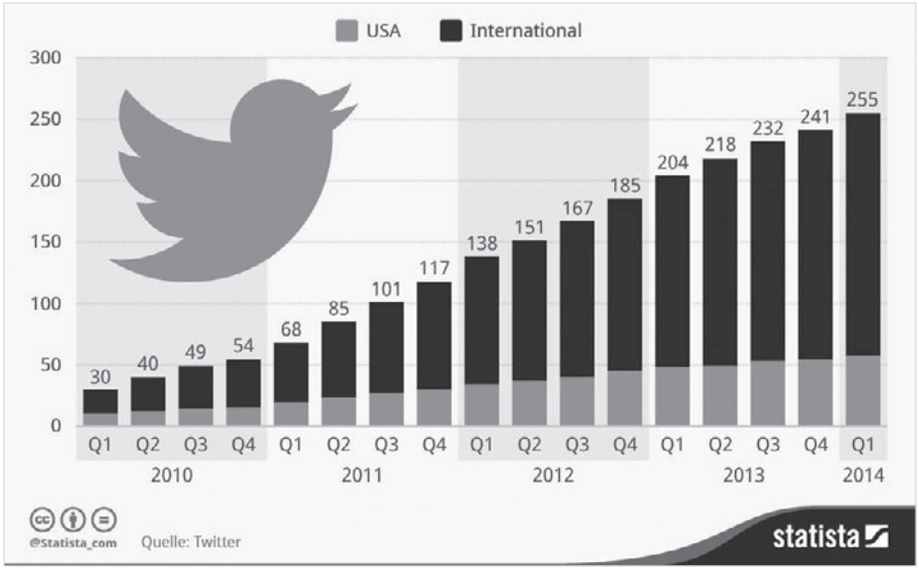
Mikroblog: Twitter

Blogs (Abkürzung von Weblog), eine Art Online-Tagebuch, sind ein inzwischen weit verbreitetes und bekanntes Phänomen. Das Wort **Mikroblog** bezeichnet eine in diesem Sinne kleine Version eine Blogs, bei dem der Autor eine sehr begrenzte Zeichenzahl (meist unter 200 Zeichen) zur Verfügung hat. Diese Tatsache ist dem Grundgedanken geschuldet, einen Mikroblog möglichst von überall und auch unterwegs betreiben zu können.[1] Einer der bekanntesten Mikroblogs ist Twitter.

Twitter – Zahlen und Fakten

Jeder kennt den kleinen blauen Vogel, doch kaum einer weiß, dass er „Larry" heißt und dass er nach dem ehemaligen Basketballspieler der Boston Celtics, Larry Bird, benannt wurde[2]. Larry ist das Symbol für den kostenlosen Dienst **Twitter**, der 2006 von Jack Dorsey, Biz Stone, Evan Williams und Noah Glass in San Francisco gegründet wurde. Der Name leitet sich ab von dem englischen Verb „to twitter", das im Deutschen mit „zwitschern" übersetzt werden kann. Über Twitter können Kurznachrichten mit einer max. Länge von 140 Zeichen versendet werden. Die Nachrichten richten sich an einen Kreis von anderen Twitter-Nutzern, die als **Follower**, zu Deutsch „Folgende" oder „Anhänger" bezeichnet werden. Anfang 2014 hatte Twitter schon über 250 Millionen aktive Nutzer, wobei 77 % der Twitter-Accounts außerhalb der U.S.A. angemeldet sind:

25 % mehr Nutzer im 1. Quartal 2014
Anzahl der monatlich aktiven Nutzer von Twitter (in Mio.)

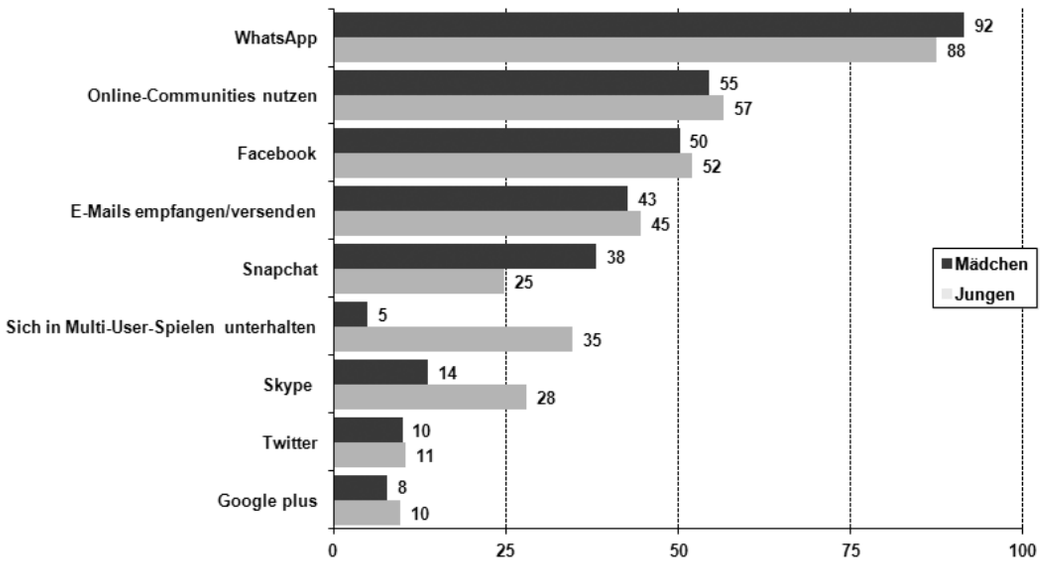


Quelle: statista (2014)[3]

Besonders viele Follower hatten im Januar 2016 Prominente wie Katy Perry (ca. 80 Millionen), Justin Bieber (ca. 73 Millionen) oder Barack Obama (68 Millionen), nachzulesen unter **http://twitaholic.com/** Hier werden regelmäßig die 100 Twitterer mit den meisten Followern aufgelistet.

Bei den deutschen Jugendlichen ist Twitter derzeit eher ein Randphänomen: Nur wenige Prozent der befragten Jugendlichen nutzen laut der Studie **Jugend, Information, (Multi-)Media** (JIM-Studie) Twitter:

Aktivitäten im Internet – Schwerpunkt: Kommunikation 2015
– Täglich / mehrmals pro Woche –



Quelle: MPFS (2015). Angaben in Prozent; Basis: alle Befragten, n=1.200 [4]

Das kleine Twitter-Lexikon
Folgende Begriffe sind wichtig, um die Funktionen und Funktionsweisen des Dienstes verstehen und nutzen zu können:

- **Tweet:** Eine Nachricht, die über Twitter übermittelt wird.
- **Retweet:** Die Weiterleitung des Tweets einer anderen Person an die eigenen Follower (s. u.). Erkennbar ist ein Retweet an dem vorangestellten „RT".
- **Twitterer/Tweeps:** Die Nutzer von Twitter, die aktiv Nachrichten verschicken. Die Nutzer können sich einen Twitter-Nutzernamen wählen, der an dem vorangestellten „@"-Zeichen, z. B. @klicksafe, erkennbar ist.
- **Hashtag:** Ist ein zusammengesetzten Wort aus den englischen Begriffen „hash" (deutsch: Doppelkreuz #) und „tag" (deutsch: markieren). Mit einem Hashtag können in Twitter (aber auch in Facebook oder Pinterest) Schlagworte gekennzeichnet werden, um die Suche innerhalb des Netzwerks zu erleichtern. In einen Tweet können beliebig viele Hashtags gesetzt werden.
- **Follower:** Die Twitter-Nutzer, die einem Twitterer folgen und dessen Tweets (kostenlos) abonniert haben. Sie können also bspw. @klicksafe abonnieren und erhalten dann automatisch alle Nachrichten, die von diesem Nutzer versendet werden.
- **Favoriten:** Dies ist eine Form der Bewertung, ähnlich wie das Liken bei Facebook. Damit kann ein Tweet gekennzeichnet werden, um deutlich zu machen, dass man diesen für bedeutsam erachtet. Retweets und Favoriten werden von Twitter statistisch ausgewertet.
- **Direktnachricht:** Nicht jeder Tweet muss sofort an alle Twitter-Nutzer gesendet werden. Direktnachrichten sind als Form der privaten Twitter-Kommunikation nur für eine Person bestimmt.

Privatsphäre und Datenschutz
Bei der Registrierung erteilt der Nutzer Twitter die Erlaubnis, die Tweets weiterzuverwenden und auch an Dritte weiterzugeben:

„Sie behalten die Rechte an allen Inhalten, die Sie über die Dienste übermitteln, veröffentlichen oder anzeigen. Durch Übermittlung, Veröffentlichung oder Anzeigen von Inhalten über die Dienste gewähren Sie uns eine weltweite, nicht exklusive, unentgeltliche Lizenz (mit dem Recht zur Unterlizenzierung), diese Inhalte in sämtlichen Medien und über sämtliche Verbreitungswege, die gegenwärtig bekannt sind oder in Zukunft bekannt sein werden, zu verwenden, zu vervielfältigen, zu reproduzieren, zu verarbeiten, anzupassen, abzuändern, zu veröffentlichen, zu übertragen, anzuzeigen und zu verbreiten."[5]

Neben dem Inhalt eines Tweets, speichert Twitter noch andere Daten. So z. B.:

- die Account-Daten mit allen Profil-Informationen
- Jede Änderung der E-Mail-Adresse im Zusammenhang mit Twitter
- die Anzahl der Tweets und deren Inhalte
- die Favoriten
- die Direkt-Nachrichten
- die Kontakte, die im Twitter-Account importiert wurden
- die Follower des Accounts und die Accounts denen man folgt
- die Listen (selbst erstellte und abonnierte bzw. in denen man auftaucht)
- die Suchanfragen
- die Logins in den Account mit IP-Adresse
- die Logins per Handy
- die Facebook-Verbindungen
- hochgeladene Bilder

Tipp:
*Die Initiative **privacy international** hält einen Vordruck bereit, mit dem man die Daten, die Twitter von einer Person gespeichert hat, anfordern kann **(s. Links und weiterführende Materialien)!***
*Dringend abzuraten ist von einer Funktion namens **Geotag.** Mittels Geotag wird jeder einzelne Tweet mit einer Ortsangabe versehen. Somit ist leicht nachzuverfolgen, wo sich eine Person wann aufgehalten hat – ganze Bewegungsprofile lassen sich damit erstellen.*

Gesellschaftliche Bedeutung von Twitter
Twitter ist für einige Menschen mehr als ein bloßer Zeitvertreib. In der Zeit des Arabischen Frühlings bspw. hatte der Dienst eine hohe politische Relevanz, denn abseits der staatlichen Medien konnten so Informationen z. B. über stattfindende Demos geteilt werden. El Difraoui hält fest: „Blogs und Foren befeuerten die Umbrüche in der arabischen Welt, die neuen Medien wurden zum Mittel der Selbstermächtigung"[6].

Neben seiner politischen Bedeutung spielt Twitter auch im zunehmenden Maß für die Forschung eine Rolle – insbesondere in den Sozialwissenschaften: Über Dienste wie Twitter, haben Forscher Zugriff auf eine große Datenmenge. Ein Beispiel: Forscher der Cornell-Universität in Ithaca haben Millionen Tweets nach Wörtern analysiert, um herauszufinden in welcher Stimmung sich die Tweeter beim Verfassen ihrer Nachrichten befanden. Sie stellten fest, dass die überwiegende Zahl der Nutzer morgens, v. a. aber kurz vor Mitternacht gute Laune hat[7].

Links und weiterführende Informationen

Webseite

www.privacyinternational.org/blog/what-does-twitter-know-about-its-users-nologs
Eine britische Wohltätigkeitsorganisation, die sich für den Datenschutz einsetzt. Auf ihrer Webseite findet sich ein Formular, mit dessen Hilfe von Twitter die gespeicherten Daten einer Person angefordert werden können.

Endnoten

[1] MIKROBLOG (2012, 07. November). Aufgerufen am 26.12.2015 unter http://social-media-abc.de/index.php?title=Mikroblog

[2] GOLIJAN, R. (2012, 28. Februar). *The Twitter bird has a name: Larry.* NBS news. Aufgerufen am 26.03.2015 unter http://www.today.com/money/twitter-bird-has-name-larry-235179

[3] STATISTA. (2014, 29. Juli). *24 % mehr Nutzer im 2. Quartal 2014* (Abs. 2). Aufgerufen am 30.10.2014 unter http://de.statista.com/infografik/1518/monatlich-aktive-nutzer-von-twitter-weltweit/

[4] MEDIENPÄDAGOGISCHER MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.) (2015). *JIM-Studie 2015, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland* (S. 32). Aufgerufen am 04.01.2016. http://www.mpfs.de/fileadmin/JIM-pdf15/JIM_2015.pdf

[5] TWITTER. (2014, 8. September). *Allgemeine Geschäftsbedingungen* (Abs. 5). Aufgerufen am 26.03.2015 unter https://twitter.com/tos

[6] EL DIFRAOUI, A. (2011, 2. November). *Die Rolle der neuen Medien im Arabischen Frühling* (Abs. 2). bpb. Aufgerufen am 26.03.2015 unter http://www.bpb.de/internationales/afrika/arabischer-fruehling/52420/die-rolle-der-neuen-medien

[7] DAMBECK, H. (2011, 29. September). *Tweet-Analyse: Twitter-Nutzer sind abends am besten drauf* (Abs. 6). spiegel.de. Aufgerufen am 26.03.2015 unter http://ml.spiegel.de/article.do?id=788448

Methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1**	**AB 2**
Titel	**Zwitschern mit Larry**	**Twitter für Newbies**
Kompetenzen	Die Schülerinnen und Schüler beschreiben eine Statistik zur Nutzung von Twitter aus der JIM-Studie und ermitteln im Gespräch die Unterschiede zur Nutzung bei Jugendlichen und Erwachsenen.	Die Schülerinnen und Schüler übertragen die Tabelle mit typischen Begriffen zur Benutzung von Twitter auf Plakate.
Methoden	Statistik-Analyse	Museumsgang
Material	Arbeitsblatt	Arbeitsblatt, Plakate (mind. DIN A3), dicke Stifte
Zeit (in Minuten)	45	90
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Zwitschern mit Larry	Twitter ist noch immer ein Erwachsenen-Phänomen, was sich aber leicht ändern kann. Die Schülerinnen und Schüler sollen hier Zahlen zur Nutzung von Twitter bei Jugendlichen kennenlernen und auswerten. In einem zweiten Schritt soll analysiert werden, warum bislang Erwachsene Twitter eher nutzen als Jugendliche. Die Twitter-Integration der Live-Stream-App Periscope ist für jugendliche Nutzer wahrscheinlich interessant. Über Periscope können Nutzer ihr Smartphone dazu nutzen, um selbst Live-Videoaufnahmen direkt ins Netz zu streamen. Über Vor- und Nachteile soll nach einer kurzen Internet-Recherche diskutiert werden. Abschließend haben die Schüler, die Twitter nutzen, die Möglichkeit, Lieblings-Hashtags oder Lieblings-Twitterer vorzustellen.
AB 2: Twitter für Newbies	Dieses Arbeitsblatt ist im Prinzip eine Fleiß-Recherchearbeit zu Twitter und den wichtigsten Begriffen rund um dieses Angebot. Vielleicht lassen Sie die Schülerinnen und Schüler selbst aus den sechs Möglichkeiten wählen und steigern so die Motivation. Die Methode Museumsgang beinhaltet, dass die Plakate alle in einem Raum aufgehängt werden. Der Präsentator / die Präsentatorin der jeweiligen Gruppe steht vor dem Plakat und erläutert – wie ein Museumsführer – das Plakat.

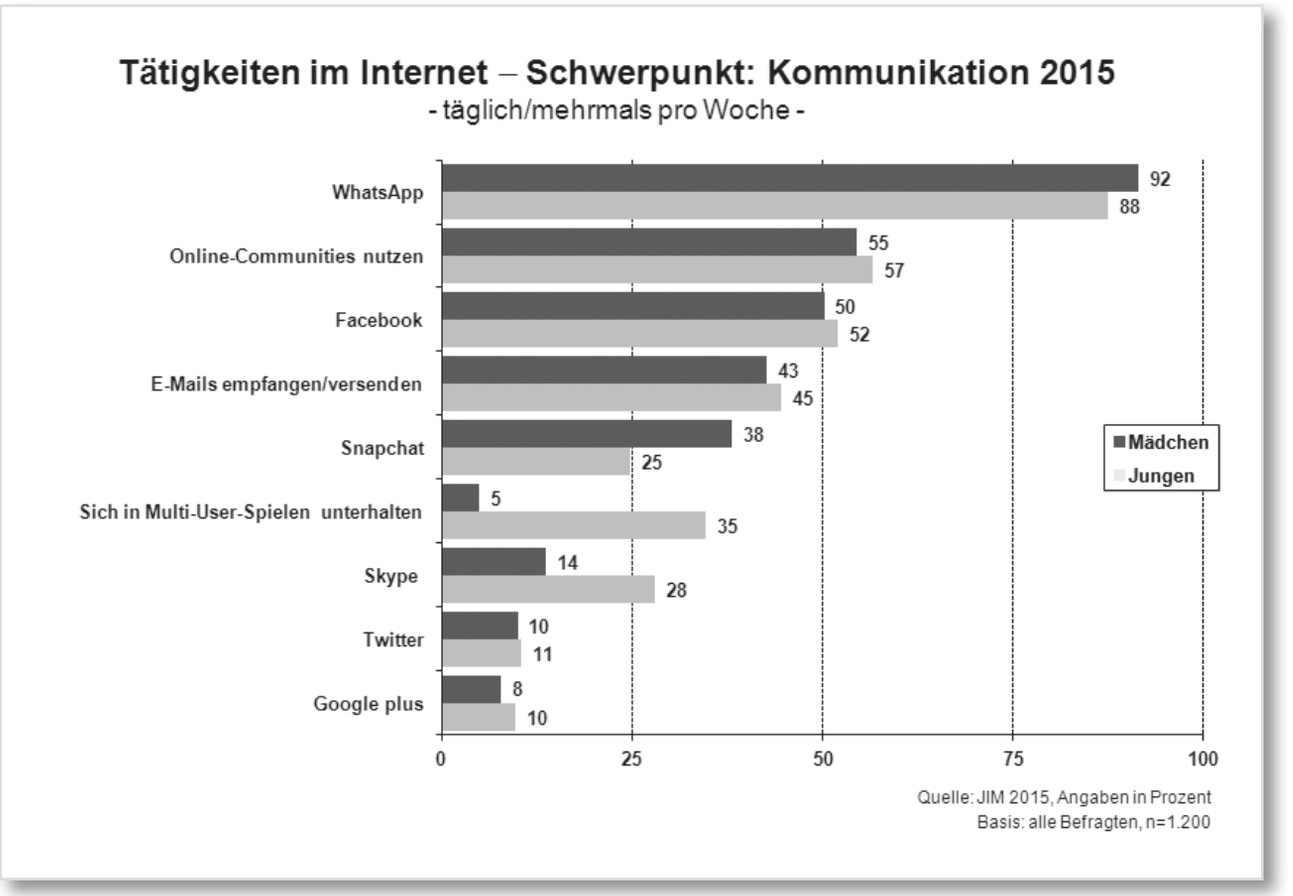
Lust auf mehr?

- Die Video-Plattform Vine, auf der Kurz-Videos von max. 6 Sekunden gepostet werden, wird ebenfalls von Twitter Inc. betrieben. Schauen Sie sich mit Ihren Schülern einige der sehr gut gemachten kurzen Kunstwerke auf **https://vine.co/** an. Die Produktion von „Vine-Videos" für den Kunstunterricht wäre sicherlich sehr interessant.
- Die Zahlen rund um die Angebote wie Twitter werden auch immer in Form von nett aufbereiteten Statistiken dargeboten. Schauen Sie doch mal unter „Internet-Minute" in einer Bildersuche (bei Google oder Bing bspw.) nach. Hier könnten die Schülerinnen und Schüler die Zahlen überprüfen oder selbst eine ähnliche Darstellung anfertigen.

Zwitschern mit Larry

Jeder kennt den kleinen blauen Vogel, doch kaum einer weiß, dass er „Larry" heißt und seinen Namen dem ehemaligen Basketballspieler Larry Bird verdankt. Die Rede ist natürlich von dem Symbol des Dienstes **Twitter,** der 2006 gegründet wurde. Der Name Twitter kommt von dem englischen Verb „to twitter", das im Deutschen mit „zwitschern" übersetzt wird.

Unter deutschen Jugendlichen ist Twitter noch nicht so verbreitet, wie folgende Statistik aus der JIM-Studie 2015 zeigt:



MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.). (2015).
JIM-Studie 2015, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland.

Arbeitsaufträge:

1. Bitte beschreibt das Diagramm aus der JIM-Studie möglichst genau. Fasst die wichtigsten Ergebnisse zusammen!
2. Unter Erwachsenen ist Twitter beliebt. Warum nicht auch bei Jugendlichen? Notiert Ideen dazu an der Tafel und diskutiert sie. Könnt ihr hier zustimmen?
3. Über die Live-Stream-App Periscope können Twitter-Nutzer Live Streams senden und empfangen. Informiert euch über Vor- und Nachteile dieser Anwendung.
4. Kennt ihr Twitterer oder auch Hashtags #, die ihr besonders toll findet? Stellt sie den anderen vor.

Twitter für Newbies

Twittern gehört unter Prominenten mittlerweile zum guten Ton. Viele Fußballspieler der deutschen Nationalelf twittern, viele Schauspieler und Politiker ebenso. Insgesamt hat Twitter etwas über 300 Millionen aktive Nutzer (Stand: 2015), die ihre Nachrichten verbreiten oder solche empfangen.

Hier kannst du Twitter etwas besser kennenlernen.

Arbeitsaufträge:

1. Bitte sucht euch mithilfe der Leitfragen und Arbeitsaufträge eines der folgenden Themen aus. Ihr dürft ganz nach Eurem Interesse auswählen!

2. Stellt das Thema auf einem Plakat dar!

	Begriffe	Beliebtheit	AGB	Datenschutz	Twitaholics	Politik
Leitfragen	Was bedeutet „Tweet", „Hashtag" und die anderen Twitter-Begriffe.	Wer nutzt Twitter und wie oft?	Was steht unter „Ihre Rechte" in den Allgemeinen Geschäftsbedingungen?	Welche Daten speichert Twitter über mich? Was sind „Geotags"?	Wer sind die fleißigsten Twitterer mit den meisten Followern?	Wann und für wen spielte Twitter eine große politische Rolle?
Arbeitsaufträge	Erstellt ein kleines Twitter-Glossar!	Recherchiert die aktuellen Nutzungszahlen und stellt sie anschaulich dar!	Stellt die Nutzungsbedingungen mit eigenen Worten kurz dar!	Fasst die Ergebnisse in einer Liste zusammen und erklärt sie!	Erstellt eine Auflistung mit maximal 10 Namen!	Nehmt zwei Ereignisse der letzten Jahre und zeigt die Bedeutung von Twitter!

3. Bereitet euch in der Gruppe auf einen **Museumsgang** vor. Dabei hängen alle Plakate im Klassenraum. Alle dürfen reihum die Plakate besuchen und die Erläuterungen hören (wechselt euch an eurem Plakat ab, jeder soll mindestens einmal erläutern!).

5|1 Jugendmedienschutz
5|2 Urheberrecht und Open Content

5

Was wir kennen sollten: Recht und Gesetze im Internet!

Jugendmedienschutz

Der Jugendmedienschutz in Deutschland
Der Jugendmedienschutz in Deutschland ist in mehreren rechtlichen Texten verankert. Diese sind im Einzelnen:

- **Jugendschutzgesetz** (JuSchG)[1]
- **Jugendmedienschutz-Staatsvertrag der Länder** (JMStV)[2]
- **Strafgesetzbuch** §§ 86, 86a, 130a, 131, 184 bis 184c (StGB)[3]

Im StGB finden sich Verbreitungsverbote zu besonders gravierenden rechtsverletzenden Inhalten, wie z. B. Propaganda, Kinderpornografie etc. Das JuSchG greift bei Inhalten, die auf sogenannten **Trägermedien** vorliegen, wie bspw. CDs, DVDs, Blu-Rays etc. Der JMStV gilt für sogenannte **Telemedien.** Darunter sind Onlinemedien, wie etwa Webseiten, Online-Spiele etc. zu verstehen. Die Zuteilung, welche Medien dem JuSchG und welche dem JMStV unterliegen, ist nicht immer einfach: bspw. im Falle eines Computerspiels, das erst auf CD auf den Markt kommt und dann als Online-Version erscheint. Abhängig davon, ob das Spiel ein Träger- oder ein Telemedium ist, sind jeweils andere Institutionen mit dessen Bewertung befasst. Zudem gelten etwas andere rechtliche Maßgaben. Das liegt daran, dass die Bestimmungen des JuSchG und des JMStV in einigen Punkten nicht deckungsgleich sind. Aufgrund der Konvergenz der Medien sind diese Abweichungen im Grunde nicht länger sinnvoll zu rechtfertigen. Das ist einer der Gründe, weshalb die Überarbeitung des JMStV, der bereits seit 2003 in Kraft ist, nun angedacht ist.

In Deutschland gewährleistet ein komplexes System bestehend aus verschiedenen Institutionen den Jugendmedienschutz. Wichtig sind v. a. die anerkannten Einrichtungen der Freiwilligen Selbstkontrolle.
In diesen Einrichtungen legen Anbieter ihre Inhalte, wie Filme oder Spiele, unabhängigen Experten zur Prüfung vor. Eine Ausnahme bilden Onlineangebote (s. u.). Die Aufgaben und Handlungsbefugnisse der Selbstkontrolleinrichtungen sind sowohl im JMStV als auch im JuSchG festgelegt. Folgende Institutionen sind im Bereich des Jugendmedienschutzes relevant:

- **Freiwillige Selbstkontrolle Kino (FSK)**
  Die FSK ist die älteste Selbstkontrolleinrichtung. Sie besteht bereits seit 1949 und prüft Kinofilme, aber auch Filme oder Serien, die auf DVD, Blu-Ry etc. erscheinen. Diese versieht die FSK auf Basis des JuSchG mit einer Altersfreigabe (0, 6, 12, 16, 18 Jahre). Die Entscheidungen der FSK wirken sich bspw. auf die Sendezeit von Filmen aus. Die Webseite der FSK ist zu finden unter: **www.fsk.de**

- **Freiwillige Selbstkontrolle Fernsehen (FSF)**
  Auf Basis des JMStV prüft die FSF Fernsehsendungen auf ihre Jugendmedienschutzrelevanz hin und vergibt Altersfreigaben (0, 6, 12, 16, 18 Jahre). Auch ihre Altersfreigaben wirken sich auf die Sendezeit von Filmen aus. Grundsätzlich gilt: Hat die FSK einen Kinofilm mit einer Alterskennzeichnung versehen und läuft dieser Film dann später auch im Fernsehen, gilt die Kennzeichnung der FSK. Die Webseite der FSF ist zu finden unter:
  www.fsf.de

- **Freiwillige Selbstkontrolle Multimediale Diensteanbieter (FSM)**
  Die FSM ist zuständig für die Prüfung von Onlinemedien, d. h. für Webseiten, Videoportale, Blogs etc. Die FSM prüft Onlineinhalte, über die eine Beschwerde vorliegt. Diese kann auch von Nutzern eingereicht werden. Ist der Inhalt jugendschutzrechtlich bedenklich, nimmt die FSM Kontakt zum Anbieter und zu der Landesmedienanstalt des Bundeslandes Kontakt auf, in denen der Anbieter sitzt, und wirkt so auf die Beseitigung des problematischen Inhalts hin. In besonders schwerwiegenden Fällen, bspw. bei Kinderpornographie, leitet die FSM diese gleich an die Strafverfolgungsbehörden weiter. Die Webseite der FSM ist zu finden unter: **www.fsm.de**.
  Die FSM ist international mit Partnern vernetzt, um bei problematischen Seiten, die im Ausland gehostet sind, handeln zu können. Nicht immer sind die Zuständigkeiten bei Web-inhalten klar, denn mittlerweile gibt es sowohl die USK online als auch die FSK.online.

- **Unterhaltungssoftware Selbstkontrolle (USK)**
  Die USK ist zuständig für die Bewertung von Computerspielen. Sie versieht Spiele auf Grundlage des JMStV mit einer Alterskennzeichnung (0, 6, 12, 16, 18 Jahre), die für die Warenverkäufer verbindlich ist. So wird verhindert, dass Kinder/Jugendliche Spiele kaufen können, die nicht für ihre Altersgruppe geeignet sind. Die Webseite der USK ist zu finden unter: **www.usk.de**

- **Bundesprüfstelle für jugendgefährdende Medien (BPjM)**
  Aufgabe der BPjM ist es, Inhalte – Trägermedien und Telemedien – daraufhin zu prüfen, ob diese in die Liste jugendgefährdender Medien aufgenommen werden müssen. Dieser Vorgang heißt **Indizierung.** Spiele, Filme, Webseiten etc., die indiziert sind, dürfen Kindern nicht zugänglich sein. Inhalte, die bereits durch USK oder FSK eine Altersfreigabe erhalten haben, dürfen nicht indiziert werden. Die Webseite der BPjM ist zu finden unter:
  www.bundespruefstelle.de

- **Kommission für jugendgefährdende Medien (KJM)**
  Die KJM ist die höchste Aufsichtsinstanz für Rundfunk und Telemedien. Sie prüft in Problemfällen, die seitens einer Landesmedienanstalt oder jugendschutz.net (s. u.) an sie weitergereicht werden, ob ein Verstoß gegen den JMStV vorliegt. Die KJM ist zuständig für die Anerkennung der Selbstkontrolleinrichtungen und der Jugendschutzprogramme. Derzeit existieren vier anerkannte Programme: **JusProg, die Telekom Kinderschutz Software** und seit dem 11. März 2015 auch **SURF SITTER Plug & Play** sowie **SURF SITTER für den PC**. Die KJM kann zudem Anträge an die BPjM stellen, Angebote zu indizieren und bezieht zu den Indizierungsanträgen der BPjM Stellung.
  Die Webseite der KJM ist zu finden unter:
  www.kjm-online.de

- **jugendschutz.net**
  jugendschutz.net ist organisatorisch an die KJM angegliedert und ist damit befasst, das Internet proaktiv auf problematische Inhalte hin zu durchforsten. Gleichzeitig nimmt jugenschutz.net auch Beschwerden von Nutzern entgegen. Die Webseite von jugdenschutz.net ist zu finden unter:
  www.jugendschutz.net

Jugendgefährdende Inhalte

Entwicklungsbeeinträchtigung und -gefährdung
Die Frage, was jugendgefährdende Inhalte sind, mag offensichtlich scheinen, mitunter ist das aber gar nicht so leicht zu klären. Laut Gesetz sind das Inhalte, die „geeignet sind, die Entwicklung von Kindern und Jugendlichen oder ihre Erziehung zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit zu beeinträchtigen" (§ 14 Abs. 1 JuSchG). Konkret können das Inhalte sein, die verrohend wirken, zu Verbrechen, Gewalttätigkeit etc. animieren, pornografisch sind etc. Je nachdem, wie drastisch die Darstellungen sind, werden sie grundsätzlich in drei Kategorien unterschieden:

Absolut verboten	Relativ verboten	Entwicklungsbeeinträchtigend
→ Inhalte sind grundsätzlich untersagt	→ Inhalte dürfen Minderjährigen nicht zugänglich gemacht werden	→ Inhalte sind nur für bestimmte Altersgruppen problematisch & dürfen nur unter bestimmten Auflagen verbreitet werden (z. B. Altersverifikation).
z. B. ■ **Harte Pornographie** *(§§ 184a, 184b StGB)* ◆ Kinderpornographie ◆ Gewaltpornographie ◆ Sexuelle Handlungen mit Tieren etc. ■ **Posendarstellung** *(§ 4 Abs. 1 S. 1 Nr. 9 JMStV)* ◆ Minderjährige in unnatürlich geschlechtsbetonter Körperhaltung ■ **Verfassungsfeindliche Propagandamittel** *(§§ 86, 86a StGB)* ◆ NS-Symbole ■ **Menschenwürdeverletzende Darstellungen** *(§ 4 Abs. 1 S. 1 Nr. 8 JMStV)* ■ **Bestimmte brutale Gewaltdarstellungen** *(§ 131 StGB)* ◆ Grausame oder unmenschliche Gewalttaten	z. B. ■ **Einfache Pornographie** *(§ 184 Abs. 1 StGB)* ◆ sexuelle Vorgänge werden reißerisch in den Vordergrund gestellt ■ **Offensichtlich schwer jugendgefährdende Inhalte** *(§ 15 Abs. 1 und 2 JuSchG)* ◆ Inhalte, deren Gefährdung für Jugendliche „ins Auge springt" ■ **Von der BPjM indizierte Inhalte** *(§ 18 Abs. 1 JuSchG)* ◆ unsittliche Inhalte ◆ verrohende Inhalte ◆ zu Verbrechen/Rassismus anreizende Inhalte … ■ **Inhalte, die keine Jugendfreigabe seitens der Einrichtungen der Freiwilligen Selbstkontrolle erhalten haben**	z. B. **Filme / Computerspiele für Kinder / Jugendliche unterhalb der Altersfreigabe** *(FSK bzw. USK)*
Inhalte dieser Kategorie unterliegen einem absoluten Verbreitungsverbot, z. T. auch Besitzverbot	Inhalte dieser Kategorie unterliegen einem Weitergabeverbot an Minderjährige	Inhalte dieser Kategorie unterliegen Abgabe- und Verbreitungsbeschränkungen

Quelle: angelehnt an Liesching (2013)[4]

Jugendgefährdende Inhalte: konkret

2014 registrierte **jugendschutz.net** 7.934 (2013: 8.111) Verstöße gegen Jugendschutzbestimmungen, davon wurden 17 % (2013: 18 %) auf deutschen Seiten festgestellt, der Rest auf ausländischen Angeboten. Sowohl im Inland als auch im Ausland löschen die Serviceprovider die problematischen Inhalte auf Anfrage in der Mehrheit der Fälle. Wie bereits 2013 betrafen auch im Jahr 2014 die häufigsten Verstöße Fälle von Darstellungen sexuellen Missbrauchs, Pornografie und extremistischen Inhalten.[5]

Kinder und Jugendliche gelangen zum einen ungewollt auf entwicklungsbeeinträchtigende Seiten im Internet: Sie vertippen sich bspw. bei der Eingabe der Internetadresse, bei der Eingabe in die Suchmaske oder werden von harmlosen Webseiten auf Erotik-Angebote weitergeleitet. Zum anderen suchen Kinder und Jugendliche auch ganz bewusst nach Inhalten, die mancher Erwachsene als problematisch erachtet. Die Gründe dafür sind vielfältig: Kinder und Jugendliche sind fasziniert von dem Verbotenen, sie treibt die Neugierde. Zudem gilt das Ansehen von gewalthaltigen oder pornografischen Inhalten oft auch als Mutprobe innerhalb der Peergroup.

Rechtsextremismus im Netz

Rechtsextremismus im Netz präsentiert sich längst nicht mehr offensichtlich und ist damit nicht für alle Nutzer einfach erkennbar. So werden rechtsextremistische Positionen, wie die Diskriminierung von Minderheiten oder eine feindliche Haltung gegenüber dem demokratischen Rechtsstaat, verschleiert, trendig, witzig und jugendaffin aufbereitet und so unter die Leute gebracht: Ein modern-ästhetisches Auftreten, emotionale (heroische) Darstellungen oder kultige, rebellische Aktionsformen dienen als Köder, um niedrigschwellig an rechtsextremes Gedankengut heranzuführen.
Verbreitet wird dieses über Webseiten sowie über Social Web-Angebote wie bspw. **YouTube, Twitter, Tumblr, Facebook** oder **VK** – das russische Pendant zu Facebook.[6]

Insgesamt verzeichnet **jugendschutz.net** im Bereich rechtsextremistischer Inhalte einen Zuwachs an Jugendschutzverstößen[7]. In den meisten Fällen geht es um die Verbreitung von Kennzeichen verfassungswidriger Organisationen, volksverhetzender oder holocaustleugnender Inhalte, die strafrechtlich absolut unzulässig und damit verboten sind. Verboten sind auch Symbole, die den illegalen Symbolen „zum Verwechseln ähnlich" (§ 86a Abs. 2 StGB) sehen, wie z. B. Hakenkreuze mit verkürzten Querbalken.
Dieser Zusatz ist nötig, da die rechtsextreme Szene durch das Abändern bekannter Kennzeichen, Parolen etc. immer wieder versucht, unter der Strafbarkeitsschwelle zu bleiben.

Pornografie im Netz
Erotische und pornografische Inhalte gibt es im Internet zuhauf: Rund 2,5 Millionen pornografische Seiten listen die Anbieter von Filtersoftware im Jahr 2011[8]. Dabei handelt es sich in erster Linie um die sogenannte **einfache Pornografie.** Unter der einfachen Pornografie sind solche Darstellungen zu verstehen, die vorwiegend auf sexuelle Handlungen, Geschlechtsorgane sowie sexuelle Stimulation fokussieren. Das ist zulässig, wenn sichergestellt ist, dass Personen unter 18 Jahren keinen Zugriff auf das Angebot haben. Das wird üblicherweise mittels Altersverifikationssystemen (AVS) gewährleistet. Deutsche Anbieter unterliegen den Bestimmungen des JMStV, der eine verlässliche Volljährigkeitsprüfung über einen persönlichen Kontakt (z. B. Ausweisdaten) vorsieht. Bei Anbietern mit Sitz im Ausland ist die Sicherheit des Zugangsschutzes oft lax – gemäß: „Bist du volljährig? Ja / Nein".

Unzulässig ist die sogenannte **harte Pornografie.** Darunter sind Darstellungen zu verstehen, die z. B. sexuelle Handlungen an und mit Tieren zeigen, sexuelle Gewalt beinhalten, kinderpornografisch sind etc. Bei Kinderpornografie ist auch alleine der Besitz strafbar. 2013 verzeichnete das Bundeskriminalamt (BKA) 4.144 Fälle von Besitz bzw. Beschaffung von Kinderpornografie[9]. **Sogenannte Posenfotos,** auf denen Kinder oder Jugendliche nackt oder spärlich bekleidet in aufreizender Weise zu sehen sind, werden zwar nicht dem Bereich der Kinderpornografie zugeordnet, sofern sie nicht den sexuellen Missbrauch zum Gegenstand haben oder noch nicht die Schwelle zur Pornografie überschritten haben, jedoch ist im JMStV geregelt, dass auch die Veröffentlichung sogenannter Posen-Darstellungen von Minderjähriger verboten ist.

Gewaltdarstellungen im Netz
Gewaltdarstellungen im Internet stammen oft aus gewalthaltigen Kino- oder Fernsehfilmen oder Spielen. Daneben existieren aber auch extreme Gewaltdarstellungen, die nur im Netz verbreitet werden. In diesem Kontext unterscheidet jugendschutz.net[10] folgende Angebote:

- **Gewalt im sexuellen Kontext**
  d. h. Sado-Maso-Szenen, bizarre Fetische etc.
- **Tasteless-Angebote:**
  d. h. Foto- und Videosammlungen von verletzten, verunstalteten, toten oder getöteten Menschen
- **Kriegsgräuel:**
  d. h. brutale Darstellungen von Kriegsgräueln, z. B. Exekutionen
- **Gewaltspiele**
  d. h. bereits indizierte Spiele / Spiele ohne Jugendfreigabe

Je nach Intensität der dargestellten Gewalt wird unterschiedlich mit den Angebote verfahren, s. obige Differenzierung in **absolut verboten, relativ verboten** und **jugendgefährdend.**

Wichtig!!
Problematische Inhalte können von Nutzern bei den folgenden Stellen gemeldet werden:

www.internet-beschwerdestelle.de

www.jugendschutz.net/hotline/index.html

Illegale und jugendgefährdende Inhalte dürfen weder durch Lehrkräfte noch durch sonstiges Schulpersonal Kindern und Jugendlichen zugänglich gemacht werden. Bereits das Gewährenlassen der Nutzung von illegalen Medieninhalten durch Schülerinnen und Schüler kann als „Unterlassen" geahndet werden.

Links und weiterführende Informationen

Webseiten

www.jugendschutz.net
Infos zum Schutz von Kindern im Internet.

www.bmfsfj.de/BMFSFJ/Service/Publikationen/publikationsliste,did=203896.html
Ein Flyer von fragFINN, der sich an Eltern richtet und einen knappen Überblick über den Kinderschutz im Internet bietet.

www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatzmodule/LH_Zusatzmodul_Rechtsextremismus_klicksafe.pdf
Das klicksafe Zusatzmodul zu Rechtsextremismus im Internet mit vertiefenden Informationen und Unterrichtsmaterialien.

www.lo-recht.de/750125.php
Eine umfassende Informationsseite rund um rechtliche Themen und ihre Relevanz für die Schule.

www.schau-hin.info/medien/internet.html
Tipps und Informationen für das sichere Surfen im Internet.

www.surfen-ohne-risiko.net
Umfassende Informationsseiten, die Eltern Hilfestellung bietet, ihre Kinder im Umgang mit dem Internet zu schützen.

www.ajs-bw.de/shop/catalogue/index.asp?wag=Medienerziehung
Literatursammlung (Shop) der Aktion Jugendschutz zum Thema „Kinder und Internet".

www.zartbitter.de
Informationsseite gegen sexuellen Missbrauch von Minderjährigen.

www.ein-netz-fuer-kinder.de
Initiative zur Förderung qualitativ hochwertiger Kinderwebseiten.

Endnoten

[1] JUGENDSCHUTZGESETZ. Aufgerufen am 26.03 2015 unter http://www.gesetze-im-internet.de/juschg/

[2] JUGENDMEDIENSCHUTZ-STAATSVERTRAG. Aufgerufen am 26.03.2015 unter http://www.kjm-online.de/fileadmin/Download_KJM/Recht/JMStV_Stand_13_RStV_mit_Titel_deutsch3.pdf

[3] STRAFGESETZBUCH. Aufgerufen am 26.03.2015 unter http://www.gesetze-im-internet.de/stgb/

[4] LIESCHING, M. (2013). *Medienrecht und Jugendschutz – Ein Überblick.* In I. Richter, H.-P. Füssel, C. Langenfeld & H.-J. Albrecht (Hrsg.), *Recht der Jugend und des Bildungswesens 2/2013* (S. 136 – 148). Berlin: Berliner Wissenschaftsverlag

[5] GLASER, S., ÖZKILIC, M. & SCHINDLER, F. (2014). Ergebnisse der Recherchen und Kontrollen.Bericht 2014: Jugendschutz im Internet. Aufgerufen am 09.12.2015 unter http://www.jugendschutz.net/fileadmin/download/pdf/bericht2014.pdf

[6] JUGENDSCHUTZ.NET (2014). *Rechtsextremismus online – beobachten und nachhaltig bekämpfen. Bericht über Recherche und Maßnahmen 2013.* Aufgerufen am 17.11.2014 unter http://www.hass-im-netz.info/fileadmin/dateien/pk2014/bericht2013.pdf

[7] Ebd.

[8] OGAS, O. & GADDAM, S. (2012). *A Billion Wicked Thoughts: What the Internet Tells Us About Sexual Relationships.* London: Plume.

[9] BUNDESKRIMINALAMT (2013). *Polizeiliche Kriminalstatistik – Bundesrepublik Deutschland Jahrbuch 2013, 61. Ausgabe.* Wiesbaden: BKA. Aufgerufen am 26.03.2015 unter https://www.bka.de/nn_196810/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2013/pks2013Jahrbuch.html?__nnn=true

[10] JUGENDSCHUTZ.NET. (2015, 17. März). *Gewaltdarstellungen im Internet.* Aufgerufen am 26.03.2015 unter http://www.jugendschutz.net/gewalt/index.html

Arbeitsblatt	**AB 1** ▶▶	**AB 2** ▶▶
Titel	**Rechtsextremismus: Recht und Gesetz – Verbote kennen!**	**Recht und Gesetz: Pornografie**
Kompetenzen	Die Schülerinnen und Schüler können **rechtsextreme Online-Inhalte auf Grundlage von Gesetzen rechtlich einordnen.**	Die Schülerinnen und Schüler schließen aus Auszügen der gesetzlichen Regelungen zur Pornografie auf die wesentlichen Bestimmungen und übertragen sie auf Fallbeispiele.
Methoden	Fallbeispiele	Partnerinterview
Material	Arbeitsblatt, Fallbeispiele, Lösungsblatt	Arbeitsblatt
Zeit (in Minuten)	45	45
Zugang Internet/PC	nein	nein

Hinweise für die Durchführung

AB 1: Rechtsextremismus: Recht und Gesetz – Verbote kennen!

Frage an die Schülerinnen und Schüler: „Warum gibt es überhaupt rechtsextreme Inhalte im Netz?" Auch rechtsextreme Ansichten, Symbole oder Propaganda im Internet sind nach dem Grundgesetz Meinungsäußerungen. Sie sind deshalb grundsätzlich durch die Meinungsfreiheit geschützt. Allerdings gilt dies nicht uneingeschränkt. Die Schüler lesen die Gesetzestexte auf dem Arbeitsblatt. Fragen zur Formulierung oder Verständnisfragen gleich im Plenum klären. Das Blatt mit den Fallbeispielen wird ausgeteilt. Da sich auf dem Blatt zwei Beispiele befinden, die strafrechtlich relevant sind, wird empfohlen, das Blatt am Ende des Unterrichts wieder einzusammeln. Das Zeigen der Beispiele im Unterricht ist aber durch die Sozialadäquanzklausel erlaubt. Das erworbene Wissen soll anschließend in Fallbeispielen auf reale Situationen angewendet werden.

Lösung
- **Fall 1 Verstoß wegen Holocaust-Leugnung**
  (Quelle: www.nationale-revolution.net/forum/showthread.php?t=9457, Stand: 14.08.2012)
- **Fall 2 grenzwertig, aber kein Verstoß**
  (Quelle: www.npd-mv.de/index.php?com=shop&view=article&id=21&mid=21, Stand: 14.08.2012)
- **Fall 3 Verstoß wegen Volksverhetzung**
  (Quelle: http://logr.org/nsolfen/2010/11/10/kristallklare-nacht , Stand: 14.08.2012)

Lösungsblatt bei Bedarf an die Schüler austeilen.

AB 2: Recht und Gesetz: Pornografie

Steigen Sie ein mit einem Fallbeispiel (siehe Aufgabe 2 AB) und fragen Sie die Schülerinnen und Schüler nach ihrer Einschätzung des Falles. Die Schülerinnen und Schüler sind, was die rechtlichen Regelungen zu (Internet-)Pornografie angeht, häufig verunsichert, interessieren sich aber für das Thema. Danach sollen die Schülerinnen und Schüler die Auszüge aus den gesetzlichen Regelungen mit der Methode „Partnerinterview" lesen (Beschreibung siehe Arbeitsmaterial). Anschließend beurteilen sie zunächst alleine, dann im Plenum die Beispiele und begründen sie mithilfe der Auszüge aus den gesetzlichen Regelungen.

Lösungen:
- **Artjom (17)** hat eine Freundin. Wenn sie nicht da ist, schaut er oft Erotikclips im Internet an.
  → Das ist erlaubt. Unter 18-Jährige dürfen Erotik ansehen, aber keine pornografischen Darstellungen.
- **Zwei Kinder unter 14 Jahren** schicken sich online Nacktbilder voneinander zu.
  → Kinder unter 14 Jahren sind schuldunfähig und können sich nicht strafbar machen (siehe § 19 StGB). Der Fall wäre bei älteren, nach Jugendstrafrecht zu beurteilenden Jugendlichen und einer expliziteren Darstellung, ein anderer, denn reine Nacktbilder sind generell keine pornografischen Schriften.
  Nur in besonderen Fällen kommt das in Betracht, etwa bei einem „aufreizenden Zur-Schau-Stellen der Genitalien oder der Schamgegend von Kindern". Dann kann es sich um eine pornografische Schrift handeln, die gemäß § 184b, § 184c StGB sexuelle Handlungen von Kindern / Jugendlichen (an sich selbst) darstellen, und diese zählt zu den so genannten Jugendpornografischen Schriften. Hier ist bereits der Besitz strafbar sowie auch die Herstellung, Verbreitung und Zugänglichmachung.

Lösungen:

- **Lehrperson Frau Schmidt** möchte mit ihren Jugendlichen über das Thema „Porno-Rap" diskutieren und ihnen den Text eines Interpreten geben, der auf der Liste der jugendgefährdenden Medien steht. Darf sie das?
  → Nein, die Texte darf sie nach JuSchG § 18 nicht an Jugendliche weitergeben.
- **Leon (19)** gibt seinem jüngeren Bruder Jan (16) eine DVD mit einem Pornofilm zum Anschauen.
  → Leon macht sich hiermit nach StGB § 184 strafbar
- **Lena (16) und Kim (15)** sehen sich im Internet Pornoclips an.
  → Das ist verboten nach StGB § 184, jedoch können Lena und Kim dafür nicht bestraft werden, denn v. a. der Internetanbieter macht sich nach deutschem Recht strafbar, wenn er den Zugang nicht für Minderjährige, z. B. mit einem Altersverifikationssystem, beschränkt.
- **Kevin (18)** gibt auf dem Schulhof mehrere pornografische Internetadressen an Sechstklässler weiter.
  → Nicht erlaubt. Hier kann u. U. ein „Zugänglichmachen" gemäß § 184 StGB geltend gemacht werden, wenn Internetadressen zu pornografischem Material angegeben oder weitergegeben werden. Verantwortungslos gegenüber Kindern wäre diese Handlung allemal.

Hinweis: Der genaue Wortlaut der gesetzlichen Vorgaben kann eingesehen werden unter:
Strafgesetzbuch (StGB), online unter: **http://www.gesetze-im-internet.de**
Jugendschutzgesetz und Jugendmedienschutz-Staatsvertrag der Länder, online unter:
www.bmfsfj.de/BMFSFJ/kinder-und-jugend,did=12862.html

Lust auf mehr?

- Im Material „Rechtsextremismus hat viele Gesichter" finden Sie Arbeitsmaterialien zum Thema Rassismus und Rechtsextremismus im Internet:
  www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatzmodule/LH_Zusatzmodul_Rechtsextremismus_klicksafe.pdf
- Zum Thema „Was sagt das Gesetz zu Pornographie" finden Sie ein weiteres Arbeitsblatt für schwächere Schülerinnen und Schüler hier:
  www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Porno/Zusatzarbeitsblatt_Lets_talk_about_Porno_1.pdf

Rechtsextremismus: Recht und Gesetz – Verbote kennen! (1/3)

Arbeitsaufträge:

1. Lest die Gesetzestexte.

In Artikel 5 Absatz 1 des Grundgesetzes heißt es: „Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten."

Das Recht auf freie Meinungsäußerung ist eingeschränkt:

- immer dann, wenn andere Personen in ihrer Ehre verletzt werden (z. B. durch Beleidigungen, Drohungen).
- wenn allgemeine Gesetze und Jugendschutzbestimmungen dies verbieten (z. B. pornografische und gewaltverherrlichende Inhalte dürfen Jugendlichen nicht zugänglich gemacht werden).

(Grundgesetz, Artikel 5 Absatz 2)

- wenn man gegen eine Gruppe von Menschen wegen ihrer Herkunft, ihrem Aussehen oder ihrer Religion zum Hass anstachelt und zur Gewalt auffordert.
- wenn man Einzelne oder Gruppen aufgrund ihrer Herkunft oder Religion beschimpft, verächtlich behandelt oder verleumdet.
- wenn man die im Nationalsozialismus begangenen Taten billigt, leugnet oder verharmlost.

(Volksverhetzung § 130 StGB)

- wenn Kennzeichen verfassungswidriger Organisationen verbreitet werden (z. B. Fahnen, Abzeichen, Uniformstücke, Parolen und Grußformen) – das ist verboten.

(§ 86a StGB Kennzeichen verfassungswidriger Organisationen)

2. Sucht euch zu zweit einen Fall aus und bearbeitet ihn so, als wärt ihr Mitarbeiter bei **jugendschutz.net**, einer deutschen Meldestelle für jugendgefährdende Inhalte. Ihr müsst selbst entscheiden, ob das Angebot strafbar ist oder zulässig. Begründet eure Entscheidung vor der Klasse. Das Wissen über die Gesetze hilft euch dabei.

jugendschutz.net *wurde 1997 von den Jugendministerien der Bundesländer gegründet und drängt auf die Einhaltung des Jugendschutzes im Internet. Die länderübergreifende Stelle setzt sich für mehr Rücksicht auf Kinder und Jugendliche im Netz ein.*

Hier könnt ihr bedenkliche Inhalte melden:

www.jugendschutz.net/hotline

Rechtsextremismus: Recht und Gesetz – Verbote kennen! (2/3)

Fall 1:

Wieviele Juden kamen bei alliierten Bombenangriffen während des 2. Weltkriegs um? Man weiss es nicht – alle betreffenden Juden wurden ja offiziell „vergast"!

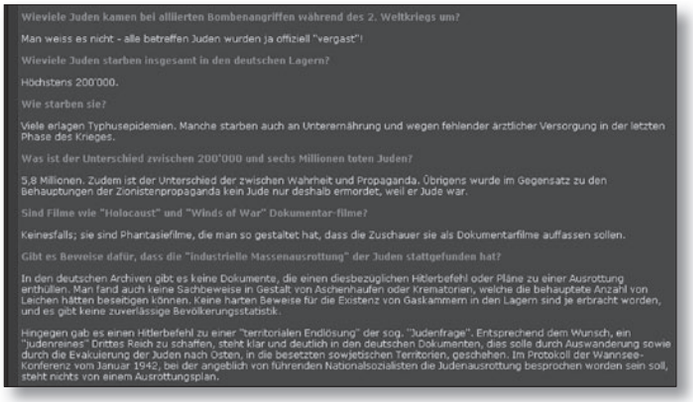
Wieviele Juden starben insgesamt in den deutschen Lagern? Höchstens 200.000.

Wie starben sie? Viele erlagen Typhusepidemien. Manche starben auch an Unterernährung und wegen fehlender ärztlicher Versorgung in der letzten Phase des Krieges.

Was ist der Unterschied zwischen 200.000 und sechs Millionen toter Juden? 5,8 Millionen. Zudem ist der Unterschied der zwischen Wahrheit und Propaganda. Übrigens wurde im Gegensatz zu den Behauptungen der Zionistenpropaganda kein Jude nur deshalb ermordet, weil er Jude war.

Sind Filme wie „Holocaust" und „Winds of War" Dokumentarfilme? Keinesfalls; sie sind Phantasiefilme, die man so gestaltet hat, dass die Zuschauer sie als Dokumentarfilme auffassen sollen.

Gibt es Beweise dafür, dass die „Industrielle Massenausrottung" der Juden stattgefunden hat? In den deutschen Archiven gibt es keine Dokumente, die einen diesbezüglichen Hitlerbefehl oder Pläne zur Ausrottung enthüllen. Man fand auch keine Sachbeweise in Gestalt von Aschehaufen oder Krematorien, welche die behauptete Anzahl von Leichen hätten beseitigen können. Keine harten Beweise für die Existenz von Gaskammern in den Lagern sind je erbracht worden, und es gibt keine zuverlässige Bevölkerungsstatistik.
Hingegen gibt es einen Hitlerbefehl zu einer „territorialen Endlösung" der sogenannte „Judenfrage". Entsprechend dem Wunsch, ein „judenreines" Drittes Reich zu schaffen, steht klar und deutlich in den deutschen Dokumenten, dies solle durch Auswanderung sowie durch die Evakuierung der Juden nach Osten, in die besetzten sowjetischen Territorien, geschehen. Im Protokoll der Wannsee-Konferenz vom Januar 1942, bei der angeblich von führenden Nationalsozialisten die Judenausrottung besprochen worden sein soll, steht nichts von einem Ausrottungsplan.



Screenshot der website

Fall 2:

Fall 3:

« Denkanstoß: Kennen sie Herschel Grynszpan?

Vor der Feldherrnhalle »

Scherben bringen Glück...

Veröffentlicht am 10.11.2010 in Geschichte , Olfen 1 Kommentar Melden

...unter diesem Motto versammelten sich am gestrigen Dienstag, dem 9. November, rund ein dutzend Kameraden, um etwas außerhalb von Olfen eine kleinere Feier anlässlich des 72. Jahrestag der Reichskristallnacht zu veranstalten. Zu allererst hielt ein Kamerad aus dem benachbarten Lüdinghausen eine Rede, welche die Geschehnisse des 9. November 1938 thematisierte. Der Auslöser zur Reichskristallnacht war nicht etwa Hitlers Wille, sondern war eine Reaktion darauf, dass der Jude Herschel Grynszpan den Diplomaten Ernst Eduarth vom Rath in Paris ermordete. Auch im Vorfeld gab es vermehrt Morde welche von Juden begangen wurden. Am ende der Rede hielt man noch eine Schweigeminute für all jene, die Opfer von mordlüsternden Juden wurden. Danach gab es noch etwas Speiß und Trank bis man sich zu später Stund´ nach Haus begab.

Heute Zeichnet sich in den Straßen Deutschlands ein ähnliches Bild ab. Türkenbanden machen die Straßen unsicher; rauben; vergewaltigen und morden. Man kann nur hoffen dass es auch in diesem Zusammenhang einen Aufruhr der Bevölkerung gibt, welche nicht mehr stillschweigend alles hinnimmt.

Was damals die Juden waren, sind heute die Türken!
Deutschland erwache!

Rechtsextremismus: Recht und Gesetz – Verbote kennen! (3/3)

Begründung Fall 1 (strafbar):

„Höchstens 200.000 Juden starben in den deutschen Lagern“:
Der Tod von 5,8 Millionen Juden wird als „Propaganda“ betitelt und nicht als „Wahrheit“. Es gebe *„keine Sachbeweise … welche die behauptete Anzahl von Leichen hätte bestätigen können“* – es gebe *„keine Beweise für die Existenz von Gaskammern“*:
Der Holocaust ist eine historische Tatsache. Mit der Bezeichnung als „Propaganda“, die nicht der Wahrheit entspricht, und der Herunterrechnung jüdischer Opfer (200.000 statt 6.000.000) wird im Artikel der Holocaust als durch die Nazis begangener Massenmord an den Juden geleugnet. Dies stellt nach Paragraf 130 Absatz 3 StGB eine Straftat dar.

Begründung Fall 2 (zulässig):

Die Äußerung „kriminelle Ausländer raus“ ist von der Meinungsfreiheit gedeckt.
Für ein Anstacheln zum Hass reicht die Aussage, dass kriminelle Ausländer Deutschland verlassen sollen, nicht aus. Anders wäre die Lage, wenn z. B. klar wird, dass dies mit Gewalt geschehen soll. Es liegt somit kein Verstoß gegen Paragraf 130 StGB (Volksverhetzung) vor.

Begründung Fall 3 (strafbar):

Text: „Scherben bringen Glück …“ – ein Artikel zu einer neonazistischen Veranstaltung zum Jahrestag der Reichspogromnacht („Reichskristallnacht“).
Im Text wird vorgetäuscht, dass die Juden in der Nazizeit selbst schuld an Gewalttaten gegen sie waren. Dies wird auf die heutige Zeit übertragen, und es wird dazu aufgefordert, gegen den türkischen Teil der Bevölkerung die gleichen Gewalttaten zu verüben, weil diese regelmäßig *„vergewaltigen, rauben und morden“*. Damit wird zu Hass gegen Türken aufgestachelt und zu Gewalt- und Willkürmaßnahmen gegen sie aufgerufen (Volksverhetzung nach Paragraf 130 StGB). Daneben war *„Deutschland erwache“* die Losung der SA bzw. der SS und ist damit als Kennzeichen einer verfassungswidrigen Organisation (nach Paragraf 86a StGB) ebenfalls strafbar.

Recht und Gesetz: Pornografie

Arbeitsaufträge:

1. Der Umgang mit Pornografie ist im Gesetz geregelt. Lest die Regelungen durch. Nutzt hierzu die Methode „Partnerinterview".

Methode „Partnerinterview" *– zu zweit mit Partner A und Partner B. Beide lesen, danach fasst Partner A das Wichtigste zusammen, Partner B wiederholt mit den Worten: „Habe ich dich richtig verstanden, dass …?" Dann Wechsel der Rollen – aber Vorsicht! Jeder darf zwei Fehler einbauen, die der andere finden muss!*

Auszüge aus gesetzlichen Regelungen

Verbreitung gewalt- oder tierpornografischer Schriften *(StGB 184 a)* Die Verbreitung ist strafbar.

Verbreitung pornografischer Schriften *(StGB § 184)* Verbot der Weitergabe von Pornografie an Minderjährige. Nach § 11 Abs. 3 StGB umfasst der Begriff „Schriften" auch Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen).

Kinder- und Jugendpornografie *(StGB 184 b + c)* Über die Verbreitung hinaus ist hier auch der Versuch der Beschaffung und der Besitz strafbar.

Die ***Darstellung von Kindern oder Jugendlichen in unnatürlich geschlechtsbetonter Körperhaltung*** in Rundfunk und Telemedien – dies gilt auch bei virtuellen Darstellungen – ist verboten (JMStV § 4, Abs. 1 Nr. 9).

Liste jugendgefährdender Medien *(JuSchG § 18)* Medien, welche von der Bundesprüfstelle für jugendgefährdende Schriften indiziert wurden, dürfen nicht an Minderjährige weitergegeben werden.

Bildträger ohne Jugendfreigabe *(JuSchG § 12)* Filme oder Spiele, die nicht oder mit „keine Jugendfreigabe" von der FSK oder der obersten Landesbehörde gekennzeichnet wurden, dürfen nicht an Minderjährige weitergegeben werden.

Rundfunk und Telemedien müssen dafür sorgen, dass Inhalte eine Alterskennzeichnung haben und von Kindern und Jugendlichen der entsprechenden Altersgruppen nicht wahrgenommen werden können (z. B. durch bestimmte Sendezeiten oder technische Zugangsbeschränkungen, Altersprüfung durch Perso-Check).

2. Beurteile die Situationen. Verboten oder nicht? Kreuze an und belege deine Antworten mithilfe der gesetzlichen Regelungen. Vergleicht eure Ergebnisse in der Gruppe.

	verboten	erlaubt
Artjom (17) hat eine Freundin. Wenn sie nicht da ist, schaut er oft Erotik-Clips im Internet an.		
Zwei Kinder unter 14 Jahren schicken sich online Nacktbilder voneinander zu.		
Lehrperson Frau Schmidt möchte mit ihren Jugendlichen über das Thema „Porno-Rap" diskutieren und ihnen den Text eines Interpreten geben, der auf der Liste der jugendgefährdenden Medien steht. Darf sie das?		
Leon (19) gibt seinem jüngeren Bruder Jan (16) eine DVD mit einem Pornofilm zum Anschauen.		
Lena (16) und Kim (15) sehen sich im Internet Pornoclips an.		
Kevin (18) gibt auf dem Schulhof mehrere pornografische Internetadressen an Sechstklässler weiter.		

Urheberrecht und Open Content

Nutzungsfreiheiten und Grenzen des Urheberrechts

Das Urheberrecht wird nicht grenzenlos gewährt. Vielmehr sieht das Urheberrechtsgesetz sogenannte **Schrankenbestimmungen** vor, nach denen bestimmte Nutzungshandlungen auch ohne Zustimmung des Rechteinhabers gestattet sind. Eine für den persönlichen Alltag besonders wichtige Regelung ist die Privatkopie. Sie erlaubt, urheberrechtlich geschützte Werke zu privaten Zwecken zu vervielfältigen, also etwa Fernsehsendungen aufzunehmen oder CDs zu brennen und die Kopien im privaten Raum zu nutzen. Andere Schrankenbestimmungen erlauben z. B. Zitate oder bestimmte Nutzungen im Rahmen der Presseberichterstattung.

Kommerziell oder nicht ist unwichtig

In Bezug auf die Nutzungsfreiheiten ist eines wichtig zu wissen: Viele denken, dass man generell alles darf, solange man nur kein Geld damit verdienen will. Ein Foto von einer fremden Webseite zu nehmen und in sein Facebook-Profil einzustellen, müsse also erlaubt sein. Das ist ein gefährlicher Irrglaube. Das Urheberrecht unterscheidet nicht grundsätzlich danach, ob man mit einer Nutzungshandlung Geld verdienen will, sondern vielmehr vorrangig zwischen öffentlichen und privaten Nutzungen. Während im privaten Bereich allerhand erlaubt ist, sind Nutzungen, die in der Öffentlichkeit stattfinden, fast immer nur mit Zustimmung des jeweiligen Rechteinhabers erlaubt. Das gilt auch und besonders für die Onlinenutzung. Etwas zum freien Ab- oder Aufruf ins Internet zu stellen, ist niemals eine private Nutzung, sondern eine öffentliche (weil eben jeder hierauf zugreifen kann).

Schulunterricht ist NICHT öffentlich!
Nutzungen im Schulunterricht sind, soweit nur Schülerinnen und Schüler aus derselben Klasse zugegen sind, nicht öffentlich. Filme vorführen, Musik abspielen und ähnliche Handlungen (das Urheberrecht nennt diese unkörperliche Nutzungshandlungen) fallen daher nicht unter das Urheberrecht und sind ohne Weiteres zulässig.

Privat ist einiges erlaubt

Privatkopien dürfen gem. § 53 Abs. 1 UrhG in der Regel auch von digitalen Werken erstellt werden (etwa **„rippen"** einer CD und Speicherung der MP3s auf einem entsprechenden Player). Entscheidend ist, dass man die Kopien nur privat nutzt. Auch die Weitergabe der gebrannten CD an Freunde oder enge Verwandte ist noch eine private Nutzung. Jedoch gelten zwei wichtige Einschränkungen: Zum einen dürfen niemals Kopierschutzmechanismen zur Erstellung der Kopie umgangen werden; Kopiergeschützte Inhalte sind also tabu. Zum anderen dürfen Vorlagen für eine Kopie nicht aus offensichtlich illegalen Quellen stammen. Eine nicht unwichtige Selbstverständlichkeit sei deutlich gesagt: Zuwiderhandlungen gegen das Urheberrecht sind mit zivilrechtlichen und strafrechtlichen Sanktionen belegt. Es kann also teuer werden, wenn man gegen das Urheberrecht verstößt.

Ende des Urheberrechts

Wann endet das Urheberrecht und was passiert dann? Anders als das Eigentum an Sachen währt das Urheberrecht nicht ewig. Unter der Erkenntnis, dass der Zugang zu und die Nutzung von geistigen Errungenschaften von besonderer Bedeutung für die Allgemeinheit sind, werden diese mit Ablauf von **70 Jahren nach dem Tod des Urhebers gemeinfrei** (Schutzfrist). Danach ist es jedem gestattet, das Werk auf jede Art und Weise frei zu verwenden. Für die Schule sind somit alle Werke (Bücher, Lieder etc.) interessant, deren Autoren in etwa vor dem Jahr 1940 gestorben sind. Dazu gehören schon eine Menge bekannter Werke, wie z. B. der **„Struwwelpeter"** von Heinrich Hoffmann (gest. 1894).

Der Blick zurück und voraus
Das Urheberrecht war nicht immer so streng. Bei der Einführung des ***„Copyrights"*** *in England 1710 betrug die Schutzdauer 14 Jahre mit der einmaligen Möglichkeit der Verlängerung. Auf diese Tradition würden sich Menschen wie der Historiker Robert Darnton, Leiter der Harvard-Bibliothek, gerne besinnen. Darnton gründete ein nicht-kommerzielles Projekt, die* ***DPLA*** *(Digital Public Library of America), um abseits der Konzerne wie Google Bücher kostenlos digital verfügbar zu machen. Ein Blick lohnt sich:* ***www.dp.la***

Aus der Praxis
Das relativ strenge Urheberrecht in Deutschland ist von Schülern nur sehr schwer nachzuvollziehen. Insbesondere bei Inhalten, die massenhaft frei verfügbar sind (z. B. bei Fotos aus dem Internet). Lehrer können versuchen es damit zu verdeutlichen, dass die Schüler selbst mal ein berühmter Fotograf, Maler oder Musiker sein könnten und mit der Frage, welche Vielfalt an Kunst wohl noch verfügbar wäre, wenn niemand mehr dafür bezahlen würde.

Open Content und Open-Source-Software
Viele Urheber finden, dass das Urheberrecht die Nutzung von geschützten Werken zu sehr einschränkt, also zu wenig Nutzungsfreiheiten gewährt. Aus diesem Grund wurden in den 1990er-Jahren und zu Beginn des neuen Jahrtausends Initiativen wie **Creative Commons** oder die **Free Software Foundation** gegründet. Basierend auf der Idee, dass Werke möglichst frei und kostenlos kopiert, verändert und weitergegeben (auch online gestellt) werden können, entstand Anfang der 1990er-Jahre die Open-Source-Software-Bewegung und 2001 die Initiative Creative Commons. Die dahinter stehenden (US-amerikanischen) Institutionen entwickeln v. a. freie Lizenzen, die alle interessierten Urheber nutzen können, um jedem eine mehr oder weniger freie Nutzung ihrer Werke zu erlauben. In der **Foto-Community Flickr** oder bei **www.pixelio.de** finden sich z. B. Millionen frei lizenzierter Fotos, die jedermann nutzen kann. Weitere erfolgreiche Projekte sind das **freie Betriebssystem Linux** oder die **Online-Enzyklopädie Wikipedia.** Alle hierin befindlichen Inhalte dürfen von jedem nach den Regeln der jeweils geltenden Lizenzbestimmungen weitgehend frei genutzt werden.

Bedeutung für Schülerinnen und Schüler
Ein Verstoß gegen das Urheberrecht kann gravierende Folgen haben. Auch wenn die Anzeige bei der Polizei mit der Einstellung des Verfahrens und/oder der Ableistung von Sozialstunden glimpflich verläuft, bleiben die zivilrechtlichen Forderungen davon unberührt.
Im Klartext: Ein Verstoß gegen das Urheberrecht kann teuer werden! Hier zwei Beispiele:

- **Ein Jugendlicher** bot ein Lied im Internet zum Download an und wurde vom Urheber angeschrieben: Er sollte eine strafbewährte Unterlassungserklärung abgeben sowie 2000 Euro bezahlen, was er nicht tat, so dass der Fall vor Gericht kam. Obwohl der Jugendliche die Abweisung der Klage (aufgrund seiner Minderjährigkeit) forderte, wurde er in letzter Instanz zur Zahlung von Schadenersatz und Abmahnkosten verurteilt.[1]

- **Zwei Jugendliche im Alter von 14 und 16** hatten zehn Musikstücke ins Netz gestellt und damit zum Download angeboten. Das Landgericht Düsseldorf entschied, dass die Eltern als Anschlussinhaber des Internetzugangs einen Schadenersatz von 300 Euro pro Musikstück, also 3000 Euro, zu zahlen haben. Das Gericht argumentierte, dass die Eltern den Computer ihrer Kinder regelmäßig hätten kontrollieren müssen.[2]

Dabei gibt es Angebote, bei denen kostenlos freie Musik erhältlich ist, die man – meist unter Angabe der Quelle – für eigene Zwecke verwenden darf. Einige Beispiel finden sich weiter unten in diesem Kapitel.

Kopien für die Klasse
Das Urheberrecht unterscheidet generell zwischen Nutzungen in der Öffentlichkeit und außerhalb der Öffentlichkeit (v. a. im privaten Umfeld). Nutzungen in einer Schulklasse, bei denen nur die Schülerinnen und Schüler der Klasse und die Lehrer zugegen sind, werden von der Rechtsliteratur als nicht öffentlich angesehen (s. o.), wodurch sich mehr Möglichkeiten für die Verwendung fremder Werke eröffnen.

Das Urheberrechtsgesetz (zuletzt geändert durch Art. 1 G vom 05.12.2014) enthält einige Vorschriften, die auch für die schulspezifische Internetnutzung von Bedeutung sind: § 53 Absatz 3 UrhG gestattet die Herstellung von Kopien (im Sinne von Ausdrucken, Abzügen) für den Unterrichtsgebrauch, soweit es sich um kleine Teile eines Werkes, Werke von geringem Umfang oder einzelne Beiträge aus Zeitungen und Zeitschriften handeln. Die Kopien dürfen zur Veranschaulichung des Unterrichts an Schulen in der für die Unterrichtsteilnehmer erforderlichen Anzahl hergestellt werden, wobei natürlich auch auf Internetinhalte zurückgegriffen werden darf. Allerdings ist eine wichtige Einschränkung zu beachten: Kopien aus Schulbüchern bedürfen nach § 53 Absatz 3 Satz 2 UrhG immer einer Einwilligung des Verlages, sind also tabu.[3]

Die Schulministerien wissen um das Dilemma der Lehrkräfte vor Ort und sind natürlich auch bemüht, juristisch einwandfreie Regelungen zu treffen, die alltagstauglich sind. Dazu haben die Bundesländer eigene Vereinbarungen mit den Verwertungsgesellschaften und Verlagen getroffen, z. B. die „Ergänzungsvereinbarung zum Gesamtvertrag zur Einräumung und Vergütung von Ansprüchen nach § 53 Urheberrechtsgesetz (UrhG)". Darin ist festgelegt, dass auch digitale Vervielfältigungen erlaubt sind. Ab dem 1. Januar 2013 sind digitale Vervielfältigungen auch aus Schulbüchern möglich, jedoch ist diese Regelung auf Werke, die ab 2005 erschienen sind, begrenzt.

Demnach dürfen pro Schuljahr und Schulklasse 10 %, jedoch maximal 20 Seiten, vervielfältigt werden.

Auch die digitale Weitergabe ist definiert. Darunter ist zu verstehen:

- Weitergabe über digitale Medien (USB-Sticks, CDs),
- Wiedergabe über PC / Beamer / Whiteboard etc.,
- Speicherung auf mehreren Medien des Lehrers (z. B. PC und Laptop, Tablet), wobei diese aber passwortgeschützt sein müssen, sowie
- ausdrucken und an die Schüler verteilen.

Schüler wiederum dürfen digitale Kopien ausdrucken, aber nicht ihrerseits weitergeben!

Bei diesen Regelungen ist zu beachten, dass die Obergrenze der möglichen Vervielfältigungen für analoge und digitale Ausfertigungen gemeinsam gilt. Es können also nicht 10 % (bzw. maximal 20 Seiten) digital, als auch zusätzlich 10 % (bzw. maximal 20 Seiten) analog vervielfältigt werden.[4]

Zitatrecht
Nach § 51 UrhG (Zitatrecht)[5] darf bei der Erstellung eigener Werke ohne Einwilligung und Vergütung auf den geschützten Leistungen anderer aufgebaut werden. Wenn ein fremdes Werk erörtert wird, darf bspw. immer nur so viel von dem fremden Werk zitiert werden, wie für die eigenen Ausführungen erforderlich ist. Zudem ist eine Quellenangabe notwendig.

Das Zitatrecht zwar einerseits die Nutzung fremder Inhalte, hält aber durchaus einige Einschränkungen bereit: Zitieren darf man nur in eigenen Inhalten. Man könnte sagen, dass das Zitat niemals die Hauptsondern immer nur die Nebensache sein darf. Im Vordergrund muss die eigene Kreation stehen. Erstellt man beispielsweise eine Collage aus fremden Fotos oder Videoausschnitten, ist deren Nutzung nicht durch das Zitatrecht gedeckt. Denn hier besteht das ganze neue Werk nur aus Zitaten, die Eigenleistung steht also nicht im Vordergrund.

Zitate dürfen nicht zu umfangreich sein. Wie lang genau diese sein dürfen hängt vom Einzelfall ab und kann nicht generell gesagt werden. Selbstverständlich muss das Zitat einem Zweck dienen (wobei ein **„innerer Zusammenhang"** wichtig ist) und die Quelle angegeben werden muss.[6]

*Die Initiative **„Respect Copyrights"** hat Fragen rund um die Mediennutzung (vor allem für Filme und Fernsehmitschnitte etc.) sehr kompakt und anschaulich dargestellt:*
www.respectcopyrights.de

Unterrichtsmaterialien im Intranet
Viele Schulen besitzen ein geschlossenes Computernetz, ein sogenannte **Intranet,** auf das i. d. R. nur die Schulangehörigen Zugriff haben. Nach § 52a UrhG dürfen in einem solchen Intranet auch fremde Werke in gewissem Umfang den Schülerinnen und Schülern zugänglich gemacht werden. Dabei gilt: Wer Dateien in ein Schulintranet einstellt, muss dafür sorgen, dass tatsächlich nur die Unterrichtsteilnehmer hierauf zugreifen können und Unberechtigte keinen Zugriff haben. Voraussetzungen für die Nutzung im Intranet sind[7]:

- Unterrichtsbezug und strenges Zweckgebot (wirklich im Unterricht benötigte Materialien, nur für den Zeitraum der Behandlung im Unterricht, nicht auf Dauer/auf Vorrat)
- nur einzelne Artikel oder kleine Teile eines Werkes oder Werke geringen Umfangs
- Auszüge aus Materialen für den Unterrichtsgebrauch immer nur mit Zustimmung des Rechteinhabers
- Auszüge aus Filmen erst zwei Jahre nach Kinostart
- Zugriff nur für einen abgeschlossenen Teilnehmerkreis (die Klasse, der Kurs)

Geringer Umfang
Die Definition über die Frage, was denn nun genau **„ein Werk geringen Umfangs"** oder **„kleine Teile"** sind, ist in einer Vereinbarung zwischen der Kultusministerkonferenz mit den Inhabern der Rechte geregelt: **kleine Teile** sind bis zu 10 % (bzw. maximal 20 Seiten) eines Werkes oder fünf Minuten Film. **Werke geringen Umfangs** sind hiernach Druckwerke von maximal 25 Seiten, Filme von maximal fünf Minuten Länge, maximal fünf Minuten eines Musikstücks sowie alle Bilder, Fotos und sonstige (vollständige) Abbildungen.[8]

Kopieren oder Vorführen?
Der (Rechts-) Teufel steckt wie immer im Detail und das macht die Fragen des Urheberrechts in der Schule so schwierig und zum Teil absurd: Weil das Urheberrecht **Kopieren** und **Vorführen** unterschiedlich behandelt, ist es einerseits zulässig, der Klasse im Schulunterricht einen Film auf DVD vorzuführen (auch vollständig). Kleine Ausschnitte von einer DVD herunterzukopieren und ins Intranet zu stellen, ist dagegen verboten. Solche Bildträger sind ausnahmslos kopiergeschützt. Das Gesetz sagt, dass Kopierschutzsysteme in keinem Fall eigenhändig umgangen werden dürfen, auch wenn dies einem an sich legitimen Zweck dient (z. B. der Nutzung für Unterrichtszwecke). Da es aber unmöglich ist, Filmausschnitte von einer DVD auf einen Server zu kopieren, ohne die DVD vorher zu **„rippen",** ist eine Nutzung auf diesem Weg ausgeschlossen. Es bleibt die Möglichkeit, einen Film für den Unterricht aus dem Fernsehen aufzunehmen, Ausschnitte herauszukopieren und sie auf den Schulserver hochzuladen, damit die Schüler sich die Ausschnitte für Unterrichtszwecke anschauen können (denn hierfür muss kein Kopierschutz umgangen werden).

Die Schulhomepage
Die Verantwortung für die Schulhomepage hat immer der Schulleiter. Dies ist in den jeweiligen Landesschulgesetzen festgelegt. Der Schulleiter trägt letztendlich immer die Verantwortung und muss sie auch wahrnehmen, z. B. durch regelmäßige Kontrollen. Weitere Information zum Thema Recht sind z. B. bei Lehrer-Online zu finden:
www.lo-recht.de/faqs-schulhomepage.php

Hier gibt es auch eine Übersicht zur Schulhomepage:
www.lehrer-online.de/schulhomepage.php

Auch wenn die Versuchung des zuständigen Kollegen noch so groß ist: Im Internet veröffentlichte Texte und Bilder sind vielfach urheberrechtlich geschützt und dürfen nicht in die Schulhomepage eingebunden werden. Konkret heißt das: Alle Bilder (Fotos, Zeichnungen etc.) selbst machen oder die Rechte für die Veröffentlichung einholen.

Zudem gilt selbstverständlich auch für die Schulhomepage z. B. die Impressumspflicht oder das Unterlassen von Verlinkungen auf illegale Inhalte. Ein Beispielimpressum für Schulen hat Lehrer-Online veröffentlicht: **www.lehrer-online.de/musterimpressum-schulhomepage.php**

Datenschutz und Recht am eigenen Bild
Datenschutz und das Recht am eigenen Bild erfordern sowohl bei Schülerinnen und Schülern, als auch bei Lehrern einen sensiblen Umgang mit persönlichen Daten sowie Personenfotos. Dies bedeutet, dass personenbezogene Daten, wie z. B. Namen, Anschriften, E-Mail-Adressen, Fotos, Telefonnummern, Schulnoten, Kommentare zur schulischen Leistung, Fehlstundenanzahl, Religionszugehörigkeit oder Hobbys insofern zu schützen sind, dass jede Person selbst entscheiden können muss, welche personenbezogenen Daten von ihr veröffentlicht werden.

Generell ist ein sparsamer Umgang mit Daten zu empfehlen. Der bekannte Satz **„Das Internet vergisst nichts"** kann sehr anschaulich gemacht werden: Das Angebot **www.archive.org** einer amerikanischen Bibliothek hat es sich zur Aufgabe gemacht, das Internet zu archivieren. In der so genannten **Wayback-Machine** kann z. B. die Adresse der eigenen Schulhomepage eingegeben werden. Mit etwas Glück (oder Pech – je nach Sichtweise) finden sich dort alte Versionen der Schulhomepage, die eigentlich schon längst gelöscht und aus dem Netz entfernt worden sind.

Einwilligung der Erziehungsberechtigten
Bei Minderjährigen bis etwa 14 Jahren ist in jedem Fall die Einwilligung der Erziehungsberechtigten einzuholen, bei Jugendlichen von etwa 14 Jahren setzt der Gesetzgeber eine gewisse Einsichtsfähigkeit voraus, aber bis 18 Jahren sollten Erziehungsberechtigte und Minderjährige gemeinsam einwilligen. Erwachsene können natürlich frei entscheiden, welche Angaben veröffentlich werden. Eine Ausnahme gibt es: Schulische Kontaktinformationen der Lehrer, die die Schule nach außen vertreten, dürfen auch ohne Einwilligung veröffentlicht werden, z. B. die Namen der Schulleitung mit (dienstlicher) Telefonnummer o. ä.[9]

Eine Schulhomepage lebt auch davon, dass aktuelle Berichte der Schulaktivitäten, Feste, Ausstellungen, Theateraufführungen usw. mit Fotos veröffentlicht werden. Für diese gilt das Gleiche wie für alle anderen personenbezogenen Daten: Die Veröffentlichung von Fotos darf wiederum nur mit Einwilligung der fotografierten, identifizierbaren Person geschehen (dies leitet sich aus dem **„Recht am eigenen Bild"** ab). Die Einwilligung muss schriftlich erfolgen und bei Kindern bis etwa 14 Jahren ist auch hier die Einwilligung der Erziehungsberechtigten einzuholen. Bei Jugendlichen zwischen 14 und 18 Jahren entscheiden Erziehungsberechtigte und Minderjährige gemeinsam.

Aus der Praxis
Regelungen wie das ***Recht am eigenen Bild*** *sollten von Lehrern sehr ernst genommen werden – denn nur so können die gleichen Ansprüche auch an die Schülerinnen und Schüler gestellt werden, z. B. bei Fotos von der Klassenfahrt, die im Internet auftauchen.*

An dieser Stelle sei wiederholt, dass die Rechtslage nicht immer eindeutig ist und im Zweifelsfall eine verbindliche Auskunft, z. B. bei der Schulaufsicht einzuholen ist.

Legale Angebote
Der Download von Musik oder Filmen, die der Urheber freigegeben hat, ist selbstverständlich erlaubt. Hierbei können jedoch zwei Probleme auftauchen: Zum einen kann die zum Download stehende Datei mit Schadsoftware (z. B. Viren) belastet sein, zum anderen kann man nicht sicher sein, ob der Anbieter tatsächlich die Urheberrechte besitzt (und damit freigeben darf).

Zwei Tipps können helfen:

- *die Downloadquelle prüfen (ist der Anbieter seriös?), evtl. nach den Rechten erkundigen*
- *die Datei extern speichern (z. B. auf einem USB- Stick) und sofort nach dem Download mit Antiviren-Software prüfen. Vorher ist eine Prüfung leider nicht möglich.*

Kostenlose Angebote
Das Internet ist (glücklicherweise) auch immer noch Spielwiese und Tummelplatz für allerlei kostenlose Schätze, so auch im Musikbereich. Vor allem unbekannte Künstler finden eine Möglichkeit, ihre Musik zu verbreiten.

- **Jamendo** ist nach eigenen Angaben die Nummer 1 für freie Musik: **www.jamendo.com/de**
- **Tonspion:** Die gut sortierte Liste führt zu den kostenlosen Angeboten der Künstler. **www.tonspion.de**.
- **CCMixter** steht unter Creative-Commons-Lizenz und bietet kostenlose Musik: **www.ccmixter.org**
- **Eine generelle Übersicht** von Anbietern von Inhalten unter Creative-Commons-Lizenz gibt es unter **http://search.creativecommons.org/**

Mitschnitt aus dem Radio
Nach deutschem Recht ist ein Mitschnitt aus dem Radio für private Zwecke erlaubt.[11] Dies schließt die vielen Internetradio-Stationen mit ein. Und selbstverständlich hilft auch hier die passende Software, die auf Wunsch ganze Radiosendungen aufnimmt und die Musik extrahiert (bspw. **RadioFX** der Firma Tobit).

Podcasts
Zudem werden Video-Podcast-Angebote immer beliebter, so zum Beispiel in den **Mediatheken** der öffentlich-rechtlichen Sendeanstalten, wo man fast alle Sendungen live über das Internet sehen und auch danach anschauen / herunterladen kann. Bspw. **www.ardmediathek.de/fernsehen** und **www.zdf.de/ZDFmediathek**. Jedoch wurden den Sendern durch den 12. Rundfunkänderungsstaatsvertrag am 1. Juni 2009 Beschränkungen auferlegt, wie lange Sendungen im Internet abrufbar sein dürfen. Während Audios und Videos mit zeit- und kulturhistorischen Inhalten unbefristet angeboten werden dürfen, gelten für alle anderen Fristen, meist von einer Woche.

Jugendschutz
Die Portale der großen Anbieter sind meist gut geschützt und kontrolliert, aber das Thema Jugendschutz ist trotzdem problematisch. Niemand kann kontrollieren, wer wirklich am Rechner sitzt. Das gleiche gilt für jugendgefährdende Musik, die meist in Form rechtsradikaler oder pornografischer Lieder angeboten wird. Wie schon mehrfach betont: in Deutschland ist ihre Verbreitung verboten, was nicht davor schützt, sie aus ausländischen Quellen zu beziehen.

Links und weiterführende Informationen

Webseiten

www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatzmodule/LH_Zusatzmodul_Urheberrecht_klicksafe.pdf
Das klicksafe Zusatzmodul *Nicht alles, was geht, ist auch erlaubt* mit weitergehenden Informationen und Unterrichtsmaterialien zum Thema Urheberrecht

http://irights.info/fileadmin/texte/material/broschuere_klicksafe_irights_urheberrecht_internet.pdf
Eine gemeinsame Broschüre von irights.info und Klicksafe zum Thema

www.gesetze-im-internet.de/urhg/
Das Urheberrechtsgesetz im Wortlaut

www.irights.info
Weitere Informationen zum Urheberrecht bei iRights.info

www.dp.la
Digital Public Library of America

http://lehrerfortbildung-bw.de/sueb/recht/urh/
Informationen der Baden-Württembergischen Landesakademie für Fortbildung und Personalentwicklung an Schulen

www.respectcopyrights.de
Weitere Unterrichtsmaterialien zum Thema Urheberrecht

www.medienberatung.schulministerium.nrw.de/lernenmitmedien/urheberrecht.htm
Medienberatung NRW zum Urheberrecht in Schule und Unterricht

www.bpb.de/gesellschaft/medien/urheberrecht/63412/urheberrecht-in-schule-und-ausbildung?
Ein umfangreiches Dossier der Bundeszentrale für politische Bildung

www.pro-music.org/resources/GERMAN-LEAFLET-FINAL.pdf
LEGAL, SICHER UND FAIR - Nutzung von Musik, Filmen, Serien und Büchern aus dem Internet – Ein Leitfaden für Eltern und Lehrer (Jugendinitiativen Childnet International und Net Family News, Inc. mit Unterstützung von Pro-Music)

www.lo-recht.de
Rechtsportal von Lehrer-Online

www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html
Bundesamt für Sicherheit in der Informationstechnik (BSI) für Bürger

www.saferinternet.at/unterrichtsmaterialien
Österreichische Unterrichtseinheit zum Thema *„Download und Online-Kauf von Musik, Filmen und Software“*

Endnoten

[1] GRUNDMANN HÄNTZSCHEL RECHTSANWÄLTE (2012, 23. März). *Urheberrecht, Internetrecht: Haften Minderjährige für Urheberrechtsverletzungen im Internet?* Aufgerufen am 06.03.2015 unter http://www.hgra.de

[2] SOLMECKE, C. (2011, 30. August). *Landgericht Düsseldorf verurteilt Eltern zu 3.000 Euro Schadensersatz wegen Filesharing ihrer Kinder.* Aufgerufen am 26.03.2015 unter https://www.wbs-law.de/abmahnung-filesharing/landgericht-dusseldorf-verurteilt-eltern-zu-3-000-euro-schadensersatz-wegen-filesharing-ihrer-kinder-11645/

[3] URHEBERRECHTSGESETZ. *§ 53 Vervielfältigungen zum privaten und sonstigen eignen Gebrauch.* Aufgerufen am 26.03.2014 unter http://www.gesetze-im-internet.de/urhg/__53.html

[4] LANDESAKADEMIE für Fortbildung und Personalentwicklung an Schulen (2013, 28. November). *Neue Regeln für das Kopieren ab dem 1.1.2013.* Aufgerufen am 26.03.2015 unter http://lehrerfortbildung-bw.de/sueb/recht/urh/kop_2013/

[5] URHEBERRECHTSGESETZ. § 51 Zitate. Aufgerufen am 26.03.2014 unter http://www.gesetze-im-internet.de/urhg/__51.html

[6] LEHRER-ONLINE (2003, 17. Dezember). *Das Zitatrecht.* Aufgerufen am 26.03.2015 unter http://www.lo-recht.de/zitatrecht.php

[7] MINISTERIUM für Schule und Weiterbildung des Landes Nordrhein-Westfalen (2015). *Urheberrecht: Kopieren und Intranet an Schulen.* Abgerufen am 26.03.2015 unter http://www.schulministerium.nrw.de/docs/Recht/Schulrecht/Verordnungen/Kontext/Urheberrecht/index.html

[8] LANDESAKADEMIE für Fortbildung und Personalentwicklung an Schulen (2013, 28. November). *Neue Regeln für das Kopieren ab dem 1.1.2013.* Aufgerufen am 26.03.2015 unter http://lehrerfortbildung-bw.de/sueb/recht/urh/kop_2013/

[9] LEHRER-ONLINE (2006, 22. September). *Daten von Lehrkräften und sonstigem Schulpersonal.* Aufgerufen am 26.03.2015 unter http://www.lehrer-online.de/lehrkraft-daten.php

[10] GESETZ betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie. § 22. Aufgerufen am 26.03.2015 unter http://www.gesetze-im-internet.de/kunsturhg/__22.html

[11] URHEBERRECHTSGESETZ. *§ 53 Vervielfältigungen zum privaten und sonstigen eignen Gebrauch.* Aufgerufen am 26.03.2014 unter http://www.gesetze-im-internet.de/urhg/__53.html

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Open Content**	**Musik, Videos – kopieren erlaubt?**
Kompetenzen	Die Schülerinnen und Schüler wenden das Lizenzmodell Creative Commons an Beispielen an.	Die Schülerinnen und Schüler schließen aus den Auszügen des Gesetzestextes die wesentliche Merkmale des Urheberrechts und übertragen sie auf Fallbeispiele.
Methoden	Erstellen von Symbolschildern, Internetrecherche, Stichwortzettel, Handyclip	Einschätzen von Fallbeispielen
Material	Arbeitsblatt, Symbolschilder	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Open Content

Creative Commons bietet die Möglichkeit – gerade für Schüler und Studenten – kostenlos und legal Bilder, Fotos, Texte, Videos und Musik zu nutzen. Im Gegenzug könnten auch Schüler ihre Werke als CC-Lizenz zur Verfügung stellen und somit der Allgemeinheit (legal) zugänglich machen. Mit den ersten beiden Arbeitsaufträgen sollen sie die Feinheiten der CC-Lizenzen kennenlernen.
Der erste Arbeitsauftrag verursacht sicherlich etwas kreatives Chaos im Klassenraum. Die Schüler sollen sich als Symbole für die Regeln (by, nc, nd und sa) zu möglichen Kombinationen mit einem Schild vor der Brust aufstellen und die Kombination erläutern. Stehen beispielsweise die Schüler nc und sa zusammen, darf der Name des Urhebers weggelassen und das Werk verändert werden. Das Werk darf aber nicht für kommerzielle Zwecke genutzt werden und nach einer Veränderung muss es unter nc / sa-Lizenz stehen. Vielleicht lassen Sie nach einer Gruppenphase die beste dieser Performances vor der Klasse darstellen?! Die praktische Anwendung der Lizenzbestimmungen soll in der anschließenden Aufgabe gefestigt werden.

Lösungen:
Thomas Claveirole: Nennung des Namens, Weitergabe mit gleicher Lizenz
affnpack: Nennung des Namens, keine kommerzielle Nutzung und Weitergabe mit gleicher Lizenz
vince42: Nennung des Namens, keine Veränderung des Werks

Durch die Erstellung eines Handyvideos, das mit lizenzfreier Musik von Netlabels unterlegt werden soll, können die Jugendlichen das Netlabel-Angebot kennenlernen und praktisch nutzen.

AB 2: Musik, Videos – kopieren erlaubt?

Steigen Sie mit einem Beispiel aus der Tabelle auf dem AB ein und fragen Sie die Einschätzung der Schülerinnen und Schüler dazu ab. Anschließend sollen an dem Originaltext des Urheberrechtsgesetzes die Fallbeispiele überprüft werden. Die genannten Internetadressen
www.respectcopyrights.de und **www.irights.info/** haben weitergehende Informationen in gut aufbereiteter Form.
Lösung:

Fallbeispiel	Erlaubt	Kommentar
Antonio hat die neuesten Spiele von seinem Onkel, er macht dir gerne eine Kopie.	nein	Software zu kopieren ist verboten (außer Sicherungskopie). Es gibt Ausnahmen etwa für Open Source Software.
Bettina möchte sich die gekaufte Tokio-Hotel-CD auf den mp3-Player spielen.	jein	Gekaufte Musik ist nutzbar auf verschiedenen Abspielgeräten, wenn sie nicht kopiergeschützt ist.
Cedric macht eine DVD-Aufnahme seiner Lieblingssendung „Musikantenstadl" – für sich privat.	ja	Aufnahmen aus dem TV sind erlaubt, solange sie nicht weitergegeben oder veröffentlicht werden.
Cedric verkauft diese Aufnahme für 25 Euro auf dem Schulhof.	nein	Ganz klarer Verstoß gegen das UrhG.

Fallbeispiel	Erlaubt	Kommentar
Dieter singt gerne und verteilt seine eigenen Lieder kostenlos auf CD.	ja	Er selbst hat die Rechte daran, außer es handelt sich um fremde Kompositionen (im Sinne von Karaoke), dann ist es nicht erlaubt.
Emily nimmt gerne Musik aus dem Radio auf und hört sie auf dem mp3-Player.	ja	Aufnahmen aus dem Radio sind erlaubt! Es gibt bei den zahllosen Internetradios die Möglichkeit, legal und kostenlos an Musik zu kommen.
Fred hat Angst um seine Original-Software-CD und kopiert sie vorsichtshalber.	jein	Das ist nicht erlaubt. Wenn die Original-CD beschädigt wird, kann er sich an den Software-hersteller wenden.
Fred muss dafür einen Kopierschutz knacken.	nein	Das ist nicht erlaubt. Fred hat Pech, wenn die Original-CD beschädigt wird.
Gerrit fühlt sich wie ein Radio-DJ und macht ein Internet-Podcast mit (fremder) Musik.	nein	Es sei denn, Gerrit zahlt Gebühren an die GEMA. Radiosender können eine monatliche Pauschale abführen und somit alle GEMA-Musik spielen.
Gerrit erhält Beschwerden über die Musikauswahl und macht sein Podcast ohne fremde Musik.	ja	Wenn Gerrit auch Komponist und Textdichter ist und er keine Musik spielt, für die andere die Urheberrechte besitzen.
Gerrit hat eine neue Idee und liest den neuen Harry Potter-Band im Original vor – 23 Stunden lang.	nein	Es sei denn, Gerrit zahlt Gebühren an die GEMA und verwendet keine Tonträger (CDs oder DVDs). Denn die Rechte an Tonträgern liegen nicht bei GEMA, sondern bei den Labels selbst. Er müsste also z. B. Universal um Erlaubnis fragen.
Heinz ist Fan von FC Schalke. Er veröffentlicht das Logo auf seiner privaten Homepage.	nein	Das Logo ist urheberrechtlich und wahrscheinlich auch markenrechtlich geschützt und darf nur mit Einverständnis des Rechteinhabers verwendet werden.
Heinz fotografiert die Stars vom FC Schalke beim Stadtbummel in Düsseldorf.	nein	Das Recht am eigenen Bild ist zwar eingeschränkt für Personen des öffentlichen Interesses, wozu Schalker Profifußballer in Düsseldorf sicherlich gehören. Jedoch gilt dies nur für Fotos, welche diese Personen in ihrem „dienstlichen" Umfeld zeigen. Ein privater Stadtbummel gehört sicher nicht dazu.
Heinz macht tolle Fotos der Schalke-Arena und stellt sie ins Netz.	jein	Die eigenen Fotos von Bauwerken (ohne Menschen, die porträtähnlich zu sehen sind) dürfen veröffentlicht werden, wenn es sich um die Außenansicht handelt. Macht Heinz Fotos vom Innenraum der Arena und veröffentlicht diese ohne Einwilligung der Architekten im Internet, verletzt er deren Urheberrechte.

Lust auf mehr?
Urheberrecht ist auf den ersten Blick ein trockenes Juristenproblem, auf den zweiten Blick jedoch spannend, weil die Kinder und Jugendlichen direkt betroffen sind/sein können. Es stößt auf großes Interesse, die Rechtslage so gut zu kennen, dass man weiß, was erlaubt ist und was nicht (was nicht immer einfach ist – man bekommt auch von Experten oft keine genaue Antwort, weil immer der Einzelfall relevant ist). Das Thema lässt sich gut in ein Projekt mit Produktorientierung einbinden. So könnten die Schülerinnen und Schüler eigene Fallbeispiele aus ihrem Alltag konstruieren und darstellen.

Open Content (1/2)

Zu Beginn des dritten Jahrtausends ärgerten sich viele Menschen über das strenge Urheberrecht, v. a. im Internet. Ein Professor namens Lawrence Lessig schuf deshalb ein Modell, wonach man als Urheber freiwillig bestimmte Nutzungen erlauben kann. Creative Commons (CC) heißt dieses Modell und dieses Zeichen zeigt dir an, dass das Werk unter dieser CC-Lizenz steht:

creative commons

Aber so ganz ohne Regeln geht es auch bei Creative Commons nicht:

Logo	Abkürzung	bedeutet
	by	(by = von) Der Name des Urhebers muss genannt werden.
	nc	(non-commercial = nicht kommerziell) Das Werk darf nicht für kommerzielle verwendet werden, also z. B. nicht verkauft werden.
	nd	(non-derivates = keine Abänderungen) Das Werk darf nicht verändert werden.
	sa	(share alike = genau so zu teilen) Geänderte Versionen des Werkes dürfen nur unter der gleichen Lizenz weitergegeben werden.

Arbeitsaufträge:

1. Die Regeln (by, nc, nd und sa) bei Creative Commons können alle frei miteinander kombiniert werden. Malt euch Symbolschilder und stellt euch im Klassenraum in unterschiedlichen CC-Kombinationen auf. Was bedeuten die Kombinationen im Einzelnen?
2. Wie funktioniert die Google-Suche nach lizenzfreien Werken? Finde es heraus und erkläre es kurz deinem Sitznachbarn (Tipp: Schaue mal unter „Erweiterte Suche").

Open Content (2/2)

Auf vielen Internetseiten werden Inhalte angeboten, die du kostenfrei nutzen darfst, ohne eine spezielle Erlaubnis beim Urheber einholen zu müssen. Bei ***www.flickr.com*** *oder bei Wikimedia Commons findest du zum Beispiel eine Menge Bilder. Die angegebenen Lizenzbestimmungen zeigen dir, was du bei der Verwendung wiederum angeben musst. Häufig musst du den Namen des Urhebers und die Lizenz selbst angeben. Probiere es einmal aus!*

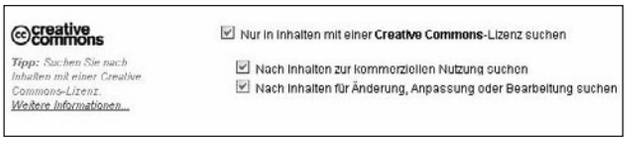


Foto	CC-Lizenz	Autor	Quelle
	by / sa	Thomas Claveirole	http://www.flickr.com/photos/thomasclaveirole/299623633/
	by / nc / sa	affnpack	http://www.flickr.com/photos/affenpack/4635278727/
	by / nd	vince42	http://www.flickr.com/photos/84609865@N00/4998370790/

3. Erkläre die Foto-Beispiele! Unter welcher Lizenz stehen die Fotos? Was darfst du damit machen? Was nicht? Was musst du bei einer Veröffentlichung beachten?

Zusatzaufgabe:
Es gibt noch weitere Beispiele für kostenlos nutzbare Werke, übrigens auch bei Musik. Recherchiere das Stichwort CC-Musik und mache dir dazu einen Stichwortzettel, auf dem du alles sammelst, was du gefunden hast.

Erstellt ein Handyvideo, unterlegt es mit lizenzfreier Musik von einem Netlabel und ladet es auf ein Videoportal.

Recherchetipp:

http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_Allgemein/Flyer_Musik_im_Netz.pdf

www.checked4you.de/netzmusik

http://creativecommons.org/legalmusicforvideos

Musik, Videos – kopieren erlaubt? (1/2)

Es gibt in Deutschland viele Gesetze, eines davon ist das „Urheberrechtgesetz". Es soll diejenigen schützen, die Werke oder andere Schutzgegenstände (gehören zum geistigen Eigentum) geschaffen haben. „Materielles Eigentum" zu stehlen ist bekanntermaßen ja auch verboten. Hier findest du den genauen Wortlaut:
www.gesetze-im-internet.de/urhg

Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz)

§ 1 Allgemeines

- Die Urheber von Werken der Literatur, Wissenschaft und Kunst genießen für ihre Werke Schutz nach Maßgabe dieses Gesetzes.

§ 2 Geschützte Werke

- (1) Zu den geschützten Werken der Literatur, Wissenschaft und Kunst gehören insbesondere:
- 1. Sprachwerke, wie Schriftwerke, Reden und Computerprogramme;
- 2. Werke der Musik;
- 3. pantomimische Werke einschließlich der Werke der Tanzkunst;
- 4. Werke der bildenden Künste einschließlich der Werke der Baukunst und der angewandten Kunst und Entwürfe solcher Werke;
- 5. Lichtbildwerke einschließlich der Werke, die ähnlich wie Lichtbildwerke geschaffen werden;
- 6. Filmwerke einschließlich der Werke, die ähnlich wie Filmwerke geschaffen werden;
- 7. Darstellungen wissenschaftlicher oder technischer Art, wie Zeichnungen, Pläne, Karten, Skizzen, Tabellen und plastische Darstellungen.
- (2) Werke im Sinne dieses Gesetzes sind nur persönliche geistige Schöpfungen.

Arbeitsaufträge:

1. Lies die Gesetze aufmerksam durch!
   Die Tabelle zeigt dir frei erfundene Beipiele.

Fallbeispiel	Erlaubt? ja/nein	Deine Begründung
Antonio hat die neuesten Spiele von seinem Onkel, er macht dir gerne eine Kopie.		
Bettina möchte sich die gekaufte Tokio-Hotel-CD auf den mp3-Player spielen.		
Cedric macht eine DVD-Aufnahme seiner Lieblingssendung „Musikantenstadl" – für sich privat.		
Cedric verkauft diese Aufnahme für 25 Euro auf dem Schulhof.		
Dieter singt gerne und verteilt seine eigenen Lieder kostenlos auf CD.		

Musik, Videos – kopieren erlaubt? (2/2)

Fallbeispiel	Erlaubt? ja/nein	Deine Begründung
Emily nimmt gerne Musik aus dem Radio auf und hört sie auf dem mp3-Player.		
Fred hat Angst um seine Original-Software-CD und kopiert sie vorsichtshalber.		
Fred muss dafür einen Kopierschutz knacken.		
Gerrit fühlt sich wie ein Radio-DJ und macht ein Internet-Podcast mit (fremder) Musik.		
Gerrit erhält Beschwerden über die Musikauswahl und macht sein Podcast ohne fremde Musik.		
Gerrit hat eine neue Idee und liest den neuen Harry-Potter-Band im Original vor – 23 Stunde lang.		
Heinz ist Fan von FC Schalke 04. Er veröffentlicht das Logo auf seiner privaten Homepage.		
Heinz fotografiert die Stars vom FC Schalke 04 beim Stadtbummel in Düsseldorf.		
Heinz macht tolle Fotos der Schalke-Arena und stellt sie ins Netz.		
Jasmin filmt gerne mit dem Handy. Sie tut dies in der Umkleidekabine.		
Jasmin filmt auch im Unterricht. Der Film macht sich gut auf YouTube.		
Jasmin filmt mit Freundinnen und fragt die Eltern, ob sie den Film veröffentlichen darf.		
Karl hat endlich die gute Download-Seite gefunden. Hier findet er alle teure Software.		

2. Fülle die Tabelle aus und vergleiche deine Lösungen mit deinem Nachbarn!

3. Finde mithilfe folgender Seiten heraus, was erlaubt und was verboten ist:

www.respectcopyrights.de *und*

www.irights.info

6|1 Cyber-Mobbing
6|2 Virtualität und Realität
6|3 Online-Sucht
6|4 Werbung und Abzocke

6

Worauf wir achten sollten: Herausforderungen im Netz

Cyber-Mobbing

Mobbing unter Kindern und Jugendlichen ist ein altbekanntes Phänomen. Doch während es sich früher auf vielleicht wenige Momente und Orte (z. B. in den Pausen oder dem Schulweg) beschränkte, ist es längst in die digitale Welt ausgeweitet. Und das bedeutet möglicherweise Mobbing rund um die Uhr und mit einem unüberschaubar großen Publikum. In den letzten Jahren hat sich dafür der Begriff **Cyber-Mobbing** durchgesetzt.

Was ist Mobbing?

Um „Cyber"-Mobbing zu verstehen, ist es sinnvoll die Abgrenzung zum herkömmlichen Mobbing zu verdeutlichen. Mobbing bedeutet:

- einen anderen absichtlich zu erniedrigen, zu demütigen oder zu schikanieren,
- jede Form gewalttätigen Handelns: mit Worten, mit Gestik und Mimik, durch Ausgrenzung, Beleidigungen, Verleumdungen, Gerüchte, Körperverletzung oder anderes
- Attacken gegen eine bestimmte Person, die wiederholt und über einen längeren Zeitraum stattfinden,
- die Täterinnen und Täter sind physisch oder psychisch stärker oder vermeintlich stärker als die Opfer und
- ein Opfer hat kaum eine Möglichkeit, sich aus eigener Kraft aus dieser Situation der Ohnmacht zu befreien.

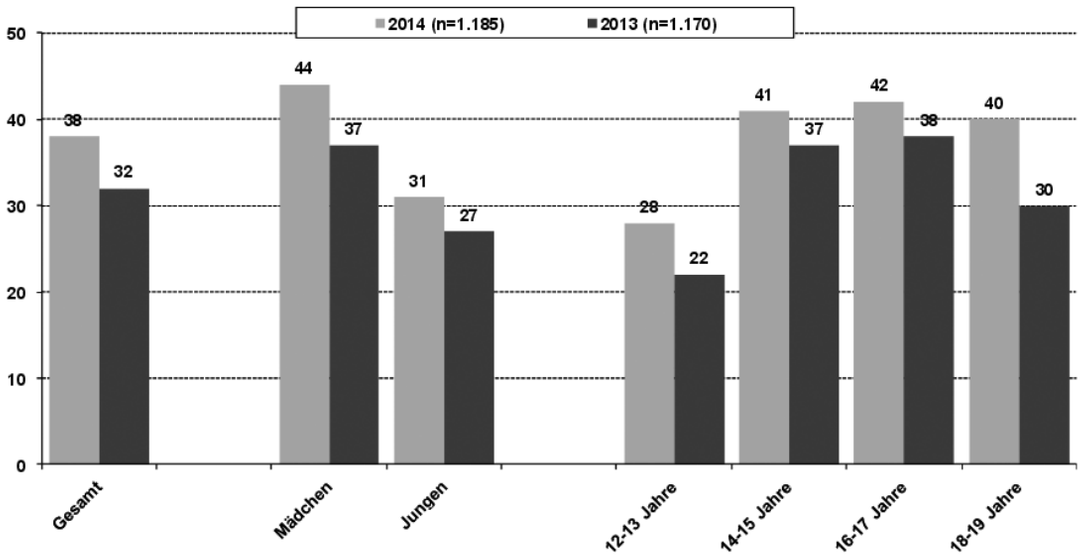
Anders als bei einem Streit oder einem Konflikt geht es bei Mobbing nicht um eine Sachfrage, sondern um Bosheit und Willkür, immer mit dem Ziel, das Opfer fertig zu machen. Es geht genau darum, dass sich der Täter mächtig fühlt und das Opfer ohnmächtig.

„Rund um die Uhr und überall"

Was Cyber-Mobbing von Mobbing unterscheidet: Was sich in der realen Welt abspielt, findet sich in der digitalen wieder. Mit Cyber-Mobbing wird Mobbing mithilfe digitaler Medien bezeichnet. Dabei werden alle Technologien benutzt, die zur Verfügung stehen: Schmäh-Videos über YouTube, Beleidigungen per E-Mail, Drohungen in einer SMS, mittels WhatsApp oder sexuell anzügliche Anrufe auf dem Mobiltelefon. Eine besondere Rolle scheinen Social Communitys wie Facebook zu spielen, denn ihre Funktionen, wie das Kommentieren von Inhalten, das Veröffentlichen von Fotos, das Verfassen von Einträgen oder das Gründen von Gruppen, bieten neben dem positiven Nutzen auch Möglichkeiten zum Mobbing. Noch perfider wird die Sache mit so genannten „Fake-Profilen", bei denen die Identität eines anderen vorgespielt wird und in dessen Namen unschöne Dinge veröffentlicht werden.

Die JIM-Studie 2014 fragte ab, ob es im Bekanntenkreis jemanden gibt, der schon einmal im Internet oder über das Handy fertig gemacht wurde. Mehr als ein Drittel der Befragten bejahte dies.

Gibt es jemanden in deinem Bekanntenkreis, der schon mal im Internet oder übers Handy fertig gemacht wurde?



Quelle: MPFS (2014); Angaben in %; Basis: Internet-Nutzer (2014: n=1.185; 2013: n=1.170) [1]

Umfrage in NRW

Besonders viel Aufsehen in den Medien erregte eine Umfrage, die das Forschungsinstitut FORSA im Auftrag der Techniker Krankenkasse in Nordrhein-Westfalen durchführte. Das Ergebnis war, dass ein Drittel der Schülerinnen und Schüler in NRW bereits einmal Opfer von Cyber-Mobbing war.[2] Trotzdem darf man nicht vergessen, dass alle Umfragen zum Thema auch kritisch zu hinterfragen sind. So gilt es bspw. zu beachen, welche Definition von Cyber-Mobbing zugrunde gelegt wurde oder welche Forschungsmethode (bspw. Online-Fragebogen oder Interviews) angewandt wurde. Mittlerweile gibt es eine Reihe auch internationaler Untersuchungen dazu.

Aus der Praxis

Dieses Thema verdient in der schulischen Arbeit breiten Raum. Es ist einfach wichtig, dass Kinder und Jugendliche die möglichen Konsequenzen kennen, wenn jemand – auch ohne böse Absicht – im Internet geärgert wird. Letztendlich und abseits von allen Fachfragen, sollte immer die Vermittlung des wichtigsten Aspekts im Vordergrund stehen: ein ***respektvoller Umgang*** *miteinander!*

Rasend schnell und unüberschaubar

Videos, Fotos und Texte in Form von Kommentaren verbreiten sich unter Jugendlichen in Zeiten der ununterbrochenen Handy-Kommunikation rasend schnell. Kaum veröffentlicht („gepostet" genannt), wissen es alle „Freunde" auf Facebook. Heute bei YouTube eingestellt, kann ein Video schon morgen Tausende Zuschauerinnen und Zuschauer haben. Und ein Gedanke kann für das Opfer besonders quälend sein: Es weiß nicht, wer das verletzende Material gesehen hat, das Publikum ist unbekannt. Bei klassischem Mobbing wissen normalerweise nur wenige um eine Attacke, weil die Täterinnen und Täter eher in einer kleinen Gruppe mit ihren Taten angeben.

Im Internet können die Angreifer vermeintlich anonym handeln. Sie brauchen zunächst keine Konsequenzen zu fürchten, dadurch handeln sie vielleicht enthemmter. Wer das Leiden seines Opfers nicht sieht, kann die Folgen seines Angriffs auch schlechter einschätzen und weniger mitfühlen.

Die Folgen für das Opfer können in beiden Fällen verheerend sein und von Unbehagen und Hilflosigkeit über Selbstzweifel und Angst bis hin zur Verzweiflung führen, an deren Ende möglicherweise der Suizid steht.

Die entstehenden Dynamiken durch die Nutzung neuer Medien begünstigen zudem das Auftreten von Racheaktionen, bei denen das ursprüngliche Opfer selbst zum Täter wird. Die Attacken können sich gegenseitig aufschaukeln und so den Mobbing-Prozess immer weiter verschlimmern.

Was ist neu?

- Eingriff rund um die Uhr, auch in das Privatleben
- Publikum ist unüberschaubar groß
- Publikum ist unbekannt
- Inhalte verbreiten sich extrem schnell
- Täter handeln anonym (geringe Konsequenzen, geringe Kosten für den Bully)
- Täter handeln enthemmter (Online-Enthemmungseffekt)
- körperliche Stärke ist unwichtig
- Folgen können schwerer abgeschätzt werden (Empathielücke)
- zusätzlich Visualisierungen (zu Gerüchten bspw.)

„Cyber-Mobbing hat viele Gesichter"

Welche Formen gibt es?

Die Forscherin Nancy Willard hat im Jahre 2007 eine Systematik der Formen von Cyber-Mobbing erstellt[3]:

- Beleidigung, Beschimpfung
- Belästigung
- Anschwärzen, Gerüchte verbreiten
- Auftreten unter falschem Namen
- Bloßstellen und Betrügerei
- offene Androhung von Gewalt
- Ausschließen

Ergänzen könnte man diese Auflistung noch um **„Happy Slapping"**, bei dem ein Opfer verprügelt wird, damit die Video-Aufnahmen per Handy ins Netz gestellt werden können.

Bystander im Mobbing-Prozess

Mobbing ist nicht nur ein Prozess zwischen zwei Personen sondern immer ein größeres Konstrukt. Im schulischen Kontext ist z. B. die ganze Klasse betroffen. Außenstehende, die über die Mobbing-Attacken Bescheid wissen, aber weder die Täter noch die Opfer unterstützen, werden als Bystander bezeichnet. Ihnen kommt in der Lösung des Mobbing-Prozesses eine Schlüsselrolle zu, denn sie können entscheidenden Einfluss auf den Verlauf nehmen. Sie können einerseits durch die weitere Unterstützung für die Täterseite die Schikanen verschlimmern, andererseits aber auch durch die sichtbare Verteidigung des Opfers – ob nun online oder von Angesicht zu Angesicht – die Täter zum Aufhören bewegen. Dabei können schon kleine Gesten der Unterstützung oder das Ansprechen der Täter weitere Handlungen positiv beeinflussen. Außenstehende Jugendliche scheinen jedoch oft das Gefühl zu haben, selbst nichts an der Situation verändern zu können.[4] Deshalb ist es besonders wichtig, die Einflussmöglichkeiten jedes einzelnen hervorzuheben!

Was tun als Betroffener?
Den wohl wichtigsten Tipp, den man jedem Opfer von Cyber-Mobbing geben kann, lautet: **Rede darüber!** Suche dir eine Vertrauensperson, die dir zuhört. Das kann sehr schwierig sein, weil dies der Punkt ist, an dem sich eingestanden werden muss, ein Opfer geworden zu sein. Der Punkt, an dem die Fehler bei sich selbst gesucht werden, die Opfer sich schämen und sich verantwortlich für die Situation machen. Der Schritt, sich einem anderen Menschen anzuvertrauen ist also ein großer! Wer niemanden findet, sollte das kostenlose Kinder- und Jugendtelefon (0800.1110333), die so genannte **Nummer gegen Kummer** wählen. Zudem können sich Betroffene mit ihren Problemen auch an **juuuport.de** wenden – eine Selbstschutzplattform von Jugendlichen für Jugendliche im Netz.

Zudem sollten Opfer Beweise sichern, was in der digitalen Welt einfacher ist als beim klassischen Mobbing. Die Täter hinterlassen Texte, Fotos oder Videos, die man auf dem eigenen Computer speichern und ausdrucken kann. Damit kann man das Gegenstück zu einem **Mobbing-Tagebuch** erstellen, in dem man alle Vorkommnisse mit Datum, Ort und Zeit notiert. Somit hat man als Opfer auch schriftliche Beweise in der Hand, sollte es nötig werden, die Attacken belegen zu müssen – gegenüber Eltern, Lehrern oder der Polizei.
Im Klassenraum und im Büro ist es schwierig dem Täter aus dem Weg zu gehen, bei digitalen Medien kann man ihn aber leicht sperren und den Zugriff erschweren. Mit einer **neuen Handy-Nummer**, dem **Spam-Filter** bei E-Mails, dem **Blockieren** im Chatroom, dem **Löschen** aus der Freundesliste usw. kann man den Täter ausschließen und ignorieren. Wichtig ist es zudem, nicht auf die Attacken zu antworten: Einerseits, um dem Täter keine neue Vorlage für die nächste Attacke zu geben, andererseits, um nicht selbst in die Täterrolle zu geraten.

Schließlich bieten viele Netzwerke, Webseiten etc. die Möglichkeit einen Missbrauch zu melden. Davon sollten Opfer Gebrauch machen, denn der Täter erfährt nicht, wer ihn gemeldet hat. Nicht zu vergessen ist, dass Beleidigungen, Verleumdungen oder üble Nachrede, Betrug oder das Einstellen von Fotos (fremde bzw. mit fremden Personen) Straftaten sind. Hier sollte man sich als letzte Konsequenz nicht scheuen, einen Rechtsanwalt einzuschalten und eine Strafanzeige zu erstatten.

Tipp: *Was tun als Betroffener?*

1. *Rede darüber!*
2. *Sichere Beweise! Führe ein Mobbing-Tagebuch.*
3. *Sperre den Täter!*
4. *Nutze die Meldemöglichkeiten!*
5. *Suche professionelle Hilfe.*

Links und weiterführende Informationen

Webseiten

www.klicksafe.de/themen/kommunizieren/cyber-mobbing/
Ausführlicher Themenbereich auf klicksafe.de zum Thema Cyber-Mobbing

www.klicksafe.de/service/fuer-lehrende/zusatzmodule-zum-lehrerhandbuch/#c1524
Das klicksafe Zusatzmodul *Was tun bei Cyber-Mobbing?* mit weitergehenden Informationen und Unterrichtsmaterialien

www.klicksafe.de/service/materialien/broschueren-ratgeber/ratgeber-cyber-mobbing/
Broschüre *Ratgeber Cyber-Mobbing. Informationen für Eltern, Pädagogen, Betroffene und andere Interessierte* von klicksafe

www.nummergegenkummer.de
Anonyme und kostenlose Beratung am Kinder- und Jugendtelefon oder am Elterntelefon

www.juuuport.de
Beratungsportal von Jugendlichen für Jugendliche

www.bke-beratung.de
Angebot für Jugendliche und Eltern der Bundeskonferenz für Erziehungsberatung (bke)

www.no-blame-approach.de
Interventionsansatz bei Mobbing an der Schule

Endnoten

[1] MEDIENPÄDAGOGISCHER Forschungsverbund Südwest (MPFS) (Hrsg.) (2014). *JIM-Studie 2014, Jugend, Information, (Multi-)Media, Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland* (S. 40). Aufgerufen am 05.03.2015 unter http://www.mpfs.de/fileadmin/JIM-pdf14/JIM-Studie_2014.pdf

[2] TECHNIKER Krankenkasse (2011). TK-Meinungspuls Gesundheit Kurzerhebung *„Cybermobbing"*. Zusammenfassung der wesentlichen Ergebnisse. Aufgerufen am 16.04.2015 unter http://www.tk.de/centaurus/servlet/contentblob/360342/Datei/3452/TK-Meinungspuls-Gesundheit-Kurzerhebung-Cybermobbing.pdf

[3] WILLARD, N. E. (2007). Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress. Champaign, Illinois: Research Press.

[4] PFETSCH, J. (2011). Studie *„Bystander von Cyber-Mobbing"*. Technische Universität Berlin. Aufgerufen am 09.04.2015 unter https://www.paedpsy.tu-berlin.de/fileadmin/fg236/Jan_Pfetsch/Pfetsch_Kurzbericht_Studie_Bystander_von_Cyber-Mobbing.pdf

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Let's fight it together**	**Recht und Gesetz**
Kompetenzen	Die Schülerinnen und Schüler erkennen an einem Film-Beispiel grundlegende Strukturen und Rollen beim Cyber-Mobbing.	Die Schülerinnen und Schüler beurteilen anhand der deutschen Gesetzeslage zum Thema Cyber-Mobbing (s. u.) in Form eines eigenen Gesetzes die Notwendigkeit einer rechtlichen Norm zur Bekämpfung von Cyber-Mobbing.
Methoden	Filmanalyse, Blitzlicht, Plenum, Kleingruppen	Partnerinterview, Klassengespräch, Partnerarbeit, Kleingruppen
Material	Arbeitsblatt, Film (s. u.)	Arbeitsblatt
Zeit (in Minuten)	90	135
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Let's fight it together	Die Schülerinnen und Schüler sollen anhand des Fallbeispiels (Film) die grundlegende Problematik des Cyber-Mobbing kennenlernen, über mögliche Motive der handelnden Personen und über mögliches eigenes Verhalten reflektieren können. Der Film „Let´s fight it together" ist bereits ein wenig älter, zeigt aber immer noch sehr gut und deutlich grundlegende Strukturen und Rollen. Mit einem „Blitzlicht" sollen die Schülerinnen und Schüler zunächst frei ihre Eindrücke des Films wiedergeben. Mit einem Arbeitsblatt können die Handlungsweisen und die Gründe aller handelnden Personen erarbeitet werden. Zum Schluss steht in einem Unterrichtsgespräch die Frage, wie jeder Einzelne anstelle der Personen im Film gehandelt hätte.
AB 2: Recht und Gesetz	Die Schülerinnen und Schüler sollen sich über die Straflage im Fall von Cyber-Mobbing informieren und eine Gesetzesvorlage dazu formulieren können. Nach der Methode „Partnerinterview", das sich auf einen Text zum Thema bezieht, sollen die Schülerinnen und Schüler in Kleingruppen die in Frage kommenden Gesetze in Form eines Plakates visualisieren und eine Formulierung für ein eigenes spezielles Gesetz finden. Lassen Sie die Schülerinnen und Schüler dazu im Internet recherchieren.

Lust auf mehr?

- Anti-Mobbing-Video-Tipps: „Too late" – Schüler lesen Social Media Posts auf Profilen von Mobbingopfern, die Selbstmord begangen haben:
  www.youtube.com/watch?v=n1HrCiLK7wc
  Was bedeutet die Aussage: Be nice. Now.
- Video Gegen Mobbing – von Schüler Benjamin Drews:
  https://www.youtube.com/watch?v=sgRSO72u8aw
- Vielleicht haben Ihre Schülerinnen und Schüler Lust, selbst ein Anti-Mobbing Video zu produzieren?

„Let's fight it together"

„Let's fight it together" – das bedeutet übersetzt etwa „Lasst es uns zusammen bekämpfen". So heißt ein kleiner Film von 7 Minuten Länge, der in Großbritannien mit Schülerinnen und Schülern gedreht wurde. (Lass Dich nicht abschrecken, er ist auf Englisch, aber das meiste wirst Du verstehen!)..

Quelle: Crown Copyright. Mit freundlicher Genehmigung von Childnet International.

Arbeitsaufträge:

1. Schaut Euch den Spot „Let's fight it together" aus Großbritannien unter folgender Internetadresse an:
   www.digizen.org/cyberbullying/fullfilm.aspx
   mit deutschen Untertiteln: **www.digizen.org/cyberbullying/fullfilm_de.aspx**

2. Schildert Eure Eindrücke zum Film! Benutzt dazu die Methode „Blitzlicht", dazu muss jede Schülerin/jeder Schüler reihum zwei Sätze sagen, alle anderen dürfen dies nicht kommentieren.

3. Wie sind die Eindrücke von dem Film in Eurer Klasse? Versucht, möglichst viele Aussagen zusammenzufassen, und notiert diese an der Tafel.

4. Im Film spielen verschiedene Personen mit. Nun sollt Ihr Euch den Figuren nähern. Füllt dazu die folgende Tabelle aus („Wie" und „Warum"):

Personen	Joe (die Hauptperson, das Opfer)	Kim („die Täterin")	Lehrerin	Mutter	Rob, der Mitläufer
Wie? (So verhält sich…)					
Warum? (Mögliche Gründe für das Verhalten)					
Und wir? (So hätten wir uns verhalten)					

5. Überlege nun zunächst alleine, danach diskutiere diese Frage mit Deinem Sitznachbarn: Wie hättest Du Dich anstelle der Personen im Film verhalten?

6. Einige Dich mit Deinem Partner auf ein mögliches Verhalten, und notiere dies ebenfalls in der Tabelle („Und wir?").
   Redet nun in der Klasse über Eure Tabelleneinträge.

Recht und Gesetz (1/2)

„Jeder, der denkt, das Internet sei anonym, der glaubt auch, er werde im Kaufhaus nicht gefilmt" – so oder so ähnlich könnte man böswillig sagen, wenn Täter von Cyber-Mobbing sich sicher fühlen. Bei jedem Zugriff auf das Internet werden (in Deutschland übrigens für sechs Monate) die Verbindungs-daten beim Provider gespeichert. Es ist also leicht heraus-zufinden, wer wann und wo im Internet unterwegs war. Und bei einer möglichen Straftat darf ein Richter diese Verbindungs-daten kontrollieren.

Doch auch wenn man den Täter oder die Täterin erwischt, was passiert dann? Welche Strafen drohen den Tätern?

1. Arbeitsauftrag: Gesetze kennenlernen
Leider gibt es (noch?) keine eigenen Gesetze zu Cyber-Mobbing. Es greifen aber mehrere Gesetze des Strafgesetzbuches (StGB).
Lest die Gesetze bitte in Form eines „Partnerinterviews".

Methode „Partnerinterview"
Zu zweit mit Partner A und Partner B. Beide lesen, und danach fasst Partner A das Wichtigste zusammen, Partner B wiederholt mit den Worten „Habe ich dich richtig verstanden, dass …?". Dann Wechsel der Rollen – aber Vorsicht! Jeder darf zwei Fehler einbauen, die der andere finden muss!

§ 185 Beleidigung
Die Beleidigung wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe und, wenn die Beleidigung mittels einer Tätlichkeit begangen wird, mit Freiheits-strafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§ 186 Üble Nachrede
Wer in Beziehung auf einen anderen eine Tatsache behauptet oder verbreitet, welche denselben verächt-lich zu machen oder in der öffentlichen Meinung herabzuwürdigen geeignet ist, wird, wenn nicht diese Tatsache erweislich wahr ist, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe und, wenn die Tat öffentlich oder durch Verbreiten von Schriften (§ 11 Abs. 3) begangen ist, mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§ 187 Verleumdung
Wer wider besseres Wissen in Beziehung auf einen anderen eine unwahre Tatsache behauptet oder verbreitet, welche denselben verächtlich zu machen oder in der öffentlichen Meinung herabzuwürdigen oder dessen Kredit zu gefährden geeignet ist, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe und, wenn die Tat öffentlich, in einer Versammlung oder durch Verbreiten von Schriften (§ 11 Abs. 3) begangen ist, mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

§ 238 Nachstellung
(1) Wer einem Menschen unbefugt nachstellt, indem er beharrlich
1. seine räumliche Nähe aufsucht,
2. unter Verwendung von Telekommunikationsmitteln oder sonstigen Mitteln der Kommunikation oder über Dritte Kontakt zu ihm herzustellen versucht,
3. unter missbräuchlicher Verwendung von dessen personenbezogenen Daten Bestellungen von Waren oder Dienstleistungen für ihn aufgibt oder Dritte veranlasst, mit diesem Kontakt aufzunehmen,
4. ihn mit der Verletzung von Leben, körperlicher Unversehrtheit, Gesundheit oder Freiheit seiner selbst oder einer ihm nahe stehenden Person bedroht oder
5. eine andere vergleichbare Handlung vornimmt und dadurch seine Lebensgestaltung schwerwiegend beeinträchtigt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Auf Freiheitsstrafe von drei Monaten bis zu fünf Jahren ist zu erkennen, wenn der Täter das Opfer, einen Angehörigen des Opfers oder eine andere dem Opfer nahe stehende Person durch die Tat in die Gefahr des Todes oder einer schweren Gesundheits-schädigung bringt.

§ 22 (KUG/KunstUrhG) Recht am eigenen Bild
Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden … Das Recht am eigenen Bild oder Bildnisrecht ist eine besondere Ausprägung des allgemeinen Persönlich-keitsrechts. Es besagt, dass jeder Mensch grundsätzlich selbst darüber bestimmen darf, ob überhaupt und in welchem Zusammenhang Bilder von ihm veröffent-licht werden.

Recht und Gesetz (2/2)

2. Arbeitsauftrag: Warnschilder malen
Teilt Euch bitte in 4er-Gruppen auf. Wendet diese Gesetze auf (ausgedachte oder tatsächliche) Cyber-Mobbing-Fälle an! Malt dazu ein Warnschild mit den möglichen Konsequenzen als Plakat.
Vergleicht anschließend Eure Warnschilder.
Welches ist am deutlichsten?

3. Arbeitsauftrag: Ein eigenes Gesetz formulieren
Wie könnte Eurer Meinung nach ein eigenes Gesetz gegen Cyber-Mobbing lauten? Versucht bitte, eines zu formulieren, das die Besonderheiten des „Cyber"-Mobbings berücksichtigt: Ihr könnt im Internet recherchieren, ob es in anderen Ländern bereits ein Gesetz gegen Cyber-Mobbing gibt.

Tipp:
Auf der Webseite **www.juuuport.de** *beraten Jugendliche andere Jugendliche, wenn sie Opfer von Cyber-Mobbing geworden sind. Schau doch mal vorbei!*

Mein Gesetz gegen Cyber-Mobbing:

.....

.....

.....

.....

.....

.....

.....

.....

Virtualität und Realität

Unsere Lebenswelt wird immer stärker von virtuellen Elementen durchdrungen.[1] Dabei ist von einer Virtualisierung die Rede. Diese äußert sich z. B. in einer Entmaterialisierung von Lebensvorgängen wie der Arbeit am Bildschirm, Videokonferenzen oder dem Einkaufen über das Internet.

> *Es gibt für das 21. Jahrhundert die Idee des bekannten Physikers Michio Kaku eines* ***„ubiquitous computing"*** *(zu Deutsch etwa: Rechnerallgegenwart): Vom „smart house" zum „intelligent planet" mit einem „Internet der Dinge" und einer totalen Vernetzung![2]*

Was auf den ersten Blick scheint wie eine akademische Diskussion hat doch weitreichende praktische Konsequenzen. Kinder und Jugendliche bewegen sich zunehmend in digital konstruierten Räumen, die nur virtuell existieren. Dort kommunizieren sie mit echten Menschen, die aber unter Umständen eine virtuelle Identität angenommen haben. All dies zu erkennen, einzuordnen und die richtigen Konsequenzen zu ziehen, ist eine große Herausforderung. Insbesondere für junge Menschen, die weniger reale Lebenserfahrung mitbringen, die sie zum Vergleich heranziehen können. Die Frage, wer hinter einem Kommunikationspartner steckt, ist in der über das Internet vermittelten Kommunikation einfach schwierig. Und während Erwachsene oft eine gesunde Skepsis beweisen, zeigen Kinder und Jugendliche hier ihre Naivität, die sie entwicklungsbedingt besitzen dürfen.

Alle sind Freunde

Erschwerend kommt hinzu, dass viele Begriffe aus der realen Welt für digitale Zwecke verwendet werden und somit die Unterscheidung erschweren, zum Beispiel „**Chat-Partner**" und vor allem das Wort **„Freund",** das für alle Facebook-Kontakte verwendet wird. „Du bist jetzt mit Kevin befreundet" kostet uns einen Mausklick – ein großer Unterschied zur Realität, wo (echte, tiefe) Freundschaft sehr kostbar und selten ist.

Ein junges Phänomen

Die Erfahrungen der Menschheit mit virtuellen Identitäten in Form von Geschichten sind alt und mit Büchern seit einigen Jahrhunderten eingeübt. Selbst fiktive Figuren in Bild und Ton gibt es seit Aufkommen des Kinos und seit zwei Generationen mit dem Fernsehen. Doch selbst hier haben Jüngere Schwierigkeiten Fiktion von Realität zu unterscheiden. Erinnert sei an TV-Formate des **„scripted reality"**, bei dem Schauspieler so tun, als handele es sich um eine Dokumentation (Beispiele sind „Familien im Brennpunkt" auf RTL, „Pures Leben" auf Sat.1 oder „Verklag mich doch" im Kanal VOX). Die Möglichkeiten einer medial vermittelten Unterhaltung sind massenhaft erst seit den Zeiten des Telefons möglich. Doch erst mit dem Aufkommen des Internets, also etwa seit Mitte der 1990er Jahre, sind das Versenden von E-Mails, das Chatten, Skypen und „Posten" von Nachrichten zur Selbstverständlichkeit geworden.

Real-Erfahrungen unabdingbar

Real-Erfahrungen sind für junge Menschen besonders wichtig: Nur so lernen sie mit allen Sinnen, verknüpfen Situationen beispielsweise mit Gerüchen, Stimmungen etc. Das eindrücklichste Beispiel bietet wohl der Vergleich eines Tierfilms mit einem Ausflug in den Wald. Psychologen und Neurobiologen sprechen hier auch gerne von der Entwicklung von **Intelligenz, Kreativität, Empathie** und **Sozialkompetenz,** die gefördert wird, wenn viele Sinne angesprochen werden.[3] Beim Chat werden viele dieser Eindrücke ausgeblendet und die Kommunikation erfolgt alleinig über Schriftzeichen, als Ersatz für den Ausdruck von Gefühlen dienen die „Emoticons" wie der berühmte Smiley :-). Jede medial vermittelte Kommunikation wird – bis zur Erfindung eines „Holo-Decks" wie im Raumschiff Enterprise – ärmer sein als die Realbegegnung mit Menschen.

In Sozialen Netzwerken

Das Netz ist unkontrollierbar, unüberschaubar und vor allem: frei zugänglich. Vielen, die Zuhause in ihren eigenen vier Wänden vor dem Bildschirm sitzen, ist nicht klar, welcher Öffentlichkeit sie sich gerade gegenüber befinden.
Gerade Soziale Netzwerke vermitteln dem Nutzer das Gefühl, sich in einem begrenzten Raum, einer geschlossenen Benutzerguppe zu befinden. Diese Annahme ist trügerisch, denn es gibt im Netz **keine Schutzräume.** Selbst in Netzwerken, die nur für Jugendliche angelegt sind und in die man beispielsweise nur über eine Einladung kommt, tummeln sich trotz Kontrollvorkehrungen, Selbstkontrollmechanismen und Moderationsfunktionen, ebenso wie in Chats, Erwachsene mit unlauteren Absichten.

Naivität junger Nutzer

Gerade junge Nutzer zeigen sich in Sozialen Netzwerken oft sehr naiv und immer aufreizender, auch – oder vielleicht gerade des Reizes wegen – in virtuellen Umgebungen, die nicht für ihr Alter bestimmt sind und geben dort viele persönliche Daten preis. Problematisch ist, dass gerade Kinder die Tragweite eines freigiebigen Umgangs mit personenbezogenen Daten wie Name, Alter oder gar Adresse im Internet generell nicht überblicken können. Die Vorkehrungen der Betreiber, beispielsweise als Nutzer bei der Anmeldung zustimmen zu müssen, die Bedeutung der Datenspeicherung und -verarbeitung verstanden zu haben, sind in der Regel völlig unzureichend. Sie können nur als minimale Hürde gesehen werden und müssten an die Nutzungsrealitäten angepasst, also zum Beispiel im Sinne einer sicheren Altersverifikation nachgebessert werden.

Die Möglichkeit, sich unter einem Pseudonym in Sozialen Netzwerken aufzuhalten, ist gerade für Kinder und Jugendliche eine richtige Maßnahme. Allerdings widerspricht sie – und das wird auch immer wieder von den Anbietern selbst kommuniziert – den eigentlichen Grundsätzen sozialer Plattformen: den Prinzipien der Auffindbarkeit, der Kommunikation und der Vernetzung.

Keine Gewissheit über die tatsächliche Identität
Eines steht fest: Man kann sich nie sicher sein, mit wem man gerade kommuniziert. Selbst in Gesprächen unter Freunden ist es möglich, dass das Handy in diesem Augenblick in fremden Händen ist. Bei der medialen Kommunikation gibt es keine Sicherheit über

- den Aufenthaltsort
- das Aussehen
- den Namen
- das Alter
- das Geschlecht
- u.v.a. (kurz: der tatsächlichen Identität)

Kinder müssen dies erst lernen, aber vielen Jugendlichen ist es durchaus bewusst. Trotzdem gibt es immer wieder Fälle, bei denen bspw. Mädchen auf Chat-Partner hereinfallen und sich Hals über Kopf verlieben, ohne das Gegenüber gesehen zu haben, geschweige denn zu kennen. In unbekannten Chatpartnern sehen Nutzer gerne das, was sie sehen möchten. Kurze Beschreibungen über das Äußere und über Eigenschaften werden mit den eigenen Vorstellungen darüber in Einklang gebracht. Diese interaktive Projektionsfläche führt dazu, dass ein Gespräch schnell vertraulich werden kann, schließlich sind einem die eigenen Vorstellungen gut bekannt.
Hat das Gegenüber böse Absichten, beispielsweise Pädokriminelle, sind diese Täter sehr gut darin, die Situation zu durchschauen und das tatsächliche Vertrauen virtuell zu erlangen. Zweifellos gehen Kinder oder Jugendliche mit einem persönlichen Treffen außerhalb des Chats ein großes Risiko ein.
Eine herbe Enttäuschung ist dabei die geringste, ein sexueller Übergriff durch einen Pädokriminellen eine der größtmöglichen Gefahren. Allerdings handelt es sich in der Regel um seltene Einzelfälle. Dabei kann der Täter seine Identität bis zum Treffen verschleiern, teilweise enthüllt er sie aber schon im Vorfeld. Die Anbahnung spielt sich meist in drei Schritten ab:

1. Der Täter versucht das Vertrauen des potenziellen Opfers zu gewinnen, um es gezielt nach Name und Adresse auszuhorchen.
2. Durch Kontakt per Telefon oder SMS versucht der Täter sich zu versichern, dass er es auch wirklich mit einem Kind zu tun hat, um seine Erfolgsaussichten abzuwägen.
3. Der Täter vereinbart mit dem Opfer ein Treffen an einem für Kinder attraktiven Ort z. B. einem Zoo, einem Schwimmbad o.Ä.

Aus der Praxis
Viele Schülerinnen und Schüler verdrehen mittlerweile die Augen, wenn Erwachsene ihnen erzählen, dass eine virtuelle Identität u. U. nichts mit der realen zu hat. So kann sich hinter einem vermeintlich 15jährigen Chatpartner auch ein erwachsener Mann verbergen. Dieser Umstand ist den meisten zwar klar, jedoch gibt es immer wieder Fälle, wo junge (und auch ältere) Menschen darauf hereinfallen.

Bestätigung online
Man kann in der Virtualität viel leichter Bestätigung erhalten. In dieser Falle stecken zuweilen auch Online- oder Computerspiel-Abhängige, die regelrecht in die virtuelle Welt emigrieren (s. Kapitel 6_3: Online-Sucht).

Endnoten

[1] FRITZ, J. (1997). Lebenswelt und Wirklichkeit. In J. Fritz & W. Fehr (Hrsg.), *Handbuch Medien: Computerspiele* (S. 13–30). Bonn: Bundeszentrale für Politische Bildung.

[2] KAKU, M. (1998). *Visions: How Science Will Revolutionize the 21st Century.* New York: Anchor Books.

[3] BUERMANN, U. (2008). Kinder und Jugendliche zwischen Realität und Virtualität. bpd (Hrsg.) *Aus Politik und Zeitgeschichte. Neue Medien – Internet – Kommunikation.* 39/2008 (S. 34–40). Aufgerufen am 16.04.2015 unter http://www.bpb.de/apuz/30970/kinder-und-jugendliche-zwischen-virtualitaet-und-realitaet?p=all

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**„Wer ist wer? Ein Spiel zum Nicht-Kennenlernen!"**	**Freunde**
Kompetenzen	Die Schülerinnen und Schüler hinterfragen „Profile" im Internet.	Die Schülerinnen und Schüler erörtern den Begriff Freundschaft und differenzieren zwischen „Freunden", „Kumpels" und „Bekannten" anhand von Fallbeispielen.
Methoden	Spiel, Partnerarbeit, Plenum	Placemat, Fallbeispiele, Kleingruppen, Plenum
Material	Arbeitsblatt (mit Fotos), Schere, Kleber, leere Blätter	Arbeitsblatt, großes Papier
Zeit (in Minuten)	90	90
Zugang Internet/PC	nein	nein

Hinweise für die Durchführung

AB 1: „Wer ist wer? Ein Spiel zum Nicht-Kennen-lernen!"

Das Arbeitsblatt soll spielerisch hinführen zur Problematik der Virtualität und Realität. Die Fotos der Tiere sind so gewählt, dass bestimmte Assoziationen, bspw. aus Fabeln, möglich sind wie Löwe = stark oder Esel = stur o.ä. Dies sind selbstverständlich keine Wahrheiten, können aber im Spiel genau dazu benutzt werden, sich zu verstecken oder darzustellen. Die anschließende Diskussion dient der eigentlichen Reflexion und Übertragung auf die Realität. So sollen die Schülerinnen und Schüler erkennen, dass die Profile in den meisten Anwendungen wie WhatsApp oder Facebook etc. von den Usern selbst erstellt sind und genauso fantasievoll sein können wie die Profile des Spiels. Der Merksatz an der Tafel könnte lauten: „Jedes Profil ist selbst erstellt und muss nicht wahr sein!" o. ä.

AB 2: Freunde

Die Schülerinnen und Schüler sollen darüber nachdenken können, was ein Freund/eine Freundin ist und anschließend diese – eigene – Definition an Beispielen anwenden.
Der Einstieg erfolgt am Beispiel der üblichen Social Communities, die die Schülerinnen und Schüler leicht nachvollziehen können. Daran knüpft die Frage an, was ein Freund/eine Freundin überhaupt ist. Mithilfe der Methode „Placemat" (s. u.) sollen sie in Kleingruppen eine Definition erarbeiten. Diese kann je nach Gruppe ganz unterschiedlich sein. Es bietet sich an, hier einen ausführlichen Austausch nach der Gruppenphase zu ermöglichen.
Mit der Unterscheidung von „echten Freunden", „Kumpels" und „Bekannte" soll versucht werden, die drei Kategorien „echte Freunde", „kenne ich persönlich" und „kenne ich nicht persönlich" zu definieren. Die Schülerinnen und Schüler sollen in der Tabelle die Beispiele diskutieren (vielleicht kommen sie zu einer anderen Einschätzung, s.u.) und eigene Beispiele finden. Es bietet sich an, einige an die Tafel zu schreiben und zu besprechen. Die Bearbeitung der Tabelle ist sicherlich individuell, aber vielleicht dient dies der Orientierung:

Das würde ich mit ihnen tun/ihnen erzählen:	Mit echten Freunden: „Freunde"	Mit anderen, die ich persönlich kenne: „Kumpels"	Mit Menschen, die ich nur aus dem Internet kenne: „Bekannte"
A. Meine heimliche Liebe verraten	Ja	Nein	Nein
B. Über den Streit mit meinen Eltern berichten	Ja	Vielleicht	Nein
C. Ins Kino gehen	Ja	Ja	Nein
D. Einen Blick in das Tagebuch werfen lassen	Nein	Nein	Nein
E. Meinen Spitznamen verraten	Ja	Ja	Vielleicht

Lust auf mehr?
Lassen Sie die Schülerinnen und Schüler mit einem Avatar-Creator wie bspw. der App Bitstrips oder dem South Park Creator Studio (☺ **www.sp-studio.de/**) Comic-Avatare von sich erstellen. Spannend ist hier ein Vergleich: Wie ähnlich sind sie den Schülerinnen und Schülern?
Die Avatare können auch als Profilbild in den Sozialen Netzwerken weiter verwendet werden.

Wer ist wer? Ein Spiel zum Nicht-Kennenlernen! (1/3)

Im Netz trifft man schon manchmal komische Typen … willi123 und susi17 sind dabei wohl eher normale Spitznamen, die im Internet „Nicknames" heißen. Es ist so einfach eine fremde Identität anzunehmen und in eine Rolle zu schlüpfen. Umso schwerer ist es, diese zu entlarven und man kann sich nie ganz sicher sein, wer wer ist. Wie es zugehen kann, das dürft ihr in einem kleinen Spiel erfahren.

Ziel des Spiels:
Finde heraus, wer sich hinter dem Steckbrief verbirgt!

Tipp:
Alle dürfen lügen, aber vielleicht kann man aus diesen Lügen auch etwas über die Person erfahren!

Spielregeln:
Jeder darf ein Profil erstellen und in drei Runden ergänzen.

1. Runde: Suche dir ein Foto eines Tieres aus, das du auf deinen Steckbrief klebst.
Erfinde dir dazu einen Nickname, den du gut lesbar dort einträgst.

Mischt die Profile heimlich und legt sie alle aus.
Jeder darf nun raten (bitte den Tipp auf dem unteren Feld eintragen),
wer sich hinter den Steckbriefen verbirgt.
Diejenigen, deren Profil erraten wurde, scheiden aus.

2. Runde: Ergänze deinen Steckbrief um die Beschreibung deines Aussehens und deiner Körper-Merkmale.
Selbstverständlich darfst du flunkern!

Wie oben … mischen und erraten!

3. Runde: Ergänze deinen Steckbrief um deine Hobbys und Vorlieben.

Wie oben… mischen und erraten!

Wer ist wer? Ein Spiel zum Nicht-Kennenlernen! (2/3)

Das Profil

Foto	
Dein Nickname:	
Dein Aussehen:	
Deine Hobbys/ Vorlieben:	
Hinter diesem Profil versteckt sich:	

Arbeitsaufträge:

1. Spielt das Spiel!
2. Wertet anschließend das Ergebnis aus!
   War es schwer, ein Profil einer Mitschülerin / einem Mitschüler zuzuordnen?
   Woran habt ihr sie / ihn erkannt?
   Wann war es unmöglich?
3. Übertragt die Beispiele auf das Internet.
   Diskutiert in der Klasse die Frage, wie man mit (fremden) Profilen umgehen sollte!
4. Formuliert dazu einen Merksatz an der Tafel.

Wer ist wer? Ein Spiel zum Nicht-Kennenlernen! (3/3)

Quellen:

1. *Schmetterling: M. Großmann / pixelio.de*
2. *Specht: uschi dreiucker / pixelio.de*
3. *Kuh: Joujou / pixelio.de*
4. *Fliege: uschi dreiucker / pixelio.de*
5. *Pferd: Rainer Sturm / pixelio.de*
6. *Katze: berggeist007 / pixelio.de*
7. *Hund: uschi dreiucker / pixelio.de*
8. *Gans: Albedo / pixelio.de*
9. *Frosch: Sommaruga Fabio / pixelio.de*
10. *Löwin: Dieter Schütz / pixelio.de*
11. *Trampeltier: Klaus Mackenbach / pixelio.de*
12. *Esel: Lisa Schwarz / pixelio.de*
13. *Ziege: Ruth Rudolph / pixelio.de*
14. *Adler: Willi Haimerl / pixelio.de*
15. *Wolf: saskia wend / pixelio.de*
16. *Lamm: daniel stricker / pixelio.de*

Freunde

Freunde, Freunde, Freunde – was für eine Menge an „Freunden“ hat man doch bei Facebook, WhatsApp, Instagram, Twitter, Snapchat und und und und. Dabei sollten „Freunde“ doch etwas ganz Besonderes und Kostbares sein, oder? Hier sollst du darüber nachdenken, was ein Freund für dich ist.

Arbeitsaufträge:

1. Was ist ein Freund/eine Freundin? Findet euch z. B. in 4er-Gruppen zusammen. Überlege bitte zunächst alleine (vielleicht mithilfe eines „Placemats“) und diskutiert danach in eurer Gruppe darüber. Stellt eure Ideen danach den anderen Gruppen vor!

2. Worin besteht der Unterschied zwischen „Freunden“, „Kumpels“ und „Bekannten“? Vergleiche sie und fülle folgende Tabelle aus:

Das würde ich mit ihnen tun/ihnen erzählen:	Mit echten Freunden: „Freunde“	Mit anderen, die ich persönlich kenne: „Kumpels“	Mit Menschen, die ich nur aus dem Internet kenne: „Bekannte“
A. Meine heimliche Liebe verraten			
B. Über den Streit mit meinen Eltern berichten			
C. Ins Kino gehen			
D. Einen Blick in das Tagebuch werfen lassen			
E. Meinen Spitznamen verraten			
F.			
G.			
H.			
I.			
J.			

3. Vergleicht eure Ergebnisse und sprecht darüber! Erstellt danach an der Tafel eine gemeinsame Tabelle!

Online-Sucht

Zahlen

Das Thema Online-Sucht wird unter Fachleuten noch sehr kontrovers diskutiert. 2011 untersuchten die Universitäten Lübeck und Greifswald das Phänomen im Auftrag des Bundesgesundheitsministeriums mit der Studie „PINTA" (Prävalenz der Internetabhängigkeit). Das Ergebnis gibt zu denken: Etwa 560.000 Menschen mussten demnach als internetsüchtig eingestuft werden. „Etwa 1 % der 14- bis 64-jährigen in Deutschland werden demnach als internetabhängig eingestuft. 4,6 % der 14- bis 64-Jährigen werden als problematische Internetnutzer angesehen. In der Regel sind Jugendliche und junge Erwachsene häufiger betroffen. In der Altersgruppe der 14- bis 24-Jährigen ist die Verbreitung am größten: 2,4 % abhängige und 13,6 % problematische Internetnutzer".[1] Eine ähnliche Studie unter Jugendlichen kam zu dem Ergebnis, dass in den untersuchten Ländern (Spanien, Rumänien, Polen, Niederlande, Griechenland, Island und Deutschland) rund 1,2 % der Jugendliche als internetsüchtig gelten müssen, fast 13 % sind gefährdet.[2]

Definition

Grundsätzlich wird „Abhängigkeit", so der fachlich korrekte Ausdruck für die umgangssprachliche „Sucht", definiert als „das unabweisbare Verlangen nach einem bestimmten Erlebniszustand", genauer:

> *„Sucht kann als das unabweisbare starke Verlangen nach einem bestimmten Gefühls-, Erlebnis- oder Bewusstseinszustand definiert werden. Dieses Verlangen kann sowohl stoffgebunden (Alkohol, Medikamente, illegale Drogen) als auch stoffungebunden (Glücksspiel, Arbeit, Sex) sein."*[3]

Üblicherweise wird diesem Verlangen alles andere untergeordnet, was man bei Alkoholkranken oder anderen Drogenabhängigen deutlich sehen kann. Bei Tätigkeiten am Computer ist dies naturgemäß wesentlich schwieriger zu beobachten.

Einordnung

Das international anerkannte medizinische Klassifikationssystem der Weltgesundheitsorganisation (WHO) „International Statistical Classification of Diseases and Related Health Problems" (ICD) kennt die Internet-Abhängigkeit in seiner aktuellen Version (ICD-10, Stand April 2015) nicht als eigenes Krankheitsbild. Zudem werden hier bisher nur stoffgebundene Abhängigkeiten berücksichtigt. Aus diesem Grunde wird eine stoffungebundene Abhängigkeit derzeit zur „Störung der Impulskontrolle" (im Original „impulse control disorder") gerechnet. In der wohl 2017 erscheinenden Neuauflage, dem ICD-11, soll es dann die neue Kategorie der „Verhaltenssucht" geben.
Bert te Wildt untersuchte mit seinem Team am Universitätsklinikum Bochum den Zusammenhang mit anderen Erkrankungen. Das Ergebnis: Teilnehmer der Studie, die als internetabhängig gelten, litten fast immer unter einer psychischen Begleiterkrankung. Bei 70 % lagen depressive Störungen vor.
Internet-Abhängigkeit wird zudem auch als Überbegriff für andere Süchte verwendet. So zum Beispiel, wenn eigentlich eine Kaufsucht, Sexsucht oder Spielsucht besteht, die im Internet ausgelebt wird.

Drei Bereiche der Internetsucht

Trotz der akademischen Diskussion um die Einordnung des Phänomens (es sei daran erinnert, dass es andere Beispiele für die schwierige / falsche Einordnung gibt bzw. gab: so tauchte Homosexualität jahrzehntelang als Krankheit in der ICD auf), sind sich die Experten einig, dass es drei Bereiche mit einer krankhaften Nutzung von Internet / Computer / Tablet / Smartphone geben kann:

- Computerspiele
- sexuelle Inhalte
- schriftliche Kommunikation.

Aus der Praxis
Nicht alles, was Schülerinnen und Schüler als „süchtiges" Verhalten bezeichnen, ist es auch tatsächlich. Das Modewort wird auch für eine intensive, manchmal exzessive Nutzung benutzt. Die Fälle echter Abhängigkeit sind mit einem hohen Leidensdruck versehen und von LehrerInnen nicht einfach zu bewältigen. Eltern sollten immer für weitere Unterstützung mit Schulsozialarbeitern, dem Schulpsychologischen Dienst und anderen Beratungsstellen in Kontakt gebracht werden.

Symptome
Wie bei allen stoffungebundenen Abhängigkeiten ist eine Abgrenzung zu „normalem" Verhalten fließend und nicht immer klar abzugrenzen. Folgende Symptome sprechen aber für ein krankhaftes Verhalten:[5]

- exzessiver Gebrauch des Internet, der immer mehr Zeit und Aufmerksamkeit der Betroffenen fordert
- unkontrolliertes Surfen
- häufiges unüberwindliches Verlangen das Internet zu benutzen
- Kontrollverluste (d. h. länger „online" bleiben als man sich vorgenommen hatte) verbunden mit diesbezüglichen Schuldgefühlen
- sozial störende Auffälligkeit im engsten Kreis der Bezugspersonen (Freunde, Partner, Familie), häufige Rügen durch unmittelbare Bezugspersonen
- nachlassende Arbeitsleistung
- Verheimlichung / Verharmlosung der Netz-Aktivitäten vor der Umwelt
- psychische Erscheinungen wie Nervosität, Reizbarkeit und Depression bei Verhinderung des Internet-Gebrauchs
- mehrfach fehlgeschlagene Versuche, die Nutzung einzuschränken

Oft treten diese Symptome in Kombination (Experten sprechen von „Komorbidität") mit stoffgebundenen Abhängigkeiten auf, also Alkohol, Tabak und / oder illegalen Drogen.

Merkmale zur Erkennung
Das für Jugendliche konzipierte Portal „www.ins-netz-gehen.de" bietet einen Selbsttest zu Computerspiel- und Internet-Abhängigkeit an:
www.ins-netz-gehen.de/check-dich-selbst/bin-ich-suechtig
Auch bei anderen Organisationen / Institutionen finden sich Selbsttests oder Fragebögen, um ein problematisches Verhalten zu identifizieren, bspw. bei
www.suchtpraevention-zh.ch/selbsttest/online-konsum
www.unimedizin-mainz.de/psychosomatik/patienten/behandlungsangebote/ambulanz-fuer-spielsucht/selbsttest-computerspiel

Inhaltlich geht es immer um die gleichen Aspekte, die hier kurz skizziert werden. Neben der rein quantitativen Abfrage des Nutzungsverhaltens (wie lange bist du wann online?) gelten folgende Aspekte zur Einordnung:

- Wenn ich nicht online bin, kreisen meine Gedanken oft darum.
- Ich habe das Gefühl, dass Online-Sein für mich immer wichtiger wird.
- Ich kann meine Zeit im Internet schwer kontrollieren und bin oft länger online, als ich mir eigentlich vorgenommen hatte.
- Wenn ich nicht online sein kann, bin ich gereizt und unzufrieden, dauert es an, werde ich unruhig und nervös.
- Meine Freunde / meine Eltern beschweren sich, dass ich zu viel Zeit vor dem Bildschirm verbringe.
- Ich habe Schwierigkeiten in der Schule, weil ich ständig vor dem Bildschirm bin statt zu lernen.
- Weil ich so viel am Computer mache, unternehme ich weniger mit anderen.
- Ich habe eine Routine und bin immer zu bestimmten Zeiten online.

Therapien

Selbstverständlich können die o. a. Fragen nur eine erste Orientierung bieten und keine zuverlässige Diagnose stellen. Und nicht jedes exzessive Verhalten ist eine Abhängigkeit, insbesondere in der Jugendphase. Sollte aber krankhaftes oder problematisches Verhalten vorliegen, kann wirklich zuverlässig nur ein Therapeut helfen. Seit einigen Jahren behandeln einige Kliniken Online- und Computerspielsucht.
Eine erste Anlaufstelle bietet die Bundeszentrale für gesundheitliche Aufklärung (BZgA) mit ihrer Sucht- und Drogen-Hotline unter 01805/31 30 31 bzw. unter
www.sucht-und-drogen-hotline.de
Ambulanz für Spielsucht:
www.unimedizin-mainz.de/psychosomatik/patienten/behandlungsangebote/ambulanz-fuer-spielsucht
Besonders schwierig wird eine mögliche Therapie, weil es – anders als bei den stoffgebundenen Abhängigkeiten – fast unmöglich ist eine völlige Abstinenz im Alltag herzustellen: Internet und Handy sind Alltagsmedien geworden.

Prävention

„Sucht hat immer eine Geschichte" heißt sehr eindrücklich das Motto einer Kampagne der Gemeinschaftsinitiative gegen Sucht, die seit 1998 von der ginko Stiftung für Prävention als Landeskoordinierungsstelle in NRW für das Gesundheitsministerium NRW koordiniert wird. Dahinter steckt die Idee, dass die beste Prävention gegen eine Suchtentwicklung darin besteht, Kinder stark zu machen, d. h. ihr Selbstvertrauen und Selbstwertgefühl zu stärken und ihre Konflikt- und Kommunikationsfähigkeit zu fördern. Nur dann können sie auch „NEIN" sagen zu Suchtmitteln aller Art (s. auch Aktion „Kinder stark machen" der Bundeszentrale für gesundheitliche Aufklärung).

Einen Überblick über den aktuellen Forschungsstand bietet Ulrike Braun von der Uni Hamburg in ihrem Buch „Exzessive Internetnutzung Jugendlicher im familialen Kontext", 2014, Springer Fachmedien-Verlag, Wiesbaden, ISBN 978-3-658-04196-0.

Links und weiterführende Informationen

Webseiten

www.klicksafe.de/service/materialien/broschueren-ratgeber/internet-handy-und-computerspielabhaengigkeit
Flyer Internet-, Handy- und Computerspielabhängigkeit: klicksafe-Tipps für Eltern

www.kinderstarkmachen.de
Initiative der BZgA zur Suchtprävention bei Kindern und Jugendlichen

www.klicksafe.de/themen/spielen/computerspiele/computersucht/hilfe-wo-finde-ich-hilfe
Übersichtsseite auf klicksafe.de mit Anlaufstellen für Betroffene

http://drogenbeauftragte.de/drogen-und-sucht/computerspiele-und-internetsucht.html
Überblick der Drogenbeauftragten der Bundesregierung zu Studien zu Computerspiele- und Internetsucht

Endnoten

[1] DROGENBEAUFTRAGTE.DE. (2014, 2. Oktober). *Computerspiele- und Internetsucht* (Absatz 6). Aufgerufen am 23.04.2015 unter http://drogenbeauftragte.de/drogen-und-sucht/computerspiele-und-internetsucht.html

[2] LÜPKE-NARBERHAUS, F. (2013, 17. Januar). *Jugendliche im Internet: ich surfe, also bin ich süchtig?* Aufgerufen am 23.04.2015 unter http://www.spiegel.de/schulspiegel/wissen/studie-zu-internetsucht-jeder-zehnte-jugendliche-gefaehrdet-a-878220.html

[3] FREY, D. & Graf Hoyos, C. (Hrsg.). (2005). *Psychologie in Gesellschaft, Kultur und Umwelt. Handbuch.* Weinheim: Beltz Psychologie Verlags Union. (S. 172)

[4] WEILER, J. (2014, 1. Oktober). *RUB-Forscher unter-sucht Internetabhängigkeit und Begleiterscheinungen.* Aufgerufen am 23.04.2015 unter http://rubin.rub.de/sites/default/files/rubin/DE-2014/18-internetsucht/rubin_2014_2_internetabhaengigkeit.pdf

[5] ONMEDA.DE. (2014, 10. Oktober). *Internetsucht: Symptome.* Aufgerufen am 23.04. unter http://www.onmeda.de/krankheiten/internetsucht-symptome-1529-4.html

[6] SCHOEN-KLINIKEN.DE. (2015). *Internetsucht, Computersucht.* Aufgerufen am 23.04.2015 unter http://www.schoen-kliniken.de/ptp/medizin/psyche/persoenlichkeitsstoerung/computer-sucht

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Computersucht**	**Online-Sucht**
Kompetenzen	Die Schülerinnen und Schüler lernen das Thema Computersucht anhand eines Spots kennen.	Die Schülerinnen und Schüler übertragen die Aussagen eines Interviews mit einer Sucht-Expertin auf einen Informationsflyer.
Methoden	Videoanalyse, Blitzlicht, Internet-Recherche	Textanalyse, Partnerinterview, Infoflyer
Material	Film, s.u. Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	nein (Ja, für evtl. weitere Recherche für Informationsflyer)

Hinweise für die Durchführung

AB 1: Computersucht

Das Phänomen der Abhängigkeit ist hochkomplex und selbst aus medizinischer Sicht nicht einfach zu charakterisieren. Mit diesem Arbeitsblatt sollen sich die Schülerinnen und Schüler dem Thema trotzdem – mit dem ironischen Video etwas leichter – nähern. Das Blitzlicht nach dem Film soll alle Äußerungen ermöglichen, die den Schülerinnen und Schülern so auf- und eingefallen sind. Die Analyse des Films mit der Tabelle ermöglicht eine gezieltere Annäherung. Warum handeln die Personen so? Die Personen benehmen sich erschreckend normal… also ganz anders als eigentlich zu erwarten ist, immerhin sind sie mit einer anderen leblosen Person konfrontiert. Im übertragenen Sinne ist zu fragen, warum? Möglicherweise, weil man Computerspielsucht in unserer digitalen Welt häufig (lange) nicht erkennen kann? Oder weil die Gesellschaft davor „noch" die Augen verschließt?
Eine mögliche Lösung könnte so aussehen:

Szene	Was passiert?	Warum handeln die Personen so?	Wie würdest du reagieren?
Mit der Freundin	Sie sitzen auf der Couch und küssen sich, er fällt um.	Die Freundin ist ganz erstaunt und weiß nicht, was sie tun soll.	Ich würde meinen Freund / meine Freundin verlassen. ODER Ich würde meinen Freund / meine Freundin wachrütteln.
In der Pausenhalle	Der Junge lehnt an seinem Freund, der geht weg und er fällt um.	Die Freunde interessieren sich für andere Dinge als den Jungen.	Ich würde meinen Klassenkameraden nicht so alleine lassen und ihn trotzdem tragen.
Im Schwimmbad	Alle schwimmen, der Junge treibt im Wasser, scheinbar tot.	Die anderen lassen den Jungen treiben, weil sie gar nicht bemerken, dass er vielleicht tot ist.	Ich würde ihn sofort aus dem Wasser holen und Mund-zu-Mund-Beatmung/ Erste Hilfe machen / leisten.
Beim Sport	Alle spielen, der Junge hängt reglos im Tor.	Die anderen spielen und bemerken den Jungen nicht.	Ich würde versuchen den Jungen aufzuwecken, damit er mitspielen kann.
Im Auto	Die Familie steigt aus, der Junge bleibt sitzen, leblos.	Der Familie ist es egal, ob der Junge noch im Auto sitzen bleibt.	Ich würde meinen Bruder nicht da sitzen lassen, sondern mit aus dem Auto nehmen.
Beim Familienessen	Die Familie isst, der Junge sitzt dabei und fällt in die Suppe.	Die Familie interessiert sich überhaupt nicht für den Jungen.	Ich würde mit meinem Bruder schimpfen, wenn er sich so benimmt. ODER Ich würde ihn füttern.
Am Computer	Der Junge erwacht und ist sehr lebhaft.	Der Junge lebt nur in der digitalen Welt, da erwacht er.	Ich würde aufhören zu spielen.

Interessant ist der letzte Punkt bzw. die rechte Spalte der Tabelle mit der Frage, wie man sich richtig verhalten kann, wenn ein Freund / eine Freundin sich so verhält wie der Junge in dem Film, der offensichtlich nur in der digitalen Welt lebt und nicht in der realen. Dafür gibt es keine einfache Lösung, aber vielleicht trotzdem gute Ideen (s. Tabelle). Die Internet-Recherche zum Suchtverhalten geschieht auf einer kindgerechten Seite, die das Phänomen sehr einfach erklärt.

Hinweise für die Durchführung

AB 2: Online-Sucht	Dieses Arbeitsblatt beinhaltet ein Interview mit Dr. Anne Pauly von der Bundeszentrale für gesundheitliche Aufklärung. Die Schülerinnen und Schüler sollen es zunächst lesen und es sich dann in Form eines Partnerinterviews gegenseitig erläutern. Vielleicht schieben Sie hier eine kurze Phase der Rückfragen und der Vergewisserung ein, ob wirklich alle es angemessen und richtig verstanden haben. Der Inhalt des Interviews soll nun in der Erstellung eines Informationsflyers Anwendung finden.

Lust auf mehr?

- Die Bundeszentrale für gesundheitliche Aufklärung hat zahlreiche Materialien zum Thema Suchtprävention: **http://www.bzga.de/themenschwerpunkte/suchtpraevention**, die eine weitergehende Erarbeitung des Themas erlauben.
- Rollenspiel: Die Schülerinnen und Schüler versetzen sich in die Rolle von Eltern, die den Informationsflyer von klicksafe gelesen haben. **http://www.klicksafe.de/service/materialien/broschueren-ratgeber/internet-handy-und-computerspielabhaengigkeit/** Stell dir vor, du wärst Mutter/Vater… lies den Flyer und führe ein Gespräch mit deinem gefährdeten Kind.

Computersucht

Der Junge interessiert sich nicht mehr für seine Freundin, nicht für seine Freunde und erst recht nicht für seine Familie. Er wirkt wie tot und erwacht erst, als er den Computer einschaltet… das ist die Handlung im Spot „Wo lebst du?“ von klicksafe.

klicksafe-Spot „Wo lebst du?“

Arbeitsaufträge

1. Bitte schaut euch gemeinsam den Film „Wo lebst du?“ an: **www.klicksafe.de/ueber-klicksafe/downloads/klicksafe-werbespots/download-wo-lebst-du**
2. Macht direkt danach ein „Blitzlicht“, in dem jeder das sagen darf, was ihm zu dem Film einfällt, ohne Kommentare der anderen.
3. Arbeitet nun in Partnerarbeit und füllt die Tabelle in Stichworten aus:

Szene	Was passiert?	Warum handeln die Personen so?	Wie würdest du reagieren?
Mit der Freundin			
In der Pausenhalle			
Im Schwimmbad			
Beim Sport			
Im Auto			
Beim Familienessen			
Am Computer			

4. Vergleicht anschließend euer Ergebnis und notiert das Wichtigste an der Tafel.
5. In dem Film geht es offensichtlich um ein Suchtverhalten. Bitte recherchiert auf dieser Seite in Partnerarbeit, was „Computersucht“ eigentlich genau ist. Schreibt die Merkmale auf!
   http://www.internet-abc.de/kinder/computersucht.php

   Wie könntet ihr als Freund / Klassenkamerad / Eltern / Sportkamerad dem Jungen helfen? Besprecht diese Frage in der Klasse!

Online-Sucht (1/2)

Interview mit Dr. Anne Pauly von der Bundeszentrale für gesundheitliche Aufklärung (BzgA, www.bzga.de), geführt im März 2015:

? Was versteht man eigentlich genau unter Online-Sucht?

Im Umgang mit Computer, Internet und Computerspielen kann sich ein Verhalten entwickeln, das zu erheblichen persönlichen und zwischenmenschlichen Problemen und Belastungen führt. Die Betroffenen haben ihren Umgang mit Internet und Computerspielen nicht mehr unter Kontrolle, sie beschäftigen sich gedanklich übermäßig stark damit, fühlen sich unruhig oder gereizt, wenn sie diese Angebote nicht nutzen können. Sie vernachlässigen andere wichtige Lebensaufgaben wegen des Computerspielens oder der Internetnutzung. Diese Symptome sind denen ähnlich, die bei Suchterkrankungen festzustellen sind.

? Wie kann man sie erkennen?

Die Grenze zwischen normaler und schädlicher Computernutzung ist schwer zu bestimmen. Eine phasenweise intensive Beschäftigung mit einem Computerspiel oder einem Internetangebot ist allein kein Grund zur Besorgnis. Auch kann man nicht sagen, ab wie vielen Stunden täglicher Computernutzung ein problematisches Verhalten vorliegt. Die Funktion des Computerspielens oder des Internetgebrauchs ist aber ein wesentliches Merkmal von problematischer Nutzung. Gefährlich werden kann es, wenn

- man den Computer als Trostspender nutzt oder ihn bei Stress anmacht, um wieder runterzukommen,
- der Computer wichtiger als die reale Welt wird,
- der Computer die Freizeitgestaltung hauptsächlich bestimmt.

? Wie entsteht sie?

Für eine Abhängigkeitserkrankung gibt es immer mehr als eine Ursache. Oft wird eine Abhängigkeitsentwicklung durch verschiedene Dinge bedingt, die in Wechselwirkung miteinander stehen.

? Sind Jugendliche besonders gefährdet?

Digitale Medien scheinen wie für Jugendliche gemacht zu sein: Selbstdarstellung, Identitätsfindung, Action-Erlebnisse und Kommunikation ohne Grenzen mit virtuellen oder realen Freunden erfüllen jugendliche Bedürfnisse. Die für Jugendlichen attraktiven Internetangebote wie Soziale Netzwerke oder Spiele können besonders bei Jugendlichen zu übermäßiger Nutzung verleiten.
Für sich genommen sind das Internet oder Computerspiele nicht nur positiv oder nur negativ.
Für Schule und Beruf ist es heutzutage äußerst wichtig, sich sicher und gezielt im Internet bewegen zu können. Daneben sind Internetangebote aber auch zu einem wesentlichen Teil der modernen Freizeitgestaltung für Jugendliche geworden.

? Wie kann man sich selbst schützen?

Keiner will süchtig sein. Denn Sucht bedeutet immer, von etwas nicht lassen zu können, das einem nicht gut tut.

- Die Grundregel lautet: Pass auf dich auf! Hab immer im Blick, wann und wie lange du deinen Computer nutzt und achte darauf, dass du nicht völlig abtauchst.
- Hilfreich ist es, wenn du dir feste Zeiten setzt, die du mit dem Computer verbringst. Leg für dich einfach eine tägliche oder wöchentliche Stundenzahl fest, damit du auch noch Zeit für andere Dinge hast. Aber sei ehrlich zu dir selbst und halt dich dran.
- Sport ist die beste Medizin? Auf jeden Fall hält Sport fit, du kommst auf andere Gedanken und kannst dich dabei auch noch so richtig auspowern. Ob du nun aber regelmäßig Sport machst oder dir ein anderes Hobby suchst, Hauptsache es macht dir Spaß und du kommst dadurch auch mal gedanklich vom Computer weg!

Online-Sucht (2/2)

- Mal ehrlich: Wissen deine Eltern, was du so alles am Computer machst? Und gibt es deswegen häufig Ärger zu Hause? Erklär ihnen doch mal die Spiele, die du spielst oder die Seiten, auf denen du mit deinen Freundinnen und Freunden chattest. Das schafft Klarheit, auch für dich. Außerdem bist du der Profi, was das Thema betrifft, und kannst deinen Eltern noch so manches beibringen!
- „Der Computer bleibt heute mal aus!" Wie fühlst du dich bei so einer Ansage? Wirst du unruhig oder schaffst du es, die computerfreie Zeit anders zu nutzen? Mach etwas, das dir Spaß macht, in der plötzlich frei gewordenen Zeit!

? Was können Freunde und Angehörige tun?

Wenn deine Freundin oder dein Freund ein Problem haben, muss das ja nicht gleich jeder wissen. Sprich das Thema deshalb an, wenn ihr irgendwo ungestört und allein seid. Am besten an einem Ort, an dem ihr euch wohl fühlt.
Kurz vor einer Klassenarbeit kann auch deine beste Freundin oder dein bester Freund kein Problemgespräch gebrauchen. Um ein so heikles Thema anzusprechen, wähle deshalb einen Zeitpunkt, in der kein Stress herrscht. Ihr solltet auch Zeit haben, länger darüber zu reden.

Vielleicht ist deiner Freundin oder deinem Freund schon selbst aufgefallen, dass die Zeit vor dem Computer oder im Internet immer wieder aus dem Ruder läuft. Das zu ändern, fällt vielen schwer. Es bringt also nichts, wenn du Vorwürfe machst. Versuch lieber, verständnisvoll zu sein. So kannst du deine Freundin oder deinen Freund besser erreichen, sodass sie oder er auch Hilfe annimmt.
Hilfreich bei Problemgesprächen ist immer, so konkret wie möglich zu sein. Mach deiner Freundin oder deinem Freund deshalb keine allgemeinen Vorwürfe, mit denen wenig anzufangen ist. Besser du schilderst ganz genau, was dir wann aufgefallen ist oder dich gestört hat. Teile ihr oder ihm auch mit, wie die Situation für dich ist und was du dir für sie oder ihn wünschen würdest.
Deiner Freundin oder deinem Freund wird es nur besser gehen, wenn sie oder er lernt, anders mit dem Computer umzugehen. Das geht nicht von heute auf morgen. Biete deshalb gezielt deine Hilfe an. Gemeinsam könnt ihr besprechen, wie man in Zukunft auch mal auf den Computer verzichten kann.

Arbeitsaufträge:

1. Bitte lest das Interview sorgfältig.
2. Führt dazu ein „Partnerinterview" durch!
3. Arbeitet in Partnerarbeit weiter. Nutzt euer Wissen über Online-Sucht und erstellt einen 1-seitigen Infoflyer, den ihr in eurer Schule verteilen könnt.

Tipp: *Hier könnt ihr einen Selbsttest machen:*
www.suchtpraevention-zh.ch/selbsttest/online-konsum/

Werbung und Abzocke

Manchmal eher unauffällig, manchmal penetrant – auf einem Streifzug durch die Online-Landschaft bleibt man kaum von Werbung verschont.
Der Werbemarkt ist offline wie online hochdynamisch und die Werbeindustrie ständig auf der Suche nach kreativen Einfällen und neuen Marketingformen. Dies führt zu einer verwirrenden Vielfalt und zum Teil perfiden Strategien, so dass eine Unterscheidung von redaktionellem Inhalt und Werbung trotz „Trennungsgebot" und Kennzeichungspflicht im Internet bedeutend schwieriger ist als zum Beispiel bei Fernseh-Werbung. Nicht nur für Kinder kann es deshalb schwer sein, Werbeabsichten zu durchschauen.

Online-Marketing-Formen

Hier werden die wichtigsten Internet-Werbestrategien zur Unterscheidung kurz erklärt:

- **Affiliate**
  Affiliate bedeutet übersetzt „Partner" und damit ist das „Affiliate-Marketing" auch gut beschrieben. Der eigentliche Affiliate, zum Beispiel der Betreiber einer Webseite, bietet einem Anbieter, dem „Merchant", einen Werbeplatz, der provisionsabhängig vergütet wird.
- **In-Page – der Klassiker**
  Display-Advertising oder kurz „Display-Ads" kann man grob unterscheiden in „In-Stream-Videos" (s. u.) und „In-Page", also der klassische Werbebanner, welcher in den letzten Jahren eine Normierung erfahren hat.
- **Content und In-Text**
  Content-integrierte Werbung („Integrated advertising") ist im redaktionellen Bereich einer Website platziert und fügt sich gestalterisch in das Layout ein. Häufig passt die Werbeaussage auch inhaltlich zum Webangebot und ist deshalb schwer zu erkennen. In-Text-Werbung sieht man sehr oft in Diskussionforen oder Blogs. Dabei werden bestimmte Begriffe verlinkt, die mit der Werbung in Verbindung stehen.
- **In-Stream-Video-Werbung**
  Hier erfolgt die Werbung in Form eines – meist kurzen – Videos.
- **Search-Marketing**
  Werbeanzeigen auf den Ergebnislisten von Suchmaschinen: Firmen können ihre Werbung entsprechend der Suchbegriffe der Kunden einblenden.
- **Sponsoring**
  Sponsoring findet man häufig auf Internetseiten von Fernsehsendern. Es werden Gewinnspiele, Downloads oder andere attraktive Aktionen von Sponsoren präsentiert, um ein positives Image bei der jungen Zielgruppe aufzubauen.
- **Werbespiele**
  Werbespiele (Advergames, Adgames) sind gesponserte Onlinespiele, die in werbefinanzierten Websites oder auf firmeneigenen Websites eingebunden werden können.
- **Alles ist Werbung**
  Der gesamte Internetauftritt kann als Werbefläche dienen. Auch Newsletter, Gewinnspiel und Clubmitgliedschaft dienen oft Werbezwecken. Durch E-Cards und Weiterempfehlen der Seite bzw. des Artikels wird z. B. das Kind direkt zum kostenlosen und besonders vertrauenswürdigen Werbebotschafter.
- **Werbe-Mails**
  Werbe-Mails kontaktieren effektiv, weil sich der Empfänger dadurch persönlich angesprochen fühlt. Sie sind mit Hinweisen auf Produkte und Bestellmöglichkeit und zum Teil auch mit Links zu Onlineshops versehen.
- **Virales Marketing**
  Die massenhafte und schnelle Verbreitung über z. B. Soziale Netzwerke – ähnlich einem Virus.

Die Mutter aller viralen Marketingkampagnen lieferte die Firma Blendtec schon 2006. Der Hersteller von Standmixern ließ vor laufender Kamera seinen Gründer Tom Dickson auf YouTube allerlei Gegenstände wie Golfbälle, Fotoapparate, Batterien und Handys zu feinem Pulver mixen. Mit einem Budget von 50 Dollar schaffte die Firma eine Umsatzsteigerung von 700 %:[1]
www.youtube.com/user/Blendtec

Umgang mit Online-Werbung
Insgesamt erfordert der Umgang mit Internetwerbung von Nutzern unterschiedliche Handlungsstrategien. Er stellt somit höhere Anforderungen an ihre Medienkompetenz als beispielsweise der Umgang mit Fernsehwerbung. Es gibt also nicht die „eine" Strategie.

Vermischung von Inhalt und Werbung
Oft sind redaktionelle Inhalte und Werbung vermischt. Insbesondere Spiele dienen dazu, subtile Werbebotschaften und Produktinformationen zu liefern. Kinder sind meist nicht in der Lage, dies zu durchschauen. Produktinformationen, Shops und Gewinnspiele vermengen sich mit allgemeinen Inhalten, Communitys und Chat-Räumen. Auch für Internetwerbung gelten Richtlinien, die von Werbetreibenden einzuhalten sind. Nach dem „Trennungsgebot" muss Werbung deutlich erkennbar sein. Sie sollte z. B. den Schriftzug „Werbung" oder „Anzeige" tragen und sich in der Gestaltung deutlich von der restlichen Internetseite unterscheiden.

Aus der Praxis
Das Thema Werbung ist ein Standard-Thema der Sozialwissenschaften (Politik, Sozialkunde etc.) und eignet sich daher gut als fächerverbindendes Projekt..

Jugendliche und Werbung

Bei Jugendlichen finden sich zum Teil sehr unterschiedliche Herangehensweisen an Online-Werbung. Im Jahr 2014 hat das JFF-Institut für Medienpädagogik im Auftrag des Bayerischen Staatsministeriums für Umwelt und Verbraucherschutz die Studie „Jugendliche und Online-Werbung im Social Web" durchgeführt und in diesem Zusammenhang einige Erkenntnisse über die Altersgruppe der 12-16 Jährigen gewinnen können:[2]

- Die für die befragten Jugendlichen wichtigsten Plattformen sind durchweg kommerzielle Angebote;
- Beliebte Angebote wie Facebook, YouTube und Skype informieren zwar über die teils nur schwer als solche Werbeformen, jedoch in einer für Jugendliche kaum nachvollziehbaren Art und Weise;
- Überwiegend kritisieren die Jugendlichen Online-Werbung;
- Die Umgangsweisen der Jugendlichen sind hinnehmend, nutzenorientiert und nur selten unterbindend;
- Die Jugendlichen erkennen zwar Gestaltungsmittel von Werbung, von den Geschäftsmodellen und Auswertungsverfahren für personalisierte Werbung haben sie jedoch keine Vorstellung.

Zusammenfassend und etwas vereinfacht könnte man sagen, dass die Jugendlichen sich sehr wohl bewusst sind, dass sie massenhaft und fast ausschließlich kommerzielle Angebote nutzen. Sie stehen der Werbung auch kritisch gegenüber, aber sie haben eine falsche Selbsteinschätzung bezüglich ihrer Verbraucher und vor allem handeln sie nicht entsprechend. Sie können Werbeangebote, Formen personalisierter Werbung und die dahinterliegenden Interessen oft nicht erkennen.[3]

Abzocke

Social Engineering

Was früher einfach „Abzocke" genannt wurde und rechtlich meistens als „Betrug" (§ 263 StGB) bezeichnet wird, heißt in der Internet-Sprache „Social Engineering". Damit ist gemeint, dass Internetnutzer so manipuliert werden, dass sie vertrauliche Informationen preisgeben, etwas Bestimmtes kaufen oder sogar Geld überweisen ohne Gegenleistung. Der Klassiker ist die zu Tränen rührende E-Mail über jemanden in Not und das Versprechen auf eine reiche Belohnung in der Zukunft. Doch heute sind die Methoden subtiler:

Wie laufen die „neuen" Betrugs-Methoden ab?

Ob Intelligenztests oder Prognosen zur eigenen Lebenserwartung: die Teilnahme an Gewinnspielen, Warenprobentests oder Offerten zu Gratis-SMS – Anbieter locken und wollen neben persönlichen Angaben wie Alter und Geschlecht, auch den vollständige Namen und die Postanschrift erhalten.

Die Maschen

Die Verbraucherzentrale Niedersachsen listet die typischen Maschen der Abzocker auf[4]:

- Ungenügende Kostenhinweise
- Aktionspreise und Sonderangebote
- Kosten versteckt im Kleingedruckten
- Häkchen = Verzicht auf Widerruf
- Erschlichene Daten, z. B. über Gewinnspiele
- Versteckte Anbieter mit unzureichendem Impressum
- Irreführende Internet-Adresse, die so ähnlich klingen wie eine bekannte und seriöse

Wer aufgrund einer solchen unzureichenden Preisinformation darauf herein fällt und sich registriert, kann sich in der Regel gegen die geltend gemachten Forderungen wehren und die Zahlung verweigern. Die Betreiber der entsprechenden Seiten wissen genau, dass sie vor Gericht kaum eine Chance hätten und versuchen daher die Betroffenen durch Einschüchterungen in Form von Mahnungen oder Inkassoschreiben zur „freiwilligen" Zahlung zu bewegen.

Typische Merkmale

Die Angebote sind so gestaltet, dass deren Nutzung auf den ersten Blick kostenlos erscheint. Gleichzeitig lockt oft die Teilnahme an einem tollen Gewinnspiel, bei dem hohe Sach- oder Geldpreise zu gewinnen sind. Tatsächlich fallen jedoch entweder einmalige Nutzungsentgelte (meist 30 oder 59 Euro) an oder der Nutzer schließt sogleich ein dauerhaftes, kostenpflichtiges Abonnement (z. B. Zeitschriften- oder Klingelton-Abo) ab. Zu finden sind die entstehenden Kosten entweder im Kleingedruckten ganz unten auf der Seite, so dass der Nutzer erst herunterscrollen muss oder sogar nur in den Allgemeinen Geschäftsbedingungen (AGB), die extra angeklickt und teilweise seitenweise gelesen werden müssen.

Tipps

Worauf sollte man achten bevor man sich bei einem Angebot registriert? Grundsätzlich gilt, bei allem was mit „Gratisangebot", „Clubmitgliedschaft" oder „Gewinnspiel" und Ähnlichem wirbt, auf jeden Fall zweimal nachzusehen, ob sich irgendwo ein Preishinweis versteckt. Je größer die Wörter „kostenlos" oder „gratis" angepriesen werden, desto größer sollte auch Ihre Vorsicht sein. Spätestens wenn Sie aufgefordert werden, Ihre persönlichen Daten anzugeben, sollte Sie auf folgende Punkte achten:

- ***Werfen Sie** unbedingt einen Blick ins Kleingedruckte (AGB) und scrollen Sie die Internetseite bis ganz nach unten. Durchsuchen Sie dann die Seiten danach, ob sich dort ein Kostenhinweis versteckt. Es mag zwar anstrengend sein, seitenweise AGB zu lesen, doch gerade im Internet sind diese die beinahe einzige Informationsquelle um herauszufinden, auf was man sich tatsächlich einlässt.*
- ***Achten Sie** auf den „Haken mit dem Haken" und vergewissern Sie sich, ob nicht noch ein ungewolltes Kästchen aktiviert ist. In besonders arglistigen Fällen werden auch manchmal nur Verweissternchen (*) verwendet und die dazugehörige Anmerkung der Preis stehen irgendwo am unteren Rand der Seite.*
- ***Gehen Sie** mit Ihren persönlichen Daten grundsätzlich sparsam um! Prüfen Sie vor allem ganz genau, an wen Sie Ihre Bankdaten weitergeben!*
- ***Bevor Sie** per Mausklick Ihre Anmeldung bestätigen, lesen Sie die Vertragsbedingungen gewissenhaft durch. Ist dort die Rede von (Mindest-) Vertragslaufzeiten oder Kündigungsfristen, weist dies meistens auf eine vertragliche Bindung hin, die mit Kosten verbunden ist.*
- ***Prüfen Sie**, wie Sie Kontakt zum Anbieter herstellen können! Im so genannten Impressum muss Identität und Anschrift angegeben sein. Achten Sie darauf, dass dort nicht nur ein Postfach angeführt ist. Wenn der Anbieter im Ausland sitzt, kann es bei Reklamationen schwierig sein, Ihre Rechte durchzusetzen.*
- ***Lassen Sie** sich nicht durch die Teilnahme an einem tollen Gewinnspiel blenden! Die versprochenen Gewinne sollen zumeist nur von den Kosten ablenken.*
- ***Werden Sie** deutlich über Ihr Widerrufsrecht informiert? Bei Vertragsabschlüssen im Internet haben Sie oftmals die Möglichkeit, den Vertrag innerhalb von zwei Wochen zu widerrufen. Erfolgt keine ordnungsgemäße Belehrung über das Widerrufsrecht, können Sie zumeist den Vertrag noch länger rückgängig machen.*

Button-Lösung

Zum 1. August 2012 trat in Deutschland eine Gesetzesänderung beim § 312g des Bürgerlichen Gesetzbuches (BGB) in Kraft, die als „Button-Lösung" (seit 2014 gleichlautend im § 312j) bekannt wurde. Darin ist geregelt, dass Online-Händler dazu verpflichtet sind, vor einer kostenpflichtigen Bestellung im Internet folgende Informationen „klar, verständlich und in hervorgehobener Weise zur Verfügung zu stellen"[5]:
Die gesamte Bestellübersicht mit

- Produktmerkmalen,
- Mindestlaufzeit,
- Gesamtpreis,
- Versandkosten und
- Zusatzkosten.

Der Button selbst darf ausschließlich mit „zahlungspflichtig bestellen" oder einer ähnlich eindeutigen Formulierung beschriftet sein.

Beweispflicht der Händler

Verstößt der gewerbliche Händler gegen die o. a. Button-Vorschriften, kommt kein Vertrag zustande und damit auch keine rechtskräftige Bestellung des Produkts. Wichtig ist dabei im Fall der Fälle, dass die Beweislast beim Anbieter liegt, d.h. er muss beweisen, dass er ordnungsgemäß über die Zahlungspflicht informiert hat.

Was tun im Falle einer Abmahnung?

Das Wort „Abmahnwelle" hat den Weg in den deutschen Sprachschatz gefunden und bezeichnet die massenhafte Abmahnung durch Rechtsanwälte, vor allem bei Urheberrechtsverletzungen. Dabei ist die Abmahnung als Rechtsmittel eigentlich eine gute Idee, soll sie doch Streitigkeiten auf direktem und kostengünstigem Wege – ohne sofort ein Gericht einzuschalten – beilegen. Das Problem daran ist, dass sofort sehr hohe Streitwerte unterstellt werden und somit eine Abmahnung lukrativ ist. Nach etwa 600.000 Abmahnungen im Jahre 2010 (ausgewiesen in der Jahresstatistik des „Abmahnwahn e.V."[6]) mit einem Volumen von 500 Millionen Euro und geschätzten 4,3 Millionen Abmahnungen in Deutschland bislang, reagierte der Gesetzgeber. Am 1. Oktober 2013 trat das „Gesetz gegen unseriöse Geschäftspraktiken" (UWGuaÄndG) in Kraft, das eine Reihe von Neuerungen für Abmahnungen enthält. Die wohl für Verbraucher wichtigste ist der § 97a des Urheberrechtsgesetzes[7]:

§

Für die Inanspruchnahme anwaltlicher Dienstleistungen beschränkt sich der Ersatz der erforderlichen Aufwendungen hinsichtlich der gesetzlichen Gebühren auf Gebühren nach einem Gegenstandswert für den Unterlassungs- und Beseitigungsanspruch von 1.000 Euro, wenn der Abgemahnte

1. *eine natürliche Person ist, die nach diesem Gesetz geschützte Werke oder andere nach diesem Gesetz geschützte Schutzgegenstände nicht für ihre gewerbliche oder selbständige berufliche Tätigkeit verwendet, und*
2. *nicht bereits wegen eines Anspruchs des Abmahnenden durch Vertrag, auf Grund einer rechtskräftigen gerichtlichen Entscheidung oder einer einstweiligen Verfügung zur Unterlassung verpflichtet ist.*

Das heißt: Beim ersten Vergehen darf der Streitwert für Privatpersonen 1.000 Euro nicht übersteigen. Und damit ist auch die entsprechende Höhe der Abmahnung gedeckelt.

Wenn die Forderung auf jeden Fall unberechtigt ist, dann rät die Verbraucherzentrale, sie sicherheitshalber mit einem Schreiben (per Einschreiben!) abzuwehren. Dazu stellt sie Musterbriefe zur Verfügung: **www.vz-nrw.de/musterbriefe-onlineabzocke**.
Eigentlich muss auf Drohungen in E-Mails, Briefen usw. nicht reagiert werden und es darf ein Mahnbescheid des Gerichts abgewartet werden, der innerhalb von 14 Tagen beantwortet werden muss. Sinnvoll ist es in der Regel eine Rechtsberatung in Anspruch zu nehmen, bei Kindern und Jugendlichen natürlich durch die Eltern.

App-Zocke

Abzocke-Methoden gibt es schon lange auf dem Handy, erinnert sei an die vielbeworbenen Klingelton-Abos. Seit der massenhaften Verbreitung von Smartphones entwickeln sich ganz neue Betrugsmethoden über Apps. Kostenlose Apps auf dem Smartphone finanzieren sich meist über Werbung und hier bringen sich Abofallen, meist getarnt als simple Werbeeinblendung, in Stellung.
Problematisch sind auch sogenannte In-App-Käufe. Darunter versteht man kostenpflichtige Zusatzfunktionen, die man im Rahmen einer App erwerben kann. Bei Spielen kann es sich dabei beispielsweise um „extra Leben" oder erweiterte Versionen des Spiels handeln. Durch viele, scheinbar kleine Beträge kann sich so eine stolze Summe ansammeln.
Vor Kostenfallen in Bezug auf die In-App-Käufe kann man sich schützen, indem man diese sperrt. Dazu kann man in den meisten Smartphone-Betriebssystemen Beschränkungen setzen. Anleitungen dazu gibt es unter **www.klicksafe.de/themen/kommunizieren/smartphones/apps-abzocke/**

Drittanbietersperre aktivieren!

Vor Abofallen und damit vor unerwarteten Kosten kann man sich durch die sogenannte Drittanbietersperre schützen. Der Drittanbieter ist in diesem Fall der Anbieter des ungewollten Abos. Die Sperrung erreicht man durch einen Anruf bei seinem Mobilfunkanbieter oder einem entsprechend an diesen gerichteten Brief. Eine Vorlage für ein solches Schreiben ist auf der Internetseite der Verbraucherzentrale Niedersachsen zu finden: **www.verbraucherzentrale-niedersachsen.de/link1810509A.html**

Links und weiterführende Informationen

Webseiten

www.klicksafe.de/themen/kommunizieren/smartphones/apps-abzocke/
Informationen auf klicksafe.de zu Abzocke bei Apps

www.handysektor.de/abo-abzocke/uebersicht.html
Übersichtsseite von handysektor zum Themenbereich Abo+Abzocke

www.klicksafe.de/service/materialien/broschueren-ratgeber/abzocke-im-internet-erst-durchblicken-dann-anklicken/
Flyer Abzocke im Internet von klicksafe und der Verbraucherzentrale NRW

www.internet-abc.de/eltern/abzocke-kostenfallen.php
Informationen für Eltern zu Abzocke im Internet von Internet-ABC

www.vz-nrw.de/musterbriefe-onlineabzocke
Musterbriefe der Verbraucherzentrale NRW

www.verbraucherzentrale-niedersachsen.de/link1810509A.html
Vorlage für die Drittanbietersperre der Verbraucherzentrale Niedersachsen

Endnoten

[1] SAUER, P. J. (2015, 12. Mai). *Confessions of a Viral Video Superstar.* Aufgerufen am 13.05.2015 unter http://www.inc.com/articles/2008/06/blendtec.html

[2] JFF. (2014). *Kernergebnisse der Studie „Jugendliche und Online-Werbung im Social Web".* Aufgerufen am, 13.05.2015 unter www.jff.de/jff/aktivitaeten/forschung/artikel/art/ergebniszusammenfassung-der-studie-jugendliche-und-online-werbung/

[3] BRÜGGEN, N., Dirr, E., Schemmerling, M. & Wagner, U. (2014): *Jugendliche und Online-Werbung im Social Web. Herausgegeben von Bayerisches Staatsministerium für Umwelt und Verbraucherschutz.* Aufgerufen am 13.05.2015 unter www.jff.de/jff/fileadmin/user_upload/Projekte_Material/verbraucherbildung.socialweb/JFF-Studie_Jugendliche_Online-Werbung_SocialWeb.pdf

[4] VERBRAUCHERZENTRALE Niedersachsen (2015). *Internetabzocke: Die Maschen der Betrüger.* Aufgerufen am 13.05.2015 unter http://www.verbraucherzentrale-niedersachsen.de/RG458571A0AM/linkpdf?unid=461711A

[5] BÜRGERLICHES Gesetzbuch (BGB). *§ 312j Besondere Pflichten im elektronischen Geschäftsverkehr gegenüber Verbrauchern.* Aufgerufen am 13.05.2014 unter http://www.gesetze-im-internet.de/bgb/__312j.html

[6] INTERESSENSGEMEINSCHAFT gegen den Abmahnwahn (2014). Abmahnstatistik 2010. Aufgerufen am 13.05.2015 unter http://www.iggdaw.de/filebase/index.php/Entry/8-Abmahnstatistik-2010/

[7] URHEBERRECHTSGESETZ. *§ 97a Abmahnung.* Aufgerufen am 13.05.2015 unter http://www.gesetze-im-internet.de/urhg/__97a.html, Aufruf vom 20.07.2014

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Internet – alles Werbung?**	**Google = Werbung?**
Kompetenzen	Die Schülerinnen und Schüler erkennen anhand einer Liste von Internet-Werbeformen entsprechende Beispiele auf Webseiten.	Die Schülerinnen und Schüler beschreiben die Werbeformen AdSense, AdWords und Behaviour Targeting und übertragen dies in ein Rollenspiel.
Methoden	Tabelle, Internet-Recherche, Unterrichtsgespräch	Internet-Recherche, Rollenspiel, Unterrichtsgespräch
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	90	135
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Internet – alles Werbung?	Die Schülerinnen und Schüler sind sich oft darüber im Klaren, dass sie von Werbung umgeben sind, es ist für sie normal. Vielleicht können Sie in einem Unterrichtsgespräch den einleitenden Satz „Werbung möchte nur eines: Dich zum Kauf auffordern!" thematisieren. Die Liste der Werbeformen kann ergänzt werden, da die Werbeindustrie ständig neue Formen entwickelt, wenn sich alte als gewohnt und deshalb wenig effektiv herausstellen. Vielleicht finden die Schülerinnen und Schüler sogar weitere Werbeformen, die nicht in das aufgeführte Raster passen. Nach der grundsätzlichen Erarbeitung der Formen sollen die Schülerinnen und Schüler praktische Beispiele finden. Sie dürften fündig werden bei den großen Anbietern wie Amazon, YouTube, Google, aber auch bei den kommerziellen Fernsehsendern wie RTL oder Pro7 etc. Werbe-E-Mails sind sicherlich ebenfalls leicht zu finden und vielleicht finden Sie ein aktuelles Beispiel für virales Marketing (in Sozialen Netzwerken) für das sich Werbetreibende aus Effizienzgründen gerne engagieren. Die Ergebnisse sollen sich die Schülerinnen und Schüler gegenseitig vorstellen, indem nur die Seite genannt wird und die Werbeform selbst gesucht werden soll.
AB 2: Google = Werbung?	Die Schülerinnen und Schüler sollen sich innerhalb ihrer Gruppen über das System von AdSense und AdWords sowie „Behavioral Targeting" informieren. In der gespielten Fernsehdiskussion zum Thema „Alles nur Werbung oder was? Müssen Jugendliche beschützt werden?" lernen sie, sich mit den verschiedenen Positionen auseinander zu setzen. Wichtig ist eine anschließende Distanzierung von den Rollen und eine Reflexion des „Spiels".

Lust auf mehr?

- Werbung ist ohnehin Bestandteil vieler Lehrpläne. Die immer stärkere Internetwerbung ist sicherlich ein spannendes Thema. Hier gelten die üblichen Werberegeln und -mechanismen nur zum Teil, da es sich um ein interaktives Medium handelt. Vielleicht ist ein Vergleich von Werbung in Zeitung, Fernsehen und Internet spannend.
- Media smart bietet Materialpakete für Lehrer sowie interaktive Spiele und Übungen, die vor allem jüngeren Kindern helfen, Werbung zu durchschauen: **www.mediasmart.de**

Internet – alles Werbung? (1/2)

Stört dich Werbung? Sie ist allgegenwärtig und hat immer das gleiche Ziel:
Dich zum Kaufen aufzufordern.
Im Fernsehen kann man Werbung ganz gut erkennen, aber im Internet ist Werbung oft schwierig vom Inhalt der Seite zu unterscheiden.

Es gibt viele verschiedene Werbeformen im Internet, die sich ständig weiterentwickeln.
Hier findest du einige typische: Achtung, jetzt kommen viele englische Ausdrücke aus der Werbesprache.

A Affiliate
Affiliate bedeutet übersetzt „Partner" und damit ist das „Affiliate-Marketing" auch gut beschrieben. Bei dieser Werbung bietet der Betreiber einer Webseite einer anderen Firma Platz für Werbung (selbstverständlich gegen Bezahlung)

B In-Page – der Klassiker
Display-Advertising oder kurz „Display-Ads" kann man grob unterscheiden in die Formen von „In-Page" und „In-Stream Videos". Mit „In-Page" ist das klassische Werbebanner gemeint, das man oft als Rechteck oben und seitlich entdecken kann.

C Content und In-Text
Content-integrierte Werbung („Integrated advertising") ist im redaktionellen Bereich einer Website platziert und ist oft nur schwer zu erkennen. Dabei werden bestimmte Begriffe verlinkt, die mit der Werbung in Verbindung stehen.

D In-Stream-Video-Werbung
Hier erfolgt die Werbung in Form eines – meist kurzen – Videos. Das sieht man häufig auf Videoplattformen wie YouTube.

E Search-Marketing
Hier kennen alle die Form der Werbung in der Suchmaschine Google. Dabei können Firmen ihre Werbung entsprechend der Suchbegriffe der Kunden einblenden.

F Sponsoring
Dabei werden Gewinnspiele, Downloads oder andere attraktive Aktionen von Sponsoren präsentiert, um ein positives Image bei der jungen Zielgruppe aufzubauen.

G Werbespiele
Werbespiele (Advergames, Adgames) sind gesponserte Onlinespiele, die in werbefinanzierten Websites oder auf firmeneigenen Websites eingebunden werden können.

H Alles ist Werbung
Der gesamte Internetauftritt kann als Werbefläche dienen. Auch Newsletter, Gewinnspiele und Clubmitgliedschaften dienen oft Werbezwecken.

I Werbe-Mails
Werbe-Mails sind mit Hinweisen auf Produkte und Bestellmöglichkeiten und zum Teil auch mit Links zu Onlineshops versehen.

J Virales Marketing
Damit ist eine massenhafte und schnelle Verbreitung (wie ein Virus eben) der Werbebotschaft über Soziale Netzwerke gemeint.

Internet – alles Werbung? (2/2)

Arbeitsaufträge:

1. Suche im Internet nach Beispielen für die Werbeformen A bis J. Fülle folgende Tabelle aus:

Werbeform	Internet-Adresse	Werbung für	So sah die Werbung aus
A			
B			
C			
D			
E			
F			
G			
H			
I			
J			

2. Findest du auch Beispiele für ziemlich gut versteckte Werbung?
   Wenn ja, dann stelle sie den anderen vor:
   Nenne ihnen die Seite und lasse sie selbst suchen.

Tipp: *Bei Blinde Kuh gibt es ein lustiges Spiel: „Pop-up-Kong-Fu“*
www.blinde-kuh.de/spiele/popupkongfu/

Google = Werbung?

Google *gilt als der Perfektionierer des Werbesystems im Internet. Google Inc. wurde 1998 gegründet und hat seinen Hauptsitz im Mountain View, Kalifornien. Seit 2004 ist es ein Börsenunternehmen. Bereits 2005 hatte Google einen marktbeherrschenden Anteil an allen Suchanfragen im Internet. Am 14.4.2007 kaufte Google die Werbefirma DoubleClick für einen Preis von 3,1 Mrd. Dollar. Google verwendet die Systeme „AdWords" und „AdSense".*

Das Ziel von Werbung ist, dich zum Kauf aufzufordern. Leider (für die Werbetreibenden) hat normale Werbung hohe Streuverluste (wie viele kaufen schon ein Produkt nach einer normalen Fernsehwerbung?), deshalb wurden neue Formen der Werbung entwickelt. Ein Verfahren heißt „Behavior Targeting" und dies funktioniert besonders gut in interaktiven Medien wie dem Internet.

Arbeitsaufträge:

1) Teilt euch bitte einer der folgenden Gruppen zu:

Jugendliche oder Jugendlicher	Vater oder Mutter	Firma Malki	Google
Du bist genervt von der Werbung und versuchst, dich vor ihr zu schützen.	Du bist besorgt, wie viel Werbung es für Kinder und Jugendliche gibt.	Du möchtest für dein Produkt „Malki-Schokolade" Werbung für Jugendliche machen.	Du verkaufst Werbung über AdWords und AdSense.
Informiert euch bitte darüber, wie AdWords funktioniert.			
Informiert euch darüber, wie AdSense funktioniert.			
Informiert euch darüber, was „Behavior Targeting" ist und wie es funktioniert.			
Entwickelt eine Strategie, eure Interessen zu vertreten.			

2) Bereitet in den Gruppen eine „Fernseh"-Diskussion vor, in der über die Frage diskutiert werden soll: „Alles nur Werbung oder was? Müssen Jugendliche beschützt werden?" Die vier Aufgaben unter den Rollenbeschreibungen helfen euch dabei.

3) Führt diese Diskussion durch (wählt noch eine neutrale Moderatorin oder einen neutralen Moderator).

4) Besprecht danach den Verlauf und die Ergebnisse. Versucht dabei die Frage der Diskussion zu beantworten!

Tipps:

- ***http://adwords.google.de***
- ***http://www.google.com/adsense/start***

Es gibt in Deutschland klare gesetzliche Regelungen für Werbung für Kinder und Jugendliche, die leider nicht immer eingehalten werden.
Werbung

- *muss im Fernsehen deutlich zu erkennen sein und darf Kindersendungen nicht unterbrechen*
- *darf keine direkte Kaufaufforderung an Kinder und Jugendliche haben (Kinder, kauft das!)*
- *darf Kinder und Jugendliche nicht auffordern, ihre Eltern zu überreden*
- *darf nicht die „Unerfahrenheit" und „leichte Beeinflussbarkeit" von Kindern ausnutzen*
- *darf Kinder und Jugendliche nicht in gefährlichen Situationen zeigen*
- *darf Süßigkeiten nicht als „gesunde Lebensmittel" darstellen*
- *darf Jugendliche nicht beim Trinken von Alkohol zeigen*
- *darf keine Jugendsprache oder Situationen in der Tabakwerbung zeigen*
- *darf keine Models in der Tabakwerbung haben, die jünger als 30 Jahre sind*

7|1 Spam und Schadsoftware
7|2 Hoaxes, Kettenbriefe und Shitstorms
7|3 Illegale Downloads und Tauschbörsen

7 Was wir nicht brauchen: Unerwünschtes und Unnötiges

Spam und Schadsoftware

Spam

Als **Spam** oder auch **Junk** werden unerwünschte Werbe-E-Mails bzw. unerwünschte Nachrichten bezeichnet. Der Ursprung des Begriffs „Spam" ist nicht ganz klar, steht jedoch vermutlich in Zusammenhang mit dem Akronym des Dosenfleischs **Sp**iced H**am** der Firma **Hormel Foods**.[1] Die britische Komikergruppe **Monty Python** verwendete dann 1970 das Wort in einem Sketch in derartigem Übermaß, dass es wohl zum Synonym für die massenhafte und unerwünschte Verbreitung von etwas wurde.[2] „Junk" hingegen kommt aus dem Englischen und bedeutet schlicht „Abfall" oder „Müll".

Spam-Mails lohnen sich für die Absender, denn zum einen ist der Mail-Versand kostenlos und zum anderen öffnen Nutzer noch immer – versehentlich oder bewusst – Werbe-Mails. Einige Spam-Mails sind nicht nur nervig, sondern können auch Schaden anrichten: Durch vireninfizierte Spam-Mails kann der Computer des Adressaten ohne dessen Wissen Teil eines sog. **Botnets** werden. Das ist ein Netz bestehend aus mehreren Computern, die von Dritten ferngesteuert werden können, um bspw. Spam-Mails zu versenden oder gar andere Computer zu attackieren.[3] Diese automatisierten Computerprogramme werden in Anlehnung an das englische Wort für Roboter (**robot**) als **Bots** bezeichnet.

Spam-Mails sind meist nicht mehr bloß allgemein gehaltene unerwünschte Werbebotschaften. Viele Spam-Mails sprechen den Adressaten persönlich an – bspw. durch die Verwendung des Vor- und Nachnamens – und sind attraktiv gestaltet.

Spam kann in unterschiedlichen Kontexten auftauchen und verschiedene Formen annehmen.

Formen von Spam

Spam-Mail

Unerwünschte Werbe-Mails sind die wohl häufigste Spam-Form. Das amerikanische Software-Unternehmen **Symantec** hielt in seinem Bericht für den Monat Juni 2015 fest, dass 49,7 % des gesamten erfassten E-Mail-Verkehrs Spam war.[4] Spam-Mails können in drei Arten differenziert werden:

- **Scam**
  Scam (zu Deutsch „Betrug") bezeichnet E-Mails, die Angebote für besonders günstige, einmalige Waren oder Geschäfte enthalten und den Adressaten auffordern, diese zu kaufen. Der Käufer erhält nach der Überweisung des Geldes das versprochene Produkt jedoch nicht.[5]
- **Hoax**
  Hoax (zu Deutsch „Täuschung" oder auch „Falschmeldung") bezeichnet eine Spam-Mail, die in Form eines Kettenbriefes versandt wird und die Aufforderung beinhaltet, die E-Mail an möglichst viele Freunde und Bekannte weiterzuleiten. Inhaltlich geht es in den Hoax-Mails meist um Warnungen, Einladungen oder Aufrufe. Hoaxes werden natürlich nicht nur per E-Mail versandt. Sie kursieren auch in Sozialen Netzwerken wie bspw. Facebook.[6] Meist sind die Hoaxes schlicht nervig – einige allerdings enthalten auch Viren, die den Computer des Empfängers infizieren, schlimmstenfalls ausspionieren oder gar fernsteuern können.
- **Phishing**
  Phishing setzt sich zusammen aus den beiden englischen Begriffen „Password" und „Fishing" und bezeichnet das kriminelle Abgreifen wichtiger Passwörter. Betrüger schicken gefälschte Nachrichten an Nutzer, um an deren Zugangsdaten, bspw. für das Bankkonto zu gelangen. Die Mails verlinken auf Seiten, die vorgeben von seriösen Kreditinstituten zu sein und greifen so die Bankdaten derjenigen Nutzer ab, die auf diesen Seiten aktiv sind.[7]

Spam dieser Art findet sich nicht nur in E-Mails, sondern auch in Sozialen Netzwerken. Dort gibt es auch weitere Arten von Spam: So finden Nutzer auf ihrer Pinnwand bspw. Posts vor, die ihr Interesse wecken sollen, z.B. mit einer spannenden Aussage oder einem verlockenden Privat-Video eines Stars. Wird dieser Post dann angeklickt, gelangen die Nutzer meist nicht auf den erwarteten Inhalt. Stattdessen wird den Freunden des Nutzers angezeigt, dass er oder sie besagten Post **geliked** hat. Auf diese Weise werden solche Posts schnell verbreitet und mit ihnen schlimmstenfalls auch Viren. Facebook bietet hier bspw. die Möglichkeit an, derartige Beiträge zu melden und als Spam zu deklarieren.

Suchmaschinen-Spam
Suchmaschinen-Spamming bezeichnet den Versuch, das Ranking einer Webseite innerhalb der Suchergebnisse mittels unlauterer Methoden zu verbessern. Das funktioniert auf verschiedenen Wegen: bspw. durch die unnatürlich häufige Verwendung eines Suchbegriffs im Text der Webseite, deren Ranking verbessert werden soll. Oder es werden eigens Seiten generiert, die ausschließlich Links auf die Seiten enthalten, die optimiert werden sollen. Hintergrund ist hier, dass Suchmaschinen die Relevanz einer Webseite nicht zuletzt auch an der Menge und Qualität der Verlinkungen durch andere Seiten messen. Suchmaschinen-Anbieter identifizieren solche Seiten aber immer effektiver als Spam und strafen sie durch Ausschluss aus ihrem Such-Index ab.[8]

Mobile Spam
Da das Smartphone ein medialer Alleskönner ist und viele Funktionen, wie z. B. E-Mail, Internet und damit auch Dienste wie Soziale Netzwerke auf sich vereint, sind auch die Spam-Formen nicht grundlegend neu: Spam kann in Form von Spam-Mails oder SMS-Spam auftreten und birgt die gleichen Gefahren wie auch für Desktop-Computer (z. B. Viren, Botnets). Auch über die verschiedenen Apps, wie z. B. **WhatsApp**, **Snapchat** oder **Instagram** können unerwünschte Werbebotschaften versendet werden. Meist ist es möglich, diese dem Anbieter direkt zu melden.

Spam: Was sagt das Gesetz?
In Deutschland ist das unaufgeforderte Zusenden von Werbung laut § 1 des Gesetzes gegen den unlauteren Wettbewerb (UWG) dann verboten, wenn die Werbung in unzumutbarer Weise belästigt.[9] Aus diesem Grund verschicken Spammer ihre Botschaften ent-weder über Internetanbieter aus dem Ausland oder über Botnets. Wenn Spam im Postfach gelandet ist, muss der Adressat diesen gemäß Artikel 10 des Brief-, Post- und Fernmeldegeheimnisses selbst löschen bzw. durch entsprechende Programme automatisch löschen lassen.[10] Auch in § 6 des Telemediengesetzes (TMG) findet sich eine konkrete Regelung über die „kommerzielle Kommunikation": Eine E-Mail darf ihren werblichen Charakter in Absender- und Betreffzeile nicht verschleiern und muss für den Nutzer klar erkennbar sein.[11] Art. 13 der europäischen Datenschutzrichtlinie über die elektronische Kommunikation (2002/58/EG) sieht überdies vor, dass das Versenden von Werbung nur mit vorheriger Einwilligung zulässig ist (Opt-in-Verfahren).[12]

Schutz vor Spam
Spam ist meist ärgerlich, aber harmlos. Kritisch wird es, wenn Spam mit Viren infiziert ist oder auf entwicklungsbeeinträchtigende Inhalte, wie z. B. Webseiten mit problematischen Gewalt- oder Sexualdarstellungen, verlinkt. Um Spam vorzubeugen und dessen Anzahl zu beschränken, sind folgende Maßnahmen hilfreich:

1. *Mit der eigenen E-Mail-Adresse bedacht um-gehen und evtl. eine zweite E-Mail-Adresse im Sinne einer „Wegwerfadresse" anlegen*

Viele Dienste-Anbieter im Internet, seien es Shops, Newsletter, Portale etc. verlangen bei der Registrierung die E-Mail-Adresse des Nutzers. Da diese Adress-Daten leicht in die Hände von Werbetreibenden geraten können bzw. die Daten ganz bewusst von einigen Dienste-Anbietern weitergegeben werden, lohnt es sich, eine zweite E-Mail-Adresse anzulegen. Diese kann immer dann angegeben werden, wenn man keinen Wert auf News, Benachrichtigungen über Sonderangebote etc. seitens des Dienste-Anbieters legt. Einige E-Mail-Provider bieten sogar spezielle E-Mail-Accounts an, die nur für kurze Zeit gültig sind und die eingehende E-Mails nach einem bestimmten Zeitraum automatisch löschen. Anbieter, die solche **Wegwerf**-Adressen bereitstellen, sind u. a.: **https://www.trash-mail.com/**

http://www.wegwerfemail.de/ oder **http://spoofmail.de/**. Selbst große E-Mail-Provider wie bspw. **Yahoo!** bieten ihren Nutzern die Möglichkeit, unter der eigenen (richtigen) E-Mail-Adresse, Wegwerf-Adressen einzurichten.

❷ *Nicht auf Spam reagieren, d. h. keine Anhänge / Links öffnen*

Wichtig ist, nicht auf Spam zu reagieren und sich weder beim Absender der Nachricht zu beschweren, noch Anhänge oder Links zu öffnen. Letztere könnten mit Viren verseucht sein und damit den Computer infizieren. Die Rückmeldung beim Absender des Spams bestätigt diesem die Richtigkeit der Adresse, was schlimmstenfalls zu noch mehr Spam-Mails führen kann! **Wichtig:** Dieses Prinzip gilt auch für die Abwesenheitsnotiz bei Urlaub. Diese muss unbedingt nach dem Spam-Filter geschaltet werden, da sonst die Spammer ebenfalls wissen, dass die E-Mail-Adresse korrekt ist.

❸ *Spam-Filter und Schutzprogramme installieren*

Spam-Filter sind entweder direkt auf dem Computer des Nutzers installiert (z. B. im Fall von Outlook) oder aber sie liegen auf dem Server des E-Mail-Providers. In letzterem Fall kann der Nutzer den Filter nicht weiter beeinflussen und muss auf ausreichenden Schutz vertrauen. In dem Falle eines eigenen Filters ist der Nutzer für das regelmäßige Update des Spam-Filters selbst verantwortlich, kann allerdings auch Einstellungsänderungen selbst vornehmen. Neben einem Spam-Filter sollte jeder Computer zudem über ein funktionsfähiges Virenschutzprogramm verfügen, das in regelmäßigen Abständen aktualisiert wird. Auch eine sog. **Firewall**, zu Deutsch „Brandschutzmauer", ist sinnvoll – sie überprüft alle Daten, die der User aus dem Netz lädt sowie die Daten, die von dem Computer ins Netz geschickt werden.

❹ *Spam-Filter „trainieren"*

Alle deutschen E-Mail-Provider haben einen Spam-Filter integriert. Dieser sorgt dafür, dass verdächtige E-Mails in einem separaten Spam-Ordner landen. Wenn sich doch noch die eine oder andere Spam-Mail im regulären Posteingang findet, kann diese dem E-Mail-Anbieter als Spam gemeldet werden. So kann der Anbieter das nächste Mal besser reagieren und ähnliche E-Mails direkt im Spam-Ordner ablegen.

❺ *Wachsam sein bei dubiosen Nachrichten*

Ist der Absender einer Nachricht nicht bekannt oder erscheint die Betreffzeile seltsam, dann sollte die Nachricht sowie auch ihre Anhänge oder Links nicht geöffnet werden.

❻ *Eigene E-Mail-Adresse verschleiern*

Es gibt keine Möglichkeit, die eigene E-Mail-Adresse z. B. im Impressum der eigenen Webseite sicher zu verschleiern. Es kann nur versucht werden, das Ausfindigmachen der richtigen E-Mail-Adresse für Bots zu erschweren. „@" durch „at" zu ersetzen gehört zu den einfach zu knackenden Lösungen. Schwieriger ist es für Bots hingegen, bspw. sog. **Captchas** zu entschlüsseln. Hinter „Captcha" verbirgt sich die Phrase „**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part" – Tests also, mittels derer zwischen Menschen und Programmen unterschieden werden soll. Man kennt sie in Form von Zahlen- und/oder Buchstabenkombinationen, die auf einem Bild zu sehen sind und die dann durch den Nutzer in ein separates Feld eingegeben werden müssen.[13]

❼ *Eintragung in Robinsonliste*

In die Robinsonliste können sich Verbraucher eintragen, die keine weitere unerwünschte Werbung via Post, Telefon, E-Mail, Mobil oder Fax erhalten wollen: **https://www.robinsonliste.de**.
Werbetreibende Unternehmen können die Robinsonliste mit ihrer Empfängerliste abgleichen und so sicherstellen, dass Verbraucher, die keine Werbung wünschen, auch keine erhalten. Die Eintragung in die Liste bietet allerdings keinen vollkommen sicheren Schutz vor unerwünschter Werbung, denn nicht alle Werbetreibenden halten sich an den Wunsch des Verbrauchers.

❽ *Benutzerprofile*

Auf Geräten sollte generell als normaler Benutzer und nicht als Administrator gearbeitet werden. Auf diese Weise kann Schaden, den Schadsoftware anrichten kann, beträchtlich vermindert werden.

Tipp: *Spam und rechtswidrige Online-Inhalte können an die Internetbeschwerdestelle gemeldet werden:*
http://www.internet-beschwerdestelle.de/

Links und weiterführende Informationen

Webseiten

www.klicksafe.de/themen/kommunizieren/spam/
Hier finden sich weiterführende Informationen zu Spam.

www.vz-nrw.de/home
Auf der Seite der Verbraucher-Zentrale finden sich umfassende Informationen rund um das Thema Werbung, E-Commerce, Datenschutz u. v. m.

www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Spam/Schutzmassnahmen/schutzmassnahmen_node.html
Informationsseite zu Spam vom Bundesamt für Sicherheit in der Informationstechnik.

www.lehrer-online.de/it-sicherheit.php
Informationsseite für Lehrer zu vielen verschiedenen Themen – u. a. über IT-Risiken.

http://praxistipps.chip.de/wegwerf-email-adressen-diese-anbieter-gibts_1674
Hier sind noch weitere Anbieter von sog. Wegwerf-Adressen aufgeführt.

www.datenschutzzentrum.de/selbstdatenschutz/internet/pgp/version.htm
Hier finden sich genaue Informationen zur Verschlüsselung von E-Mails mittels des Pretty-Good-Privacy-Verfahrens.

www.internauten.de/index.html?mission=E-Mail_Spam/index.html
Ein Online-Spiel, das sich an Kinder richtet und verschiedene Internetrisiken als Missionen aufbereitet – u. a. auch E-Mail und Spam.

www.youtube.com/watch?v=anwy2MPT5RE
Spam-Sketch von Monty Python aus dem Jahr 1970.

Endnoten

[1] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI). (2015). *Spam-Definition.* Aufgerufen am 10.07.2015 unter https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Spam/spam_node.html

[2] ebd.

[3] BENDRATH, R. (2009, 18. Dezember). *Botnets, Internetanbieter und Politik – auf sanften Sohlen zu neuen nationalen Strukturen der Internet-Regulierung?* [Blog-Beitrag] Aufgerufen am 10.07.2015 unter https://netzpolitik.org/2009/botnets-internetanbieter-und-politik-auf-sanften-sohlen-zu-neuen-nationalen-strukturen-der-internet-regulierung/

[4] SYMANTEC. (2015, 16. Juli). *Symantec Intelligence Report: June 2015* [Blog]. Aufgerufen am 20.07.2015 unter http://www.symantec.com/connect/blogs/symantec-intelligence-report-june-2015

[5] TECHFACTS. (2014, 15. Mai). *Was ist Scam?* Aufgerufen am 10.07.2015 unter http://www.techfacts.de/ratgeber/was-ist-scam

[6] ZIEMANN, F. (2015, 18. Juli). *TU-Berlin: Hoax-Liste.* Aufgerufen am 20.07.2015 unter http://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml

[7] VERBRAUCHERZENTRALE NRW. (2015, 21. Januar). *Spam: E-Mail-Müll auf der Datenautobahn.* Aufgerufen am 10.07.2015 unter http://www.vz-nrw.de/spam#arten

[8] LAMMENETT, E. (2007). *TYPO3 Online-Marketing-Guide. Affiliate- und E-Mail-Marketing Keyword-Advertising, Suchmaschinen-Optimierung mit TYPO3.* Wiesbaden: Verlag Dr. Th. Gabler.

[9] GESETZ GEGEN DEN UNLAUTEREN WETTBEWERB (UWG). Aufgerufen am 18.11.2014 unter http://www.gesetze-im-internet.de/uwg_2004/

[10] GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND (GG). *Artikel 10.* Aufgerufen am 20.07.2015 unter http://www.gesetze-im-internet.de/gg/art_10.html

[11] TELEMEDIENGESETZ (TMG). Aufgerufen am 20.07.2015 unter http://www.gesetze-im-internet.de/tmg/

[12] DATENSCHUTZRICHTLINIE FÜR ELEKTRONISCHE KOMMUNIKATION. (2002, 12. Juli). Aufgerufen am 18.11.2014 unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32002L0058&from=DE

[13] GOOGLE. (k. A.). *reCAPTCHA: Tough on bots easy on humans* (Absatz 3). Aufgerufen am 19.11.2014 unter http://www.google.com/recaptcha/intro/

Schadsoftware

Schadsoftware wird oft auch als **Malware** bezeichnet. Dieser Begriff setzt sich zusammen aus dem englischen **mal**icious (zu Deutsch: boshaft) und Soft**ware**. Damit sind Programme gemeint, die Schaden an Computersystemen (PCs, Chips, Handys, Smartphones etc.) anrichten, Daten ausspionieren oder sich Zugang zu privaten Computersystemen verschaffen wollen.[14] Der erste **Wurm** (s. u.) war wohl der sog. **vampire worm**, den die beiden Programmierer des **XEROX**-Unternehmens John Hepps und John Shock in den 80er Jahren programmierten: Das kleine Programm war eigentlich dazu entwickelt worden, über Nacht automatisch Prozesse abzuwickeln, die tagsüber aufgrund der hohen Auslastung des Prozessors durch das Tagesgeschäft nur schwer möglich waren. Der **vampire worm** legte jedoch eines Tages bedingt durch einen Prozessfehler alle Computer des Unternehmens lahm und musste daher entfernt werden.[15]

Als erster **Virus** (s. u.) gilt wohl die Schadsoftware **Brain**, die von zwei pakistanischen Brüdern entwickelt wurde.[16] Sie infizierte bestimmte Bereiche einer Diskette, wodurch der Zugriff auf diese extrem verlangsamt wurde. Eine Infizierung blieb durch die Nutzer in vielen Fällen unbemerkt. Seither haben verschiedene, weitaus schädlichere Malware-Programme immer wieder öffentliches Aufsehen erregt: darunter **Marburg, LoveLetter, Sasser, Flame** u. v. w. m. Es gibt verschiedene Arten von Malware:

- **Virus**
  Ein Virus ist ein Schadprogramm, das sich selbstständig vervielfältigen kann und auf diese Weise schnell verbreitet. Der Virus heftet sich an andere Programme und kann so ohne Wissen des Nutzers beim Download von Dateien aus dem Internet, über USB-Stick etc. den eigenen Computer infizieren. Die Größe des Schadens, den Viren anrichten, variiert stark: von harmlosen sinnlos ausgegebenen Textstücken bis hin zur Löschung der gesamten Festplatte.[17]

- **Wurm**
  Würmer sind dem Virus sehr ähnlich: Auch sie können sich selbstständig vervielfältigen, nachdem sie einmal ausgeführt wurden. Anders als Viren infizieren Würmer aber keine fremde Dateien und auch nicht den Startsektor eines Laufwerks. Würmer werden meist über infizierte E-Mails oder Links verbreitet. Würmer verbrauchen viele Netzwerkressourcen und können einen Computer so lahmlegen.[18]

- **Trojaner**
  Der Begriff ist angelehnt an das Trojanische Pferd der griechischen Mythologie. Entsprechend bezeichnet der Trojaner im Kontext der Schadsoftware ein Programm, das sich in scheinbar vertrauenswürdigen, seriösen Programmen versteckt.[19] Der Trojaner kann darüber unbemerkt auf dem Computer installiert werden. Oft sind Trojaner sog. **Spyware**.

- **Spyware**
  Unter Spyware sind Programme zu verstehen, die unbemerkt auf dem PC installiert werden und vertrauliche Daten, Passwörter, Surfverhalten, Informationen über benutzte Programme etc. des infizierten Computers ausspionieren (auf Englisch: „to spy"). Diese Informationen können dann einerseits für die Abzocke genutzt werden oder kommen Werbefirmen zugute, die auf dieser Basis zielgenau Werbung ausbringen können.[20]

- **Scareware**
  Scareware setzt sich zusammen aus den beiden englischen Begriffen **scare** (zu Deutsch: jmd. erschrecken) und Soft**ware**. Darunter zu verstehen sind Schadprogramme, die beim Nutzer durch gefälschte Warnmeldungen, z. B. über eine Virenifektion, Ängste schüren sollen. Dies soll den User dann dazu verleiten, eine bestimmte (Schad-) Software zu installieren.[21]

- **Ransomware**
  „Ransom" bedeutet übersetzt „Erpressung". Diese Art der Schadsoftware versucht den Nutzer zu erpressen, indem die Nutzung des Computers gesperrt und der Nutzer dazu aufgefordert wird, einen bestimmten Geldbetrag zu zahlen, um wieder auf den Rechner zugreifen zu können.[22]

- **Dialer**
  Programme, die eine Telefonverbindung oder den Versand von SMS über hochpreisige Dienste herstellen.

Aus der Praxis
Zu diesem Thema können sich die eher technisch interessierten SchülerInnen verwirklichen. Vielleicht bietet sich die Gelegenheit, ein ***Live-Hacking*** *zu besuchen – eine Veranstaltung, auf der demonstriert wird, wie leicht Hacker an Daten gelangen und Dritte ausspionieren können. Alternativ gibt es unter diesem Stichwort sehr anschauliche Vorführungen in* ***YouTube****.*

Schadprogramme: Wirtschaftlicher Schaden
Für den betroffenen Nutzer sind Schadprogramme lästig, denn es kostet Zeit, Nerven und oftmals Geld, sich der Schadprogramme zu entledigen, einen sicheren Schutz zu installieren und beständig zu aktualisieren. Laut einer Studie der Sicherheitsfirma **Norton** aus dem Jahr 2012 haben Privatpersonen durch Malware weltweit einen finanziellen Schaden von insgesamt ca. 88 Milliarden Euro erlitten.[23]

Sehr häufig infizieren Nutzer ihre Geräte unbewusst während des Surfens auf seriösen, aber gehackten Seiten bzw. auf speziell erstellten Angriffs-Webseiten. Diese Art der Infektion wird **Drive-by-Download** genannt: Hacker integrieren den Schadcode in eine Webseite, woraufhin sich dann der Nutzer alleine durch den Besuch der Website automatisch und ohne es zu wissen, mit der Malware infiziert. **Drive-by-Downloads** stellen die am weitesten verbreitete Art der Infektion mit Malware dar.[24]

Suchmaschinen-Anbieter wie Google versuchen Webseiten, die Malware enthalten, zu erkennen. Wird eine Webseite als infiziert erkannt, wird dem Nutzer, der auf die Seite zugreifen möchte, eine Warnung angezeigt.[25]

Smartphone & Schadware
Im Grunde sind mobile Endgeräte von den gleichen Schadprogrammen bedroht wie Desktop-PCs.
Durch die nahezu flächendeckende Ausstattung mit Smartphones und Tablets hat sich jedoch immer mehr Schadsoftware gezielt auf die mobilen Endgeräte spezialisiert: Es gibt Schadprogramme, welche unbemerkt Kamera und Mikrofon eines Smartphones aktivieren und die Daten aufzeichnen, Malware, die auf Standortdaten eines Gerätes zugreift und alle getätigten Aktionen nachverfolgt etc.[26]

Android-Geräte sind eher anfällig für Malware.[27] Das liegt zum einen an der hohen Verbreitung von Android-betriebenen Geräten und zum anderen daran, dass Google es seinen Nutzern relativ leicht ermöglicht, neben dem offiziellen Google-Play-Store auch weitere Stores zu nutzen, um Apps zu beziehen. Diese App-Stores von Dritten haben teilweise eine fragwürdige Sicherheitspolitik und Malware findet daher leicht Eingang. Apple verfolgt eine restriktivere Politik und prüft jeder App auf deren Sicherheit, ehe diese im App-Store eingestellt wird.

Tipp:
Das ***Bundesamt für Sicherheit in der Informationstechnik*** *bietet einen aktuellen Informationsservice und spricht Virenwarnungen aus, wenn dies eine kritische Masse deutscher Nutzer betrifft:* ***https://www.buerger-cert.de/***
Außerdem gibt es auch auf den Seiten der Antiviren-Hersteller regelmäßig Informationen über neue Bedrohung z. B. von ***Kaspersky*** *unter* ***http://www.viruslist.com****.*

Schutz vor Schadprogrammen
Um sich vor Schadprogrammen zu schützen, sind folgende Maßnahmen und Übergelungen sinnvoll:

1. ***Antivirenprogramm / Firewall installieren & aktualisieren***

Auf jedem Gerät sollten ein Antivirenprogramm und eine Firewall installiert sein. Es gibt gute kostenlose und gute kostenpflichtige Software. Gleich, für welche man sich entscheidet: es ist unbedingt notwendig, diese Software regelmäßigen Updates zu unterziehen, denn Viren verändern sich beständig und schnell ist die Anti-Viren-Software nicht mehr auf dem neuesten Stand.
Firewalls sind meist in das Antivirenprogramm integriert. Eine Firewall schützt ein Gerät vor Angriffen und unberechtigten Zugriffen aus dem Internet. Die Firewall sollte niemals ausgeschaltet sein!

❷ *Betriebs- und Anwendersoftware aktualisieren*

Nicht nur die Anti-Viren-Software und die Firewall sollten regelmäßig aktualisiert werden. Auch Betriebs- und Anwendersoftware muss laufend auf den neuesten Stand gebracht werden, damit Viren nicht durch etwaige Sicherheitslücken eindringen können. Aber Vorsicht: Die Updates sollten nur von seriösen Quellen bezogen werden, denn Updates von gängiger Software (z. B. Adobe Flash, Adobe Reader) können von Schadsoftware verseucht sein.

❸ *Risiko-Webseiten meiden*

Ein hohes Risiko, das eigene Gerät mit Malware zu infizieren, besteht beim Besuch kostenloser Pornoseiten.[28] Aber auch Streaming-Portale – Seiten, die Filme zum direkten Ansehen im Browser bereitstellen – stehen im Verruf für Malware-Attacken genutzt zu werden.[29] Aber: Ein Großteil der Malware stammt von seriösen Seiten, die von Cyberkriminellen gehackt wurden.

❹ *Nachrichten / Daten kritisch prüfen*

Nachrichten und deren Anhänge sollten nur geöffnet werden, wenn der Absender bekannt und vertrauenswürdig ist, die Betreffzeile seriös klingt und die Nachricht erwartet wurde. Das ist wichtig, da auch die Möglichkeit besteht, dass die Rechner von Freunden/ Bekannten vorab infiziert wurden. Empfehlenswert ist es daher, die Anhänge vor dem Öffnen vom Antivirenprogramm auf Bedrohungen scannen zu lassen.

❺ *App-Berechtigungen kontrollieren*

Vor dem Installieren einer App kritisch prüfen, welche Berechtigungen sie zum Funktionieren wirklich benötigt: Warum verlangt z. B. eine Taschenlampen-App Zugriff auf Kontaktdaten? Bei iOS (Apple-Betriebssystem) können Berechtigungen einzeln abgelehnt werden. Hier gilt es jedoch zu beachten, dass die betreffende App ohne Zugriffsrechte möglicherweise nicht benutzt werden kann. Bei Android (Google-Betriebssystem) war das Ablehnen von Berechtigungen lange nicht möglich. Erst mit der neuen Version 6.0 des Android Betriebssystems hat sich dies geändert: der Nutzer kann nun bei einigen Berechtigungen selbst entscheiden, ob er den Zugriff darauf erteilt oder verweigert. Jedoch gilt dies nicht für alle Berechtigungen, so dass bei allzu datenhungrigen Apps die Suche nach alternativen nach wie vor sinnvoll ist.

❻ *Benutzerprofile*

Geräte sollten immer als normaler Nutzer und nicht als Administrator genutzt werden, denn letzterer ist mit weitreichenden Berechtigungen ausgestattet. Wird das Gerät mit Malware infiziert, kann der Schädling in der Administrator-Einstellung mit Berechtigung zur System-Konfiguration weitaus größeren Schaden anrichten.

❼ *Dateien regelmäßig sichern*

In regelmäßigen Abständen sollten von den wichtigsten Dateien Sicherungskopien auf externe Festplatten angefertigt werden. Im Fall eines massiven Schadsoftware-Befalls sind diese Daten nicht verloren.

❽ *Wachsam sein*

Nutzer sollten im Internet immer auf der Hut vor Malware sein und auf den gesunden Menschenverstand vertrauen: Meldungen, Nachrichten und Aufforderungen sollten nicht blind vertraut werden.

Erkennen von Schadprogrammen

Woran kann man ein von Schadprogrammen befallenes Gerät erkennen? Am Desktop-PC lässt sich das u. U. durch folgende Indikatoren feststellen:[30]

- Verringerte Computerleistung
- Hohe Prozessorauslastung
- Langsame Internetverbindung
- Programme starten/schließen sich automatisch
- Vermehrte Werbeeinblendungen

Bei mobilen Endgeräten ist ein Virenbefall, neben der Prüfung durch eine Antiviren-Software, u. U. auch anhand folgender Indikatoren feststellbar:[31]

- Langsame Internetverbindung, hoher Datenverbrauch
- Hohe Prozessorauslastung
- Hoher Energieverbrauch
- Überhöhte Telefonkostenabrechnung: Abo-Gebühren, teure Premium-Nummern etc.

Links und weiterführende Informationen

Webseiten

www.av-test.org/de/antivirus
Hier finden sich detaillierte Testberichte zu Antivirenprogrammen auf Desktop-PCs und mobilen Endgeräten.

www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/sicherheitskompass.html
Der Sicherheitskompass der Polizei beschäftigt sich mit den 10 häufigsten Sicherheitsrisiken.

www.bka-trojaner.de
Hier gibt es Hilfestellung zur Beseitigung diverser Ransomware.

http://praxistipps.chip.de/bin-ich-teil-eines-botnetzes-so-finden-sies-heraus_12330
Auf dieser Seite kann getestet werden, ob das eigene Gerät Teil eines Botnets ist.

www.lehrer-online.de/it-sicherheit.php
Hier finden sich Unterrichtseinheiten und Hintergrundinformationen rund um das Thema „IT-Sicherheit".

www.lehrer-online.de/viren-wuermer-trojaner.php
Hier gibt es Informationen und Unterrichtseinheiten zum Thema "Viren" und "Trojaner".

www.internauten.de/index.html?mission=Download/index.html
Auf dieser Seite findet sich ein Spiel zu Viren und Trojanern, das sich an jüngere Kinder richtet.

www.blinde-kuh.de/viren
Diese Seite bietet kindgerechte Informationen rund um das Thema „Viren".

Endnoten

[14] SPRINGER GABLER VERLAG (Hrsg.). (k.A.). *Gabler Wirtschaftslexikon, Stichwort: Malware.* Aufgerufen am 20.07.2015 unter http://wirtschaftslexikon.gabler.de/Archiv/1408508/malware-v4.html

[15] BRENTON, C. & Hunt, C. (2003). *Network Security. The Expertise You Need to Protect Your Network from Common Threats* (2. Auflage). Alameda, CA: Sybex.

[16] MILOŠEVIĆ, N. (k. A.). *History of malware*. [Blog] Aufgerufen am 19.11.2014 unter http://www.inspiratron.org/HistoryOfMalware.php

[17] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI). (2015). *Schadprogramme: Viren.* Aufgerufen am 20.07.2015 unter https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Schadprogramme/Viren/viren_node.html

[18] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI). (2015). *Schadprogramme: Würmer.* Aufgerufen am 20.07.2015 unter https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Schadprogramme/Wuermer/wuermer_node.html

[19] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI). (2015). *Schadprogramme: Trojaner.* Aufgerufen am 20.07.2015 unter https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Schadprogramme/TrojanischePferde/trojanischepferde_node.html

[20] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI). (2015). *Schadprogramme: Spyware.* Aufgerufen am 20.07.2015 unter https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Schadprogramme/Spyware/spyware_node.html

[21] PURSCHE, O. (2013, 05. Juni). Schadprogramme täuschen Virenbefall nur vor. *welt.de*. Aufgerufen am 19.11.2014 unter http://www.welt.de/wirtschaft/webwelt/article116828024/Schadprogramme-taeuschen-Virenbefall-nur-vor.html

[22] POLIZEI-PRAEVENTION.DE. (k. A.). *PC gesperrt? Ransomware.* Aufgerufen am 20.07.2015 unter http://www.polizei-praevention.de/themen-und-tipps/pc-gesperrt-ransomware.html

[23] NORTON. (2012). *2012 Norton Cybercrime Report*. Aufgerufen am 20.07.2015 unter http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

[24] MCCORMACK, C. (2011). *SOPHOS: Die vier Grundsätze für umfassenden Web-Schutz.* Aufgerufen am 21.07.2015 unter http://www.sophos.com/de-de/medialibrary/Gated%20Assets/white%20papers/sophos4rulescompletewebprotectionwpna.pdf?la=de-DE.pdf

[25] IHLENFELD, J. (2012, 20. Dezember). *Google warnt vor gehackten Webseiten.* golem.de. Aufgerufen am 19.07.2015 unter http://www.golem.de/1012/ 80227.html

[26] VILSBECK, C. (2014, 05. März). *Android ist Ziel von 97 % der mobilen Malware.* techchannel.de. Aufgerufen am 19.07.2015 unter http://www.tecchannel.de/kommunikation/news/2053774/android_ist_ziel_von_97_prozent_mobiler_malware/

[27] WINTERER, A. (2013, 07. Juli). *Viren-Attacken: Android-Smartphones in Gefahr?* [Blog-Beitrag]. Aufgerufen am 19.07.2015 unter http://blog.zdf.de/hyperland/2013/07/viren-attacken-android-smartphones-in-gefahr/

[28] SCHISCHKA, S. (2013, 18. April). *Gefährliche Malware auf kostenlosen Pornoseiten.* pcwelt. Aufgerufen am 19.07.2015 unter http://www.pcwelt.de/news/Gefaehrliche_Malware_auf_kostenlosen_Porno-Seiten-Gefahr_im_Web-7839179.html

[29] ZOLLONZ, A. (2013, 05. Juni). *Virus auf movie2k: Streaming-Plattform verbreitet Malware.* netzwelt.de. Aufgerufen am 20.07.2015 unter http://www.netzwelt.de/news/96091-virus-movie4k-streaming-plattform-verbreitet-malware.html

[30] ZELCH, B. (2013, 08. April). *Ist mein Computer infiziert? 5 Symptome bei einem Malware-Befall.* (Absatz 1-4). Aufgerufen am 07.12.2014 unter https://www.austrosec.at/2013/04/ist-mein-computer-infiziert-5-symptome-bei-einem-malware-befall/

[31] T-ONLINE. (2013, 19. November). *Ist Ihr Smartphone gehackt?* (Absatz 1–5). Aufgerufen am 07.07.2015 unter http://www.t-online.de/handy/smartphone/id_62854486/trojaner-test-ist-mein-smartphone-gehackt-.html

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Spam-Mails – wie schützt du dich?**	**Ein ganzer Zoo im Computer und auf dem Handy?**
Kompetenzen	Die Schülerinnen und Schüler erarbeiten die Möglichkeiten zum Schutz vor unerwünschten E-Mails (sogenannten Spam-Mails).	Die Schülerinnen und Schüler lernen verschiedene Formen von Schadsoftware kennen und können eine Übersicht anfertigen.
Methoden	Einzelarbeit, Partnerarbeit, Unterrichtsgespräch, Ergänzungs-Übung	Partnerinterview, Plakat, Experte (optional), Partnerarbeit, Einzelarbeit
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja (nur für das Video von Monty Python notwendig)	ja

Hinweise für die Durchführung

AB 1: Spam-Mails – wie schützt du dich?

Anhand dieses Arbeitsblattes sollen die Schülerinnen und Schüler die drei „goldenen" Regeln des E-Mailing kennen lernen und begründen können. Die Form des E-Mailing kann dabei gewählt werden, wenn die Möglichkeiten dazu bestehen, ansonsten lassen Sie die Begründung vielleicht einfach als zusammenhängenden Text schreiben.

Die Ergänzungen zu den Sätzen soll eine kleine Wissensabfrage zum E-Mailing sein, denn oft beherrschen Schülerinnen und Schüler das E-Mailing, wissen aber nichts mit CC oder BCC o. ä. anzufangen:

Mögliche Antworten:

- Der Betreff einer E-Mail ist wichtig, weil … der Empfänger daran sofort sehen kann, ob es eine Spam-Mail ist oder nicht, auch ohne sie zu öffnen.
- Wenn ich mehrere Empfänger habe, mache ich Folgendes … Ich schreibe sie in die Empfängerzeile, getrennt durch ein Komma (Dies kann von Programm zu Programm variieren).
- Das BCC beim E-Mailing steht für … Blind Carbon Copy, also eine „blinde" Kopie. Die anderen Empfänger der E-Mail können diesen BCC-Empfänger nicht sehen.
- Anhänge öffne ich nur von … Bekannten oder Freunden oder wenn ich weiß, von wem er stammt.
- Große Dateien über 10 MB verschicke ich nur, wenn … es unbedingt notwendig ist und ich beim Empfänger nachgefragt habe.
- Ich habe zwei E-Mail-Adressen, weil … ich eine private benutze für meine Freunde und Bekannten.
- Eine andere gebe ich öffentlich weiter. Die privaten E-Mail-Adressen bekommen nur … meine Freunde und Bekannten.
- Das mache ich mit blöden E-Mails … Ich lösche sie sofort oder ich markiere sie als SPAM.
- E-Mails von Unbekannten behandele ich so: Ich öffne nie Anhänge und bin vorsichtig mit dem Inhalt. Wenn mir etwas komisch vorkommt, lösche ich sie. Vor allem antworte ich nicht ohne weiteres.
- Auch in E-Mails bin ich höflich, weil … auf der anderen Seite keine Maschinen, sondern Menschen sitzen.

AB 2: Ein ganzer Zoo im Computer und auf dem Handy?

Die Auflistung möglicher Schädlinge für digitale Geräte ist didaktisch reduziert (s. Sachinformationen), bietet aber einen guten Einstieg in das Thema. Die Schülerinnen und Schüler sollen im ersten Arbeitsauftrag eine eigenständige Recherche auf den Seiten von klicksafe und dem Bundesamt für Sicherheit in der Informationstechnik – das sie auf diese Weise kennenlernen – vornehmen. Hier ist vielleicht etwas Hilfestellung und Vorarbeit notwendig, da diese Seiten sehr umfangreich sind und immer wieder aktualisiert werden.
Im zweiten Arbeitsauftrag sollen die Schülerinnen und Schüler nach der Informationsbeschaffung ihren Partner/ihre Partnerin informieren. Dies kann in Form eines „Partnerinterviews" geschehen: Als Synthese soll dann eine Seite mit den wichtigsten Informationen entstehen. Vielleicht besteht die Möglichkeit, auch andere Klassen über das Problem in Form eines Stationenlernens zu informieren.

Spam-Mails – wie schützt du dich?

„Spam-Mails sind eine wahre Plage, oder? Bestimmt hast du auch schon solche unerwünschten E-Mails bekommen. Der Name stammt wahrscheinlich von „SPiced hAM" (englisch für „gewürzter Schinken") was früher der Name eines Dosenfleischs war. Als Begriff für „massenhaft" und „unerwünscht" soll das Wort aus einem alten Fernsehsketch der Komikergruppe „Monty Python" stammen.
Du kannst dir den Spot hier anschauen: **http://bit.ly/19PeUMn**

Spam-Mails sind nicht nur lästig, sondern können auch gefährlich werden. Deshalb gibt es drei goldene Regeln des E-Mailing:

- niemals auf eine Spam-Mail reagieren
- den Spam-Filter „trainieren"
- die E-Mail-Adresse nicht überall angeben und immer eine zweite E-Mail-Adresse anlegen

Arbeitsaufträge:

1. Überlege, warum diese Regeln sinnvoll sind! Schreibe eine E-Mail an eine Freundin/einen Freund, in der du ihr/ihm diese Regeln erklärst. Wenn du keine Möglichkeit hast eine E-Mail zu schreiben, schreibe die Erklärung auf die Rückseite des Arbeitsblattes!

2. Aber es gibt noch weitere wichtige Dinge, die man beachten sollte. Hier findest du Hinweise, ergänze sie zu ganzen Sätzen:

Der Betreff einer E-Mail ist wichtig, weil …
Wenn ich mehrere Empfänger habe, mache ich folgendes …
Das BCC beim E-Mailing steht für …
Anhänge öffne ich nur von …
Große Dateien über 10 MB verschicke ich nur, wenn …
Ich habe zwei E-Mail-Adressen, weil …
Die privaten E-Mail-Adressen bekommen nur …
Das mache ich mit blöden E-Mails …
E-Mails von Unbekannten behandele ich so:
Auch in E-Mails bin ich höflich, weil …

Ein ganzer Zoo im Computer und auf dem Handy?

Ein wenig digitale Biologie?
Auf unserem Computer, Smartphone oder Tablet können sich zahllose Schädlinge tummeln.

Computerviren
Darunter sind solche Dinge gefasst wie Bootviren (dann startet der Computer erst gar nicht mehr), Makroviren (weit verbreitet in Office-Programmen), Datei-Viren (sie starten mit einem Programm), Polymorphe Viren (sie heißen so, weil sie sich gut verkleiden können und ständig verwandeln) und die Tarnkappen-Viren (die sich besonders gut verstecken können).

Rogueware
Rogueware ist besonders perfide: Diese Software gaukelt vor, andere Schadsoftware zu entfernen, tut aber das Gegenteil.

SpyApps
SpyApps zeichnen unbemerkt die Kommunikation auf, schalten Mikrofon und Kamera ein oder leiten den Standort des Handys weiter.

Scareware werden gefälschte Warnmeldungen u. ä. bezeichnet, die den Nutzer verunsichern und dazu verleiten sollen, andere Software zu installieren.

„Würmer"
Ein Wurm kann sich selbst vervielfältigen und automatisch Kopien verschicken. Er braucht auch kein anderes Programm (wie ein Virus), sondern arbeitet ganz selbstständig.

„Trojaner" – Trojanische Pferde
(Kennst du die Sage vom Trojanischen Pferd?) Ein Trojaner benutzt einen gemeinen Trick. Das Virus gibt vor, etwas anderes zu sein (z. B. ein Spiel oder nützliches Programm): Kaum hast du es aufgerufen, befällt es deinen Computer. In diesen Trojaner kann auch ein Spionageprogramm versteckt sein, das deinen Computer auskundschaftet (und deine Passwörter munter weiterleitet).

Hoaxes
Ein Hoax (zu Deutsch: „Jux", „Schabernack" oder „Schwindel") ist nichts anderes als eine Falschmeldung, die von Person zu Person verbreitet wird (z. B. via SMS, WhatsApp- oder Facebook-Nachricht). Ein Hoax besteht meist aus drei Elementen; einem Aufhänger, der Echtheit vermitteln soll, gefolgt von einer Aufklärung über die aus dem Internet drohende Gefahr und der abschließenden Bitte, diese Information an so viele Internetnutzer wie möglich weiterzuleiten. Echte Virus-Warnungen werden nie auf diese Weise verschickt.

Und wie kommen diese Viren, Würmer, Trojaner und Hoaxes auf deinen Computer und in dein Handy? Und wie kannst du dich davor schützen?

Arbeitsaufträge:

1. Informiere dich über das Problem auf den folgenden Seiten:

klicksafe: **www.klicksafe.de/themen/technische-schutzmassnahmen/den-pc-schuetzen/**
Bundesamt für Sicherheit in der Informationstechnik: **https://www.bsi-fuer-buerger.de/**

2. Wie sieht ein wirksamer Schutz aus? Erkläre es deiner Nachbarin/deinem Nachbarn und umgekehrt!

3. Erstelle eine Übersicht mit den wichtigsten Informationen über Viren und den Schutzmaßnahmen! Versuche doch bitte, Symbole und Bilder in deine Übersicht einzubringen.
Erstelle in einem Textbearbeitungsprogramm ein Merkblatt mit Symbolen!

Hoaxes, Kettenbriefe und Shitstorms

Hoaxes

„Hoax" kommt aus dem Englischen und bedeutet „Scherz", „Schabernack" oder auch „Schwindel". Als Hoax wird eine Falschmeldung bezeichnet, die über Soziale Netzwerke, wie bspw. Facebook, WhatsApp etc. schnell an viele Personen weitergeleitet wird.[1] Da der Inhalt der Hoaxes meist nicht völlig abwegig ist, ist es vor allem für Kinder und Jugendliche nicht immer einfach, sie als Falschmeldungen zu enttarnen. Meistens sind Hoaxes witzig bzw. nervig und harmlos. Immer wieder kommt es aber vor, dass über Hoaxes Viren eingeschleppt und Phishing-Attacken geschickt getarnt werden.

Hoaxes haben in der Regel einen reißerischen Inhalt: z. B. wird für einen Leukämiekranken dringend eine bestimmte Blutgruppe gesucht oder es wird gemeldet, dass Handys während des Aufladens explodierten und den Nutzer verletzen können, oder es wird entrüstet auf das traurige Schicksal der Bonsai-Katzen hingewiesen.[2]

Ein technischer Schutz ist angesichts des viralen Verbreitungsweges von Hoaxes nicht möglich. Umso wichtiger ist es daher, Kinder und Jugendliche über Hoaxes aufzuklären und sie so dazu zu befähigen, Falschmeldungen als solche zu erkennen.

Tipp: *Die Technische Universität Berlin führt eine Hoax-Liste, die ständig aktualisiert wird:*
http://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml

Kettenbrief

Kettenbriefe funktionieren nach dem Schneeballprinzip: Ein Empfänger erhält eine Nachricht mit einer mehr oder minder expliziten Aufforderung, diese an eine Mindestanzahl von Freunden und Bekannten weiterzuschicken.[3] Diese leiten sie dann wiederum an ihre Kontakte weiter. So verbreitet sich ein Kettenbrief innerhalb kürzester Zeit an eine große Personenzahl.

In einigen Kettenbriefen wird dem Empfänger mit Unglück, Tod etc. gedroht, wenn er die Nachricht nicht weitersendet. Andere Kettenbriefe versprechen dem Nutzer Glück, Geld etc., sollte die Nachricht weitergeleitet werden. Wieder andere setzen den Nutzer unter moralischen Druck. Gerade für junge Nutzer ist nicht immer erkenntlich, dass es sich bei dem Inhalt eines Kettenbriefes um einen (schlechten) Scherz handelt: Ende 2013 kursierte in WhatsApp eine Sprachnachricht, in der eine Computerstimme damit drohte, den Empfänger und dessen Mutter umzubringen, wenn die Nachricht nicht an mind. 20 weitere Personen weitergeleitet wird. Viele Kinder fühlten sich durch die Botschaft bedroht und wandten sich daraufhin an Eltern, Lehrer und Polizei.[4]

Eine neuere Entwicklung im Bereich der Kettenbriefe ist die Nominierung einer Person mittels WhatsApp oder Facebook, sich einer bestimmten Herausforderung zu stellen: Im Sommer des Jahres 2014 kursierte in den Sozialen Medien die sog. **ALS Ice Bucket Challenge**, an der selbst Prominente aus Politik, Sport, Gesellschaft etc. teilnahmen. Der Nominierte hatte die Aufgabe, sich einen Kübel eiskaltes Wasser über den Kopf zu schütten und dann drei weitere Personen zu nominieren, dies ebenfalls zu tun. Die Aktion sollte zudem gefilmt und das Video als Beweis im Internet bereitgestellt werden. In die Welt gesetzt wurde die **Ice Bucket Challenge** für den Zweck, auf die seltene Krankheit **Amyotrophe Lateralsklerose** (ALS) hinzuweisen. Ursprünglich war angedacht, dass sich nur diejenigen Personen der Ice Bucket Challenge unterziehen sollten, die nicht bereit waren für den guten Zweck zu spenden. Mit zunehmender Popularität der Challenge beteiligten sich viele Personen nicht nur mit einer Eiswasserdusche, sondern auch an der Spende.[5]

Bedenklich werden derartige Kettenbriefe bzw. Challenges vor allem dann, wenn zu riskanten Aktionen aufgerufen wird. Dies ist aber nicht immer der Fall: In den Sozialen Netzwerken lässt sich aktuell noch eine weitere Form des Kettenbriefes identifizieren: Nutzer nominieren zwei Freunde oder Bekannte, die dann ihre 10 Lieblingsbücher, -songs etc. angeben müssen. Diese nominieren dann wiederum je zwei Personen etc.

INFO: *Bekannterweise werden nicht nur schadhafte Inhalte in viraler Form über das Internet verbreitet. Eine neue, durch das Internet entstandene Sonderform der Kommunikation sind sog.* ***Memes****. Dabei handelt es sich um Bilder und kurze Videos, die vielfach verbreitet und dabei z. B. kopiert, erweitert, neu betitelt oder fast komplett verändert werden. Doch so schnell wie die einzelnen Memes aufgetaucht sind, so schnell sind sie meist auch wieder verschwunden. Dennoch entwickeln sich auf diese Weise interessante Dynamiken bezüglich dessen, worüber gesprochen wird und was gerade von allgemeinem Interesse ist. Einen kurzen Überblick über die Entstehung und Bedeutung von Memes findet sich hier:*
www.thegap.at/rubriken/stories/artikel/wie-das-meme-zum-meme-wurde/

Shit- und Candystorm

„Shitstorm" ist eine neudeutsche Wortschöpfung, im Englischen ist stattdessen der Begriff **„Online-Firestorm"** gebräuchlich. Ein Shitstorm ist eine Empörungswelle in Form von massenhafter Schmähkritik gegen eine Person oder eine Sache via Soziale Netzwerke, Messenger etc. Nach Sascha Lobo, einem bekannten deutschen Blogger, ist ein Shitstorm ein „Prozess, wo in einem kurzen Zeitraum eine subjektiv große Anzahl von kritischen Äußerungen getätigt wird, von denen sich zumindest ein Teil vom ursprünglichen Thema ablöst und stattdessen aggressiv, beleidigend, bedrohend oder anders attackierend geführt wird"[6]. Die Dynamik, die ein solcher Shitstorm entfalten kann – wie viele Nutzer sich daran beteiligen und ob, bzw. wie er medial aufgegriffen wird – ist kaum abzuschätzen.

Ein Shitstorm kann begründet oder unbegründet sein, kann Einzelpersonen oder Unternehmen, Verbände, Parteien etc. betreffen. Für eine Einzelperson kann ein Shitstorm – gleich ob begründet oder unbegründet – schlimme psychische Folgen haben (siehe **Kapitel 6_1 Cyber-Mobbing**). Für ein Unternehmen, einen Verband oder eine Partei, die sich einem Shitstorm ausgesetzt sehen, besteht die begründete Befürchtung eines Image-Verlustes mit den damit verbundenen negativen Auswirkungen auf Verkaufs- bzw. Mitgliederzahlen:

- Die Firma Henkel sah sich 2011 massiven Anfeindungen im Netz gegenüber: Sie hatte zu einem Designwettbewerb für das Pril-Etikett im Rahmen einer limitierten Edition aufgerufen, aber nicht mit den absurden Vorschlägen gerechnet, die von den Online-Nutzern eingingen. Als Henkel die Gewinnerliste bereinigte, kam es zum Shitstorm.[7]

- Der Deutsche Fußballbund veröffentlichte via Twitter anlässlich des 100. Länderspielsieges ein Foto zweier deutscher Fußballspieler aus dem Jahr 1942, auf deren Trikots ein Hakenkreuz zu sehen war. Der DFB sah sich genötigt, das Bild nach einem Shitstorm wieder zu löschen.[8]

- Die Partei Bündnis 90/Die Grünen erlebten vor der Bundestagswahl 2013 einen Shitstorm. Die Partei hatte sich für die Einführung eines sogenannten Veggie-Tages ausgesprochen. An einem Tag in der Woche sollten Kantinen nur fleischlose Kost anbieten. Die Grünen wurden daraufhin u. a. als Ökofaschisten bezeichnet.[9]

Problematisch an den Shitstorms ist u. a. auch, dass potenziell die Möglichkeit besteht, diese bewusst loszutreten und zu befeuern – bspw. durch gefälschte Posts etc. – um Konkurrenten zu schaden.

Nicht immer besteht diese Art von Massenphänomen aus negativer Kritik. Es gibt sie auch unter umgekehrtem Vorzeichen: Der Adressat wird dann mit positivem Zuspruch überhäuft.[10] Diese Form wird als **„Candystorm"** bezeichnet. Geprägt wurde dieser Begriff von Twitter-Nutzern und Grünen-Mitgliedern, die dem Aufruf von Volker Beck (Die Grünen) folgend dessen Kollegin Claudia Roth dazu ermunterten, weiterhin Parteivorsitzende zu bleiben. Neben Claudia Roth kamen bislang einige Politiker, Prominente und Unternehmen in einen Candystorm.

Shit- und Candystorms können ein enormes Machtpotenzial entfalten: Unternehmen, politische Entscheidungsträger, Einzelpersonen etc. können nicht sicher davon ausgehen, dass (vermeintliches) Fehlverhalten unbemerkt und ungestraft bleibt. Auf der einen Seite können Shit- und Candystorms daher als Korrektiv zum Aufzeigen und Anprangern von Missständen fungieren. Auf der anderen Seite ist klarzustellen, dass ein Shit- bzw. ein Candystorm keine Mehrheitsmeinung abbilden, emotional geführt werden und daher unter Umständen die Möglichkeit für eine konstruktive Auseinandersetzung verbauen.

Links und weiterführende Informationen

Webseiten

http://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml
Die Technische Universität Berlin führt eine Hoax-Liste, die ständig aktualisiert wird.

http://www.feinheit.ch/media/medialibrary/2012/04/shitstorm-skala_2.pdf
Shitstorm – Skala, die von der Social Media Expertin Barbara Schwede und Daniel Graf entwickelt wurde.

www.fr-online.de/digital/claudia-roth-und-der-candystorm,1472406,20860688.html
Ein Artikel zum neuen Phänomen „Candystorm".

Endnoten

[1] TERNIEDEN, H. (2009, 17. Dezember). *Jahrzehnt des Hoaxing: Unglaublich, aber falsch.* spiegel.de. Aufgerufen am 10.07.2015 unter http://www.spiegel.de/panorama/gesellschaft/jahrzehnt-des-hoaxing-unglaublich-aber-falsch-a-666310.html

[2] ZIEMANN, F. (2014, 10. November). *TU Berlin: Hoax-Liste*. Aufgerufen am 07.07.2015 unter http://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml

[3] ZIEMANN, F. (2014, 19. November). *TU Berlin: Hoax-Info Service*. Aufgerufen am 07.07.2015 unter http://hoax-info.tubit.tu-berlin.de/hoax/#8

[4] MILDE, S. (2015, 10. Januar). *WhatsApp: Vorsicht vor diesen Kettenbriefen.* chip.de. Aufgerufen am 07.07.2015 unter http://praxistipps.chip.de/whatsapp-vorsicht-vor-diesen-kettenbriefen_37162

[5] SUEDDEUTSCHE.DE. (2014, 25. August). *Was Sie über das Phänomen Eiskübel wissen müssen*. Aufgerufen am 03.07.2015 unter http://www.sueddeutsche.de/panorama/ice-bucket-challenge-was-sie-ueber-das-phaenomen-eiskuebel-wissen-muessen-1.2102571

[6] LOBO, S. (2010, 21. April). *How to survive a shitstorm* [Video]. Aufgerufen am 02.12.2014 unter https://www.youtube.com/watch?v=-OzJdA-JY84

[7] BREITHUT, J.(2011, 20. Mai). *Soziale Netzwerke: Pril-Wettbewerb endet im PR-Debakel.* spiegel.de. Aufgerufen am 10.07.2015 unter http://www.spiegel.de/netzwelt/netzpolitik/soziale-netzwerke-pril-wettbewerb-endet-im-pr-debakel-a-763808.html

[8] GLINDMEIER, M. (2014, 22. November). *Tweet zeigt Siegbild von 1942: DFB blamiert sich mit dem Foto aus Nazi-Zeit.* spiegel.de. Aufgerufen am 10.07.2015 unter http://www.spiegel.de/sport/fussball/dfb-twittert-nazi-bild-von-1942-a-1004449.html

[9] VON BOEHN, V. H. (2013, 05. August). *Gründe Pläne für Vegetarier-tag lösen Shitstorm aus.* derwesten.de. Aufgerufen am 06.07.2015 unter http://www.derwesten.de/politik/gruene-plaene-fuer-vegetarier-tag-loesen-shitstorm-aus-id8278629.html

[10] TAGESSPIEGEL.DE. (2012, 12. November). *Candystorm statt Shitstorm auf Twitter*. Aufgerufen am 10.07.2015 unter http://www.tagesspiegel.de/politik/gruenen-chefin-claudia-roth-candystorm-statt-shitstorm-auf-twitter/7376754.html

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Falschmeldungen – nicht immer harmlos**	**Shitstorm**
Kompetenzen	Die Schülerinnen und Schüler erkennen die Strukturmerkmale von Falschmeldungen, die als „Hoaxes" bekannt sind.	Die Schülerinnen und Schüler erkennen Merkmale des Internet-Phänomens „Shitstorm" und Möglichkeiten der Bewertung. Sie beurteilen die Legitimität solcher Aktionen.
Methoden	Gruppenarbeit, versch. Präsentationsmöglichkeiten	Gruppenarbeit, Internet-Recherche, Mind-Map
Material	Arbeitsblatt (je nach Präsentationsform versch. Materialien wie Papier, Stifte, Kleber)	Arbeitsblatt, (evtl. großes Papier für große Mind-Map)
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Falschmeldungen – nicht immer harmlos	Hoaxes laden für den aufgeklärten Betrachter oft zum Schmunzeln ein, trotzdem darf man ihre Bedeutung nicht unterschätzen. Die Schülerinnen und Schüler sollen hier einige der modernen Sagen („urban legends") aus dem Internet unter dem Begriff der „Hoaxes" kennenlernen und sich mithilfe der Internet-Adresse der Technischen Universität Berlin über den aktuellen Stand informieren. Hier könnten Sie eine Phase einbauen, in der die Schülerinnen und Schüler über ihre eigenen Erfahrungen berichten, aber auch über ihre Ängste sprechen können. Gerade jüngere Schülerinnen/Schüler können von bspw. Gewaltandrohung sehr verängstigt sein. Wie immer bei diesen Themen gilt es, sensibel zu reagieren. Mit dem letzten Arbeitsauftrag sollen die Schülerinnen und Schüler ihre Erkenntnisse kreativ umsetzen und damit das Gelernte festigen.
AB 2: Shitstorm	Sascha Lobo bezeichnet sich selbst als Autor, Blogger, Microblogger und Strategieberater und ist vielfach in den Neuen (wie auch in den alten) Medien präsent. Seine Definition eines Shitstorms ist nicht wissenschaftlich, kennzeichnet aber trotzdem sehr anschaulich das Phänomen. Auf der Grundlage der Beaufort-Skala zur Einteilung von Windstärken (die den Erdkunde-Kolleginnen und -Kollegen geläufig sein dürfte) versuchen Schwede und Graf eine Einteilung der Shitstorms. Hier dürfen Sie sehr leistungsstarke Schülerinnen und Schüler gerne zum kritischen Hinterfragen einer solchen Einteilung auffordern. Sie soll dazu dienen, den Shitstorm nicht pauschal zu verurteilen, sondern auch qualitativ zu bewerten. In der Mindmap sollen die Schülerinnen und Schüler ihre Erkenntnisse darstellen und sie sich gegenseitig präsentieren. Im letzten Arbeitsauftrag gehen die Schülerinnen und Schüler noch einen Schritt weiter mit der Frage, ob ein Shitstorm nicht auch positive Seiten haben kann, zum Beispiel als demokratisches Instrument der Meinungsäußerung. **Quellen** Definition: Lobo, S. (2012, 21. April). *How to survive a shitstorm* [Video]. Aufgerufen am 02.12.2014 unter **https://www.youtube.com/watch?v=-OzJdA-JY84** **Bildquelle:** „Sascha Lobo" von Matthias Bauer (flickr: Matthias Bauer) - originally posted to Flickr as Sascha Lobo. Lizenziert unter CC BY-SA 2.0 über Wikimedia Commons - **https://commons.wikimedia.org/wiki/File:Sascha_Lobo.jpg#/media/File:Sascha_Lobo.jpg**

Lust auf mehr?
Moderne Mythen oder urban legends sind ein schier unerschöpfliches Thema, das sich im Internet kongenial unterbringen lässt. Dazu gehören ganze Gebilde von Verschwörungstheorien, die früher in Büchern und Zeitschriften nur ein kleines Publikum fanden, nun aber weltweit ausgebreitet werden. Für historisch interessierte Schülerinnen und Schüler könnte als Beispiel hier die These von der „Nicht-Mondlandung" der Amerikaner kritisch hinterfragt werden.

Falschmeldungen – nicht immer harmlos

Hoaxes nennen Experten die vielen Falschmeldungen, die im Internet kursieren. Beliebte Hoaxes sind u. a.:

- Personen mit bestimmte Blutgruppe für einen Leukämie-Kranken gesucht
- Vorsicht! Handy explodiert beim Aufladen!
- Spritzen-Nadeln von HIV-Infizierten im Kinositz versteckt!
- Die Flugnummer Q33NY einer der Maschinen, die am 11.09.2011 ins World Trade Center flog, ergibt in der Schriftart **Wingdings** folgende Botschaft:

Q33NY

▽

Wingdings

▽

Quelle: The Museum of Hoaxes (www.hoaxes.org)

Die meisten Hoaxes sind schlicht witzig oder nervig. Einige jedoch spielen ganz bewusst mit Emotionen wie der Angst vor Tod oder Krankheit, Rachegefühlen etc. Unter folgender Adresse kannst du eine ständig aktualisierte Liste von Hoaxes finden, die von der Technischen Universität Berlin betreut wird:
http://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml

Arbeitsaufträge:

1. Teilt euch in 4er-Gruppen auf. Zwei von euch informieren sich über Hoaxes allgemein. Die anderen beiden informieren sich über Kettenbriefe, die per E-Mail, über Soziale Netzwerke oder Messenger-Apps verschickt werden. Sucht jeweils 2–3 Beispiele heraus, die ihr besonders interessant findet.

2. Tauscht euch in der Gruppe aus und stellt euch die Ergebnisse gegenseitig vor!

3. Denkt gemeinsam darüber nach, warum diese Hoaxes und Kettenbriefe in Umlauf gebracht werden und welche Folgen sie haben können.

4. Überlegt und recherchiert, wie man sich schützen kann! Erstellt Tipps zum Schutz für jüngere SchülerInnen. Ihr dürft eine der folgenden Präsentationsformen wählen:

   A einen Aufkleber
   B max. zehn einfache Sätze
   C ein Symbol / Piktogramm
   D ein Werbeplakat
   E einen Reim / ein Gedicht
   F ein Maus-Pad

Shitstorm

„Als Shitstorm wird ein Internet-Phänomen bezeichnet, bei dem innerhalb eines kurzen Zeitraums eine subjektiv große Anzahl kritischer Äußerungen getätigt wird, von denen sich zumindest ein Teil vom ursprünglichen Thema entfernt und stattdessen aggressiv, beleidigend oder bedrohend sind“

(nach Sascha Lobo, 2012).

Foto: Matthias Bauer

Die Wissenschaftler Barbara Schwede und Daniel Graf versuchten gar eine Skala zu beschreiben für die Stärke eines Shitstorms: Von 0 (keine kritischen Rückmeldungen) über 4 (Herausbildung einer vernetzten Protestgruppe. Wachsendes, aktives Follower-Publikum auf allen Kanälen) bis Stufe 6 (ungebremster Schneeball-Effekt mit aufgepeitschtem Publikum. Tonfall mehrheitlich aggressiv, beleidigend, bedrohend.).

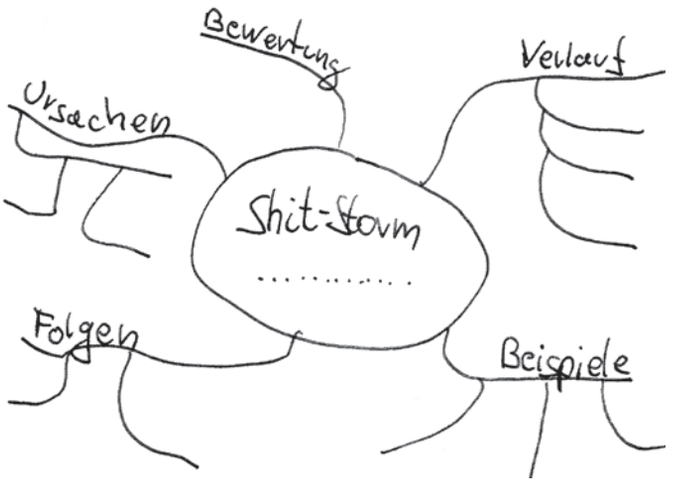
Arbeitsaufträge:

1. Informiert euch über einen Shitstorm aus dem vergangenen Jahr. Versucht herauszufinden, warum und wie er entstanden ist, wie er verlaufen ist was die Folgen waren. Versucht, den ausgewählten Shitstorm in der Skala von Schwede und Graf zu verorten. Diese ist zu finden unter

   http://www.barbaraschwede.ch/blog.html bzw.

   http://tinyurl.com/038ug8g

2. Stellt eure Ergebnisse in Form einer Mind-Map dar:



3. Shitstorms können auf der einen Seite für Einzelpersonen, Unternehmen, Verbände etc. problematisch sein und sie schädigen. Auf der anderen Seite können Shitstorms durch ihr Machtpotenzial auf Missstände hinweisen und sogar darauf hinwirken, diese zu beheben. Diskutiert diese zwei Seiten eines Shitstorms in der Klasse. Versucht, Regeln aufzustellen, wann ein Shitstorm in Ordnung wäre.

Illegale Downloads und Tauschbörsen

Illegale Downloads

Rechtslage

Aktuelle Blockbuster noch vor dem offiziellen Kinostart sehen, die neuste CD der angesagten Band herunterladen, benötigte Software aus dem Internet ziehen? Das ist mit ein wenig technischem Know-how nicht weiter schwer. Viele Personen laden illegal hochgeladene Daten aus ominösen Internetquellen auf den eigenen Computer herunter. In Deutschland laden laut einer gemeinsamen Studie des **Bundesverbands der Musikindustrie** (BVMI), des **Börsenvereins des deutschen Buchhandels** und der **Gesellschaft zur Verfolgung von Urheberrechtsverletzungen** (GVU) 3,7 % der Nutzer illegal Medieninhalte herunter.[1] Am häufigsten werden einzelne Musiktitel heruntergeladen, dicht gefolgt von Spiel- und Kinofilmen, Musikalben und TV-Serien.[2]

Wer Medieninhalte hochlädt, ohne deren Urheber zu sein, macht sich nach dem Urheberrecht strafbar, denn das Recht ein Werk zu vervielfältigen und zu verbreiten liegt alleine bei diesem selbst. Dies ist im Urheberrechtsgesetz (UrhG) Abs. 4, § 16 und § 17 geregelt. Auf einen Verstoß gegen das Urheberrecht können empfindliche Geldstrafen fällig werden (siehe **Kapitel 5_2 Urheberrecht und Open Content**). Das Herunterladen der Mediendaten ist grundsätzlich erlaubt, wenn die Kopien ausschließlich zu privaten Zwecken genutzt werden. Voraussetzung dafür aber ist, dass die Kopien nicht aus „offensichtlich rechtswidrigen" Quellen stammen dürfen.[3] User, die dabei ertappt werden, illegal Mediendateien hochzuladen bzw. aus dem Internet herunterzuladen, werden von beauftragten Anwaltskanzleien dazu aufgefordert, eine Unterlassungserklärung abzugeben und Schadenersatz zu zahlen. Die dabei verlangte Schadenersatzsumme ist meist sehr hoch angesetzt und teilweise auch scheinbar überzogen, um mögliche Folgetäter abzuschrecken.

Gefahren

Problematisch sind die Quellen zum illegalen Download nicht nur aus urheberrechtlicher Sicht: Über diese Portale sind auch Inhalte zugänglich, die bspw. in Deutschland bestimmten Altersgruppen eigentlich nicht zur Verfügung stehen dürfen. Darunter fallen bspw. gewalthaltige Filme oder solche mit pornographischen Inhalten. Jugendschutzrechtliche Bestimmungen und somit der Schutz von Kindern und Jugendlichen vor solchen Inhalten, werden auf diese Weise untergraben (vgl. **Kapitel 5_1 Jugendmedienschutz**).

Neben Jugendschutzrechtsverletzungen bergen illegale Downloadportale darüber hinaus die Gefahr, die Geräte der Nutzer mit Schadsoftware und Werbeprogrammen zu infizieren.

***Tipp:** Es ist wichtig, SchülerInnen frühzeitig für die Urheberrechts-Thematik zu sensibilisieren und mit ihnen den Wert von Filmen, Musikclips etc. zu diskutieren.*

Illegale Tauschbörsen

Filesharing

In den Medien ist häufig von Tauschbörsen die Rede. Gemeint sind damit sog. „Filesharing"-Systeme. **Filesharing** bezeichnet die Weitergabe oder den Tausch (engl. „sharing") von Dateien (engl. „files") zwischen Internetnutzern (engl. „**Peer-to-Peer**" bzw. „**P2P**"). Für das Filesharing ist bestimmte Software erforderlich, die zuerst auf dem Rechner herunter geladen werden muss. Mittels der Software ist es dann möglich, nach einer bestimmten Mediendatei zu suchen.[4] Bei einer Suchanfrage werden diejenigen Nutzer angezeigt, welche die Mediendateien zum Download bereitstellen. Da die übertragenen Dateien häufig groß sind und damit den Download verlangsamen, werden einzelne Datenpakete von verschiedenen Anbietern heruntergeladen. Häufig wird der Nutzer, der die Dateien auf seinen Rechner lädt, bereits selbst als Anbieter der besagten Mediendatei gelistet (z. B. bei **BitTorrent**).[5] Daneben kann jeder Nutzer auch ganz gezielt eigene Dateien zum Download anbieten.

Filesharing ist nicht grundsätzlich illegal. Urheberrechte werden nur verletzt, wenn ein Nutzer Mediendateien hochlädt, deren Urheber er nicht ist oder an denen er keine entsprechenden Rechte besitzt (s. o.). Stellt ein Nutzer einen Link zum Download auf eine geschützte Datei online, begeht er somit eine Urheberrechtsverletzung.

Share- oder Filehoster

Während beim Filesharing Mediendateien von anderen Nutzern heruntergeladen werden, erfolgt der Download in anderen Fällen über sog. „**Sharehoster**" bzw. **„Filehoster"** – also über die Server eines Diensteanbieters wie z. B. **RapidShare, Megaupload**. Eine Anmeldung, um den Dienst nutzen zu können, ist hier nicht erforderlich: Jeder Nutzer kann auf die Webseite des Diensteanbieters zugreifen und Dateien hoch- bzw. herunterladen. Auch hier gilt: Sharehoster sind nicht per se illegal. Allerdings wird diese Infrastruktur auch dazu verwendet, urheberrechtlich geschützte Mediendateien zu verbreiten.[6]

Streaming

Unter „**Streaming**" wird das Abspielen von Filmen im Browser verstanden – der Film wird dabei nicht heruntergeladen. Es gibt seriöse Anbieter, die das Streaming gegen eine monatliche Gebühr ermöglichen, wie z. B. **Watchever** oder **Amazon Prime**. Abseits dieser seriösen Anbieter bewegt sich das Streaming in einer rechtlichen Grauzone.[7] Der Europäische Gerichtshof entschied in seinem Urteil von 2014, dass das Zwischenspeichern von Filmen – wie es beim Abspielen im Browser der Fall ist – keine Urheberrechtsverletzung darstellt.[8] Die Anbieter der einschlägigen illegalen Downloadquellen (z. B. **kinox.to**, **video2k** oder **Movie2k)** hingegen begehen klar eine Urheberrechtsverletzung und können dafür belangt werden. Spektakulär war der Fall der Webseite **kino.to**, dessen Betreiber verhaftet und später verurteilt wurde.[9] Die Seite wurde im Juni 2011 zwar vom Netz genommen, allerdings erschien nur einige Wochen später ihr Nachfolger **kinox.to**. Durch die sich ständig ändernden technischen Möglichkeiten des Internets ist jedoch nicht klar, wie sich die Rechtslage hier weiter entwickeln wird.

Links und weiterführende Informationen

Webseiten

www.klicksafe.de/service/fuer-lehrende/zusatzmodule-zum-lehrerhandbuch/#c1519
Das klicksafe-Zusatzmodul *Nicht alles, was geht, ist auch erlaubt* bietet umfassende Information zum Thema „Urheberrecht" sowie Unterrichtsmaterialien.

www.klicksafe.de/service/materialien/broschueren-ratgeber/nicht-alles-was-geht-ist-auch-erlaubt-urheber-und-persoenlichkeitsrechte-im-internet/
Die Broschüre ist zusammen mit iRights entstanden und beschäftigt sich mit Urheber- und Persönlichkeitsrechten im Internet.

www.klicksafe.de/themen/rechtsfragen-im-netz/
Auf klicksafe.de finden sich umfassende Informationen zu Rechtsfragen im Netz.

http://irights.info/
Auf dieser Seite finden Sie umfassende Informationen zu Rechtsfragen im Netz.

http://internet-abc.de/kinder/wwg-musik-autor-urheber-recht.php
Hier finden sich kindgerechte Erläuterungen rund um das Thema „Urheberrecht".

Endnoten

[1] GESELLSCHAFT FÜR KONSUMFORSCHUNG (GfK). (2013). *Studie zur digitalen Content-Nutzung (DCN-Studie) 2013* [PowerPoint Präsentation]. Aufgerufen am 21.07.2015 unter http://www.gvu.de/wp-content/uploads/2015/08/DCN_Studie-2013.pdf

[2] STATISTA. (2014). *Anzahl von illegalen Mediendownloads aus dem Internet im Jahr 2010*. Aufgerufen am 21.07.2015 unter http://de.statista.com/statistik/daten/studie/200320/umfrage/illegale-downloads-von-medieninhalten/

[3] VERBRAUCHERZENTRALE NIEDERSACHSEN. (k. A.). *Urheberrechtsverletzungen und ihre Folgen*. (Absatz 4). Aufgerufen am 11.08.2015 unter http://www.verbraucherzentrale-niedersachsen.de/internet-urheberrechtsverletzung-und-seine-folgen

[4] KLICKSAFE. (k. A.). *Was sind Tauschbörsen? Was ist Filesharing?* Aufgerufen am 07.07.2015 unter http://www.klicksafe.de/themen/rechtsfragen-im-netz/tauschboersen/p2p-filesharing-tauschboersen-was-ist-das/

[5] KLICKSAFE & IRIGHTS. (2014). *Nicht alles, was geht, ist auch erlaubt! Urheber- und Persönlichkeitsrechte im Internet.* Aufgerufen am 07.07.2015 unter http://www.klicksafe.de/service/materialien/broschueren-ratgeber/nicht-alles-was-geht-ist-auch-erlaubt-urheber-und-persoenlichkeitsrechte-im-internet/

[6] MÖLLEKEN, J. (2010, 14. September). *Filehoster: Hehler oder Helfer?* spiegel.de. Aufgerufen am 10.07.2015 unter http://www.spiegel.de/netzwelt/web/filehoster-hehler-oder-helfer-a-717333.html

[7] PLÖGER, S. (2014, 09. Oktober). *So gefährlich sind die illegalen Download-Portale.* welt.de. Aufgerufen am 11.07.2015 unter http://www.welt.de/wirtschaft/webwelt/article133101871/So-gefaehrlich-sind-die-illegalen-Download-Portale.html

[8] FOCUS.DE. (2014, 11. Juni). *Endgültiges Aus für Redtube-Abmahner? EU-Gericht erklärt Streaming für legal.* Aufgerufen am 20.07.2015 unter http://www.focus.de/digital/internet/endgueltiges-aus-fuer-redtube-abmahner-europaeischer-gerichtshof-streaming-ist-keine-urheberrechtsverletzung_id_3912287.html

[9] REIßMANN, O. (2011, 08. Juni). *Kino.to: Ermittler verhaften Betreibern mutmaßliche Betreiber von Raubkopie-Seite.* spiegel.de. Aufgerufen am 20.07.2015 unter http://www.spiegel.de/netzwelt/netzpolitik/kino-to-ermittler-verhaften-mutmassliche-betreiber-von-raubkopie-seite-a-767375.html

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Musik aus dem Internet?**	**Up- und Downloads – Was ist legal, was illegal?**
Kompetenzen	Die Schülerinnen und Schüler leiten Möglichkeiten für den legalen und gleichzeitig kostenlosen Musik-Download ab.	Die Schülerinnen und Schüler erkennen den Unterschied verschiedener Nutzungsformen von Up- und Downloads urheberrechtlich geschützter Materialien.
Methoden	Internet-Recherche, Tabelle, Unterrichtsgespräch, Einzelarbeit, Partnerarbeit	Internetrecherche, Gruppenarbeit, Kurzreferat, Präsentation als „Verkehrsschild“
Material	Arbeitsblatt	Arbeitsblatt, großes Papier, dicke Stifte.
Zeit (in Minuten)	90	135
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Musik aus dem Internet?

Verständlicherweise ist es die Regel, dass Musikrechteinhaber Geld verdienen wollen, und die allermeisten kostenlosen Angebote sind illegal. Aber es gibt eben auch Ausnahmen wie die Lizenz „Creative Commons“ oder vereinzelte Angebote. Die „Kindermusikbox“ ist so ein Angebot und soll hier als Beispiel dienen. Die Schülerinnen und Schüler sollen über das Problem reden, das bei kostenloser Musik aus dem Internet entstehen kann. Danach sollen sie in die Rolle des Künstlers/der Künstlerin schlüpfen und ihre Sicht der Dinge (Vor- und Nachteile) mit der eigenen Einstellung vergleichen (ebenfalls Vor- und Nachteile). Zum Schluss sollen sie lernen, genau auf eine Webseite zu schauen und das „Kleingedruckte“ zu lesen. Auf der Seite **www.kindermusikbox.de** unter **www.kindermusikbox.de/Lizenzbedingungen/** zu finden

Die Tabelle könnte so aussehen:

Für den Künstler/die Künstlerin		**Für dich**	
Vorteile	**Nachteile**	**Vorteile**	**Nachteile**
Viele hören die Musik	Sie verdienen kein Geld	Die Musik ist kostenlos	Die Qualität ist vielleicht nicht gut
Es ist billig herzustellen	Sie haben keine Kontrolle, wo die Musik auftaucht	Ich komme schnell an die Musik	Es ist vielleicht verboten
Sie brauchen keinen Plattenvertrag	Sie werden nicht berühmt	Ich kann sie vorher anhören	Ich bekomme keine CD

Außerdem sollen die Schülerinnen und Schüler verschiedene kostenlose (genauer gesagt für Deutschland GEMA-freie) Angebote zum Musik-Download kennenlernen.
Im vierten Arbeitsauftrag sollen die Schülerinnen und Schüler sich darüber informieren, welche legalen Möglichkeiten es gibt, an Musik zu gelangen. Dies sind:
- über Musikportale gegen Bezahlung
- als Download aus freien Quellen, so unter bestimmten Lizenzen und
- als Aufnahmen aus dem Radio (auch dem Internetradio)

Das Problem ist – wie oben beschrieben – dass es nicht immer einfach ist, zu sehen, ob die Quelle legal ist oder nicht. Deshalb ist es sicher von Vorteil, auf bekannten, seriösen Webseiten zu bleiben.

Aus diesem Grunde auch nochmals der ausdrückliche Hinweis auf den Mitschnitt von Musik aus dem Radio, wobei es keine Rolle spielt, ob die Technik zur Übertragung UKW, DAB oder Internet-Streaming heißt.

Hinweise für die Durchführung

AB 2: Up- und Downloads – Was ist legal, was illegal?

Die Schüler recherchieren über die beiden Nutzungsszenarien „zum Download bereitstellen" und „selbst downloaden". Sie können urheberrechtliche Probleme erkennen und denken über den legalen und illegalen Einsatz der unterschiedlichen Dienstleistungen sowie deren technisch-funktionale Unterschiede (Vergleich Tauschbörse – Filehoster) nach.
Mit dem ersten kurzen Austausch soll der Kenntnisstand (und vielleicht die Meinung) in der Lerngruppe ermittelt werden. Oft ist in diesem Bereich das Unrechtsbewusstsein bei Jugendlichen nicht sehr ausgeprägt, es existiert aber eine diffuse Vorstellung davon, dass es z. B. nicht rechtens ist, Musik weiterzugeben. Vielleicht greift an der Stelle schon die bisherige Arbeit zum Urheberrecht. Teilen Sie die Klasse in zwei Gruppen auf, z. B. nach dem Hausnummernprinzip, bei dem die Schüler durchgezählt werden und jeweils diejenigen mit den geraden und die mit den ungeraden Nummern eine Gruppe bilden. Es ist sicher ratsam, dass in jeder Gruppe Schüler sind, die sich bereits gut mit Tauschbörsen auskennen.

Die Internetrecherche ist nicht ganz einfach. Sie sollten den Schülern und Schülerinnen ausreichend Zeit geben, die Fragen zu beantworten.

Lösungen:

Aufgabe 1: Die David Guetta-Kopie – erlaubt oder nicht?
Till hat die CD illegalerweise heruntergeladen und somit auch illegalerweise zum Download zur Verfügung gestellt. Er hätte wissen müssen, dass die aktuelle Platte der Band nicht kostenlos im Internet zur Verfügung steht. Im Auftrag des Musiklabels sprechen Anwaltskanzleien Abmahnungen wegen unerlaubter Verwertung aus. Till kann also auch zu einem Schadensersatz verklagt werden.

Aufgabe 2: Die Antworten befinden sich in den Sachinformationen.

Aufgabe 3: Textvorschlag Vorfahrtsschild
Bleibt man bei Material, für das die Urheberrechte geklärt sind – sei es, weil es eigenes Material ist oder weil die Rechteinhaber eine Verbreitung erlaubt haben – oder nutzt Filehoster / Tauschbörsen zum rein privaten Gebrauch und nur passiv, ist man meist auf der sicheren Seite.

Lust auf mehr?
- Lebensweltbezug: Ist der Mitschnitt von Musik bei Videos auf YouTube legal? Diese Frage können Sie als Zusatz- oder Hausaufgabe geben.
- Ähnlich wie bei Musik verhält es sich mit Filmen, hier könnten Sie die Schülerinnen und Schüler ebenfalls recherchieren lassen.

Musik aus dem Internet?

Deine Freundin Anna hat dir vor kurzem erzählt,
dass sie sich Lieder aus dem Internet heruntergeladen hat.
Bisher hast du immer gedacht, dies sei verboten.
Auch dein Vater hat dir so etwas erzählt und
in den Nachrichten hört man das doch auch immer.

Arbeitsaufträge:

1. Stelle dir vor, du bist ein bekannter Musiker, der auch schon einige CDs gemacht hat. Würdest du wollen, dass man deine Lieder auch umsonst aus dem Internet bekommen kann? Diskutiert dies in der Klasse!

2. Setze dich mit einer Partnerin/einem Partner zusammen und überlege, welche Vorteile und Nachteile es hat, wenn man Musik kostenlos aus dem Internet herunterladen kann. Füllt die Tabelle alleine aus und vergleicht dann:

Für den Künstler/die Künstlerin		Für dich	
Vorteile	**Nachteile**	**Vorteile**	**Nachteile**

Selbstverständlich ist es verboten, Musik kostenlos aus dem Internet herunterzuladen, wenn der Künstler dies nicht erlaubt. Im Laden musst du ja auch für eine CD bezahlen. Auf **www.kindermusikbox.de** *ist das anders, der Künstler hat dort seine Musik „freigegeben" und jeder darf sie sich kostenlos anhören. Aber das ist eigentlich eine Ausnahme, denn normalerweise muss man für die Lieder bezahlen.*

www.kindermusikbox.de
www.jamendo.de
https://archive.org/details/audio

3. Schaue dir die Seiten aus dem Kasten genau an. Wo steht, dass du die Musik kostenlos benutzen darfst? Arbeitet zu zweit und zeige es deiner Partnerin/deinem Partner.

4. Dein Wunschlied läuft den ganzen Tag im Radio rauf und runter. Informiere dich, ob du Lieder aus dem Internetradio aufnehmen darfst oder nicht. Falls ja, wie darfst du das Lied nutzen? Ist die Weitergabe erlaubt? Das Anfertigen einer Kopie? Oder das Kopieren auf einen mp3-Player?

Informiere dich hier, wie du Musik aus dem Internet legal nutzen darfst:

www.irights.info und
www.respectcopyrights.de

Up- und Downloads – Was ist legal, was illegal?

Konrad und sein Freund Till hören auf dem Heimweg von der Schule das neue David-Guetta-Album …

Super Sache, aber kann das wirklich so einfach sein? Und ist das überhaupt legal? Darf man Dateien über solche Angebote herunterladen? Was denkt ihr? Macht eine kurze Umfrage in der Klasse.

Arbeitsaufträge:

1. Teilt euch in zwei Gruppen auf und recherchiert im Internet zu der Frage, ob das legal ist.
2. Teilt euch in Gruppe A und B.
   Bereitet ein Kurzreferat (maximal 10 Minuten) zum eurem Thema vor.
   Nehmt die Fragen und Stichwörter als Hilfen für euer Referat.

Gruppe	A Zum Download öffentlich bereitstellen	B Dateien selbst downloaden
Thema	Darf ich der Öffentlichkeit Dateien zum Download anbieten?	Darf ich Dateien herunterladen?
Fragen	Was ist verboten? Was ist erlaubt? Welche technischen Unterschiede gibt es zwischen Tauschbörsen und Filehostern?	
Stichwörter für die Suche in Suchmaschinen	Privatkopieschranke, Vervielfältigung, öffentlich zugänglich machen, Filehoster, Filesharing, Tauschbörse	
Internetadressen	**http://irights.info/kategorie/themen/filesharing-streaming** **http://www.klicksafe.de/themen/downloaden/tauschboersen/** **http://www.klicksafe.de/themen/downloaden/urheberrecht/** **http://www.klicksafe.de/themen/downloaden/urheberrecht/irights/filehosting/** **http://www.klicksafe.de/themen/rechtsfragen-im-netz/irights/filehosting/s/filehosting/** Artikel: Filehoster – Hehler oder Helfer auf www.spiegel.de („Hehler oder Helfer" in die Suchmaske eingeben)	

3. Erstellt nun Verkehrsschilder für das Bereitstellen und das Herunterladen von Dateien (in Tauschbörsen und über Filehoster) mit folgenden Überschriften:

   Stoppschild: Das ist verboten! Vorfahrtsschild: Das ist erlaubt!

8|1 Kritisches Surfverhalten und Passwörter
8|2 WLANs und fremde Rechner
8|3 Digitaler Fußbabdruck
8|4 Datensicherung und -löschung

8

Was wir immer tun sollten: Mindestschutz!

Was wir immer tun sollten: Mindestschutz!
8_1 Kritisches Surfverhalten und Passwörter
8_2 WLANs und fremde Rechner
8_3 Digitaler Fußbabdruck
8_4 Datensicherung und -löschung

Kritisches Surfverhalten und Passwörter

Ob es sich nun um die Bestellung bei einem Onlineversandhandel, das Profil in einem Sozialen Netzwerk oder die Anmeldung bei einem Internetdienst handelt: Schnell sind persönliche Daten in ein Onlineformular eingetragen. Mittlerweile müsste den meisten Internetnutzern jedoch bewusst sein, dass mit persönlichen Daten nicht sorglos umgegangen werden darf und auch ein kritischer Blick auf die Weiterverwendung der Daten erfolgen sollte: Was passiert nach der Eingabe mit den Daten? Wer hat Zugriff darauf? Wie sind die Daten gesichert und welche Rechte habe ich als Nutzer?

Datenschutzgrundlagen
Folgende Angaben fallen unter den hier relevanten Datenschutz:

- Personenbezogene Daten: alle Angaben zur Person, wie z. B. Name, Adresse, Alter, Familienstand, Beruf, Zeugnisse oder Kreditkartennummern.
- Sensible Daten, wie z. B. Angaben über die Herkunft, politische Meinungen, Gesundheit oder Sexualität. Diese werden im Bundesdatenschutzgesetz als „besondere Arten personenbezogener Daten" bezeichnet.[1]

Geregelt ist der Datenschutz vor allem im Bundesdatenschutzgesetz (BDSG) und in den Landesdatenschutzgesetzen. Speziell für den Bereich des Internets finden sich die Datenschutzregelungen im Abschnitt 4 „Datenschutz" des Telemediengesetzes (TMG).[2] Folgende Grundsätze gelten:

- Es muss darüber informiert werden, was mit den beim Nutzer erhobenen personenbezogenen Daten geschieht.
- Daten dürfen immer nur solange vorgehalten werden, wie es der Geschäftszweck erfordert.
- Es dürfen nur diejenigen personenbezogenen Daten erhoben und verarbeitet werden, die für den Abschluss und Abwicklung eines Vertragsverhältnisses erforderlich sind. Bei der Registrierung für einen Dienst dürfen also nur solche Angaben als Pflichtangaben abgefragt werden, die der Anbieter tatsächlich benötigt. Alle anderen müssen freiwillige Angaben sein.
- IP-Adressen und andere Nutzungsdaten dürfen vom Anbieter nur erhoben und verarbeitet werden, soweit er dies für die Inanspruchnahme oder Abrechnung seines Dienstes benötigt.

Recht auf Auskunft und Einsichtnahme
Auf Grundlage dieses Rechts darf man – ob bei einem Unternehmen oder einer Behörde – Auskunft verlangen über:

- Daten, die zur Person verarbeitet wurden,
- den Zweck der Datenverarbeitung,
- die Herkunft der Daten oder weitere Empfänger, an die die Daten weitergeleitet werden und
- die Technologien, die zur Verarbeitung der Daten benutzt wurden.

Sind die verarbeiteten Daten nicht richtig, so hat man den Anspruch auf Berichtigung, ggf. auf Sperrung, Löschung oder sogar Schadensersatz.

Nicht nur deutsches Recht ermöglicht diese Einsichtnahme, sondern auch europäisches. Genaueres wird in der aktuellen Datenschutzrichtlinie (Richtlinie 95/46/EG) geregelt. Diese soll in den nächsten Jahren durch eine umfangreiche, zeitgemäße Neuregelung, die „Datenschutz Grundverordnung", ersetzt werden (Stand: August 2015).[3]

Aus der Praxis

Ein eindrucksvolles Beispiel für die Herausgabe gespeicherter Daten ist dabei sicherlich, wenn Nutzer beispielsweise eine Daten-CD von Facebook anfragen, wie dies der österreichische Jura-Student Max Schrems im Jahre 2011 tat. Facebook schickte ihm daraufhin eine CD mit einer knapp 500 MB großen PDF-Datei mit über 1200 Seiten persönlicher Daten zu, die bei Facebook über ihn gespeichert wurden. Bei Minderjährigen muss der Antrag auf Einsichtnahme von den Erziehungsberechtigten gestellt werden.

Kurze Fragen und wichtige Antworten

Ehe persönliche Daten auf einer Internetseite preisgegeben werden, sollten folgende Fragen beantwortet werden:

- Finden sich auf der Internetseite die Kontaktdaten des Anbieters? (Firmennamen, Vertretungsberechtigter des Dienstanbieters, dazugehörige Anschrift mit Telefon-/Faxnummer, E-Mail-Adresse)
- Wird in einer „Datenschutzerklärung" darüber informiert, in welcher Form die personenbezogenen Daten erfasst und verarbeitet werden?
- Welche Daten sind wirklich erforderlich?
- Wird auf das Recht auf Widerruf und Widerspruch hingewiesen?
- Wer bekommt die Daten noch? Kann die Weiterleitung abgelehnt werden?
- Wird über das Recht auf Auskunft und Einsichtnahme hingewiesen?
- Welche Daten werden gespeichert und wann werden sie gelöscht? (Die Zusammenstellung eines Nutzerprofils muss abgelehnt werden können.)
- Werden die Daten bei der Übertragung verschlüsselt (URL im Browser beginnt mit „https://" statt „http://")?
- Besteht ein Unterschied zwischen notwendigen und freiwilligen Angaben?

Onlineshopping

Seriöse Online-Händler haben ein großes Interesse daran, dass die Kunden ihnen vertrauen und achten deshalb auf ein hohes Maß an Datensicherheit. Um das zu dokumentieren, verwenden sie auch Gütesiegel, die eine gewisse Qualität anzeigen sollen. Wie in anderen Bereichen, etwa bei Öko- oder Bio-Produkten, gibt es eine Vielzahl von Gütesiegeln mit ganz unterschiedlichen Qualitätsanforderungen. Die Initiative D21 (www.initiatived21.de), als Zusammenschluss von Experten aus Politik und Wirtschaft, empfiehlt auf Grundlage eigener Kriterien folgende Gütesiegel bei Onlineshops:

❶ **Trusted Shops**

❷ **TÜV Süd S@fer Shopping**

❸ **Internet Privacy Standards**

❹ **EHI geprüfter Onlineshop**

Quelle: Initiative D21[5]

Weitergehende Informationen zum Thema Onlineshopping stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Verfügung: **www.bsi-fuer-buerger.de** (z. B. unter „Einkaufen im Internet)

Beispiele und Beschwerden
Bei Verstößen gegen das Datenschutzgesetz hat man die Möglichkeit, sich bei den jeweiligen Datenschutzbehörden zu beschweren. Eine Übersicht über Kontaktadressen von Datenschutzinstitutionen in Deutschland sowie weiterführende Informationen zum Thema findet sich auf der Webseite des „Virtuellen Datenschutzbüros" des Landesbeauftragten für Datenschutz in Schleswig-Holstein:
www.datenschutz.de/institutionen/adressen

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist zu finden unter:
www.bfdi.bund.de

Passwörter

Passwortepidemie
Das US-Militär ging für Jahrzehnte mit schlechtem Beispiel voran, denn das Passwort für den Abschuss der US-Minuteman-Atomraketen war denkbar schlecht: Wie das Online-Portal „heise.de" berichtete, bestand es für fast zwei Jahrzehnte aus acht Nullen (00000000). Das Strategic Air Command (SAC) wollte vermutlich gewährleisten, dass die Soldaten in der heißen Phase des Kalten Krieges die Raketen möglichst schnell starten können.[6] Damit ist dieses Beispiel gut geeignet, das Dilemma von Passwörtern zu verdeutlichen: Sie sind immer eine Balance daraus, gut merkbar zu bleiben und auch stark, also sicher sein zu müssen.

E-Mail-Konto, Onlineshop, Onlinebanking oder Soziales Netzwerk – egal, um welchen Internetdienst es sich handelt: Passwörter sind zur Identifizierung des Nutzers unerlässlich. Sie erlauben dem Nutzer, sich vor unerlaubten Eingriffen von Fremden zu schützen. Häufig werden jedoch eher leichtsinnige Passwörter gewählt. So sind beispielsweise der Name des Partners / der Partnerin, das Geburtsdatum der Kinder oder der Namen des Haustieres sehr beliebt, jedoch auch für andere leicht zu erraten. Aber auch besonders gefällige Zahlen- bzw. Buchstabenkombinationen werden häufig gewählt.

Alljährlich werden die unsichersten Passwörter des Jahres veröffentlicht. Darunter sind regelmäßig folgende Zeichenkombinationen:[7]

- password
- 123456
- 12345678
- qwerty
- abc123
- 111111
- 1234567

Das Problem
Folgende Punkte sollten im Umgang mit Passwörtern vermieden werden:

- keine „echten" Wörter, die im Wörterbuch (Duden) zu finden sind, benutzen
- keine (Kose-)Namen verwenden
- nicht Passwort für mehrere Webdienste nutzen
- Passwörter nicht in E-Mails oder Ähnlichem weitergeben
- Passwörter nicht auf einem Zettel in der Nähe des PCs aufbewahren (beliebt ist in Büros der Aufkleber unter der Tastatur)
- vor der Eingabe des Passwortes darauf achten, dass die Webseite nicht über einen Link, sondern selbst angewählt wird
- niemanden über die Schulter schauen lassen o. ä.

Warum Passwörter nicht per Zettel am PC hängen oder in einer E-Mail weitergegeben werden sollen, ist leicht verständlich. Warum aber keine Dudenwörter? Dazu muss man wissen, wie manche Passwort-Entschlüsselungs-Software arbeitet: diese nutzen die sogenannte „Brute-Force" Methode und probieren einfach alle im Duden vorkommenden Wörter aus. Mit der entsprechenden Software geht das innerhalb von Minuten, worauf auch das BSI verweist: „(Hacker) … haben Werkzeuge, die vollautomatisch alle möglichen Zeichenkombinationen ausprobieren oder ganze Wörterbücher einschließlich gängiger Kombinationen aus Worten und angefügten Zahlen testen.
Um das zu verhindern, sollte ein Passwort bestimmte Qualitätsanforderungen erfüllen."[8]

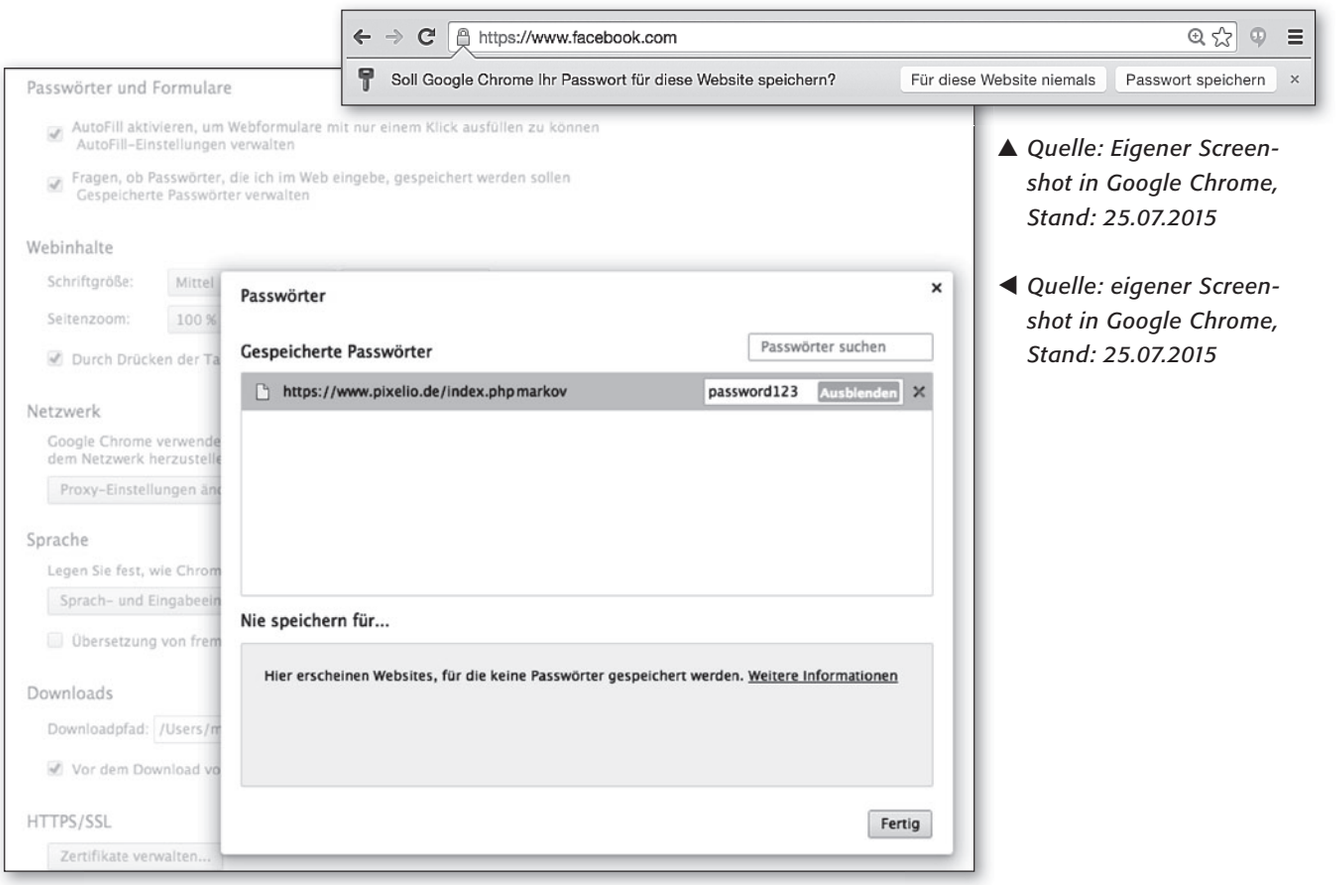
Was wir immer tun sollten: Mindestschutz!
8_1 Kritisches Surfverhalten und Passwörter
8_2 WLANs und fremde Rechner
8_3 Digitaler Fußbabdruck
8_4 Datensicherung und -löschung

Vorbeugung
Der beste Schutz ist selbstverständlich die Wahl eines starken Passworts. Aber wie sollte ein solches Passwort aussehen?[9]

Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt für die Wahl eines guten Passwortes:

- Es sollte **mindestens zwölf Zeichen** lang sein. (Ausnahme: Bei Verschlüsselungsverfahren wie z. B. WPA und WPA2 für WLAN sollte das Passwort mindestens 20 Zeichen lang sein. Hier sind sogenannte Offline-Attacken möglich, die auch ohne stehende Netzverbindung funktionieren – das geht beim Hacken von Online-Accounts nicht.)
- Es sollte aus **Groß- und Kleinbuchstaben** sowie **Sonderzeichen und Ziffern ($!%+…)** bestehen.
- Tabu sind Namen von Familienmitgliedern, des Haustieres, des besten Freundes, des Lieblingsstars oder deren Geburtsdaten usw.
- Wenn möglich sollte es nicht in **Wörterbüchern** vorkommen.
- Es sollte nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern bestehen, **also nicht asdfgh** oder **1234abcd** und so weiter.
- Einfache Ziffern am Ende des Passwortes anzuhängen oder eines der üblichen Sonderzeichen ($! ? //), am Anfang oder Ende eines ansonsten simplen Passwortes zu ergänzen, ist auch nicht empfehlenswert.

Verwaltung der Passwörter
Eine der wohl gefährlichsten Funktionen ist die Möglichkeit, Passwörter ohne spezielle Software vom Computer speichern zu lassen. So werden sie beispielsweise im Internet-Explorer gefragt, ob sie das Passwort speichern möchten (Funktion „Auto-Vervollständigen"). Beim nächsten Aufruf der Seite müssen sie es dann nicht mehr eingeben. Das ist schön bequem, aber auch schön gefährlich, denn selbstverständlich kann auch der nächste Benutzer des Computers diese Funktion nutzen. Alle modernen Browser bieten diese Funktion der Speicherung von Passwörtern an und einige machen das Auslesen der Passwörter sehr einfach, bei anderen helfen kleine, kostenlose Tools.



▲ *Quelle: Eigener Screenshot in Google Chrome, Stand: 25.07.2015*

◀ *Quelle: eigener Screenshot in Google Chrome, Stand: 25.07.2015*

Das Bild demonstriert, wie einfach Passwörter auszulesen sind, die im Browser gespeichert sind (hier: Google Chrome, Version 29.0.1547.76 unter „Einstellungen“ – „Erweiterte Einstellungen“ – „Passwörter und Formulare“ – „Gespeicherte Passwörter verwalten“). Das Passwort „password123“ dient hier nur zu Anschauungszwecken.

Neben diesen browserinternen Verwaltungsmöglichkeiten, bieten einige Hersteller Software zur Verwaltung von Passwörtern auf der Festplatte an. Mit einem „Master-Passwort“ sind alle anderen zu sichern, d. h. es muss sich nur ein einziges gemerkt werden. Hier ist Vorsicht geboten: Nur wirklich seriösen Anbietern sollte Vertrauen geschenkt werden, denn wer garantiert hier für die Datensicherheit?

Passwort-Check

Einige Webseiten bieten die Möglichkeit Passwörter zu testen. Aber auch hier sollte das Angebot nicht leichtsinnig genutzt werden: Nie das tatsächliche Passwort verwenden, sondern nur ein ähnlich aufgebautes.

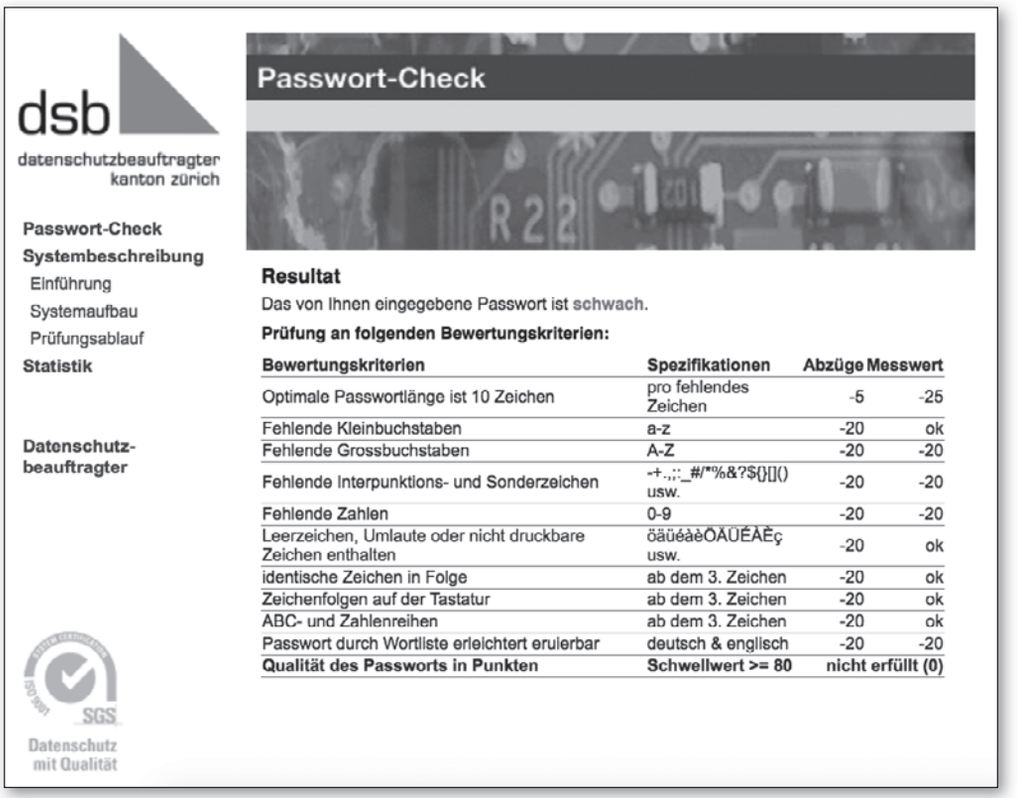
Aus der Praxis

Die Sensibilisierung für starke und geheime Passwörter kann ein Kinderspiel sein. SchülerInnen sind hier oft sehr kreativ und verstehen gut, warum sie dies trainieren sollen.

Unter **https://checkdeinpasswort.de** können Passwörter auf ihre Sicherheit überprüft werden. Darüber hinaus erhält man Tipps für eine sichere Passwortwahl.

Quelle: Eigener Screenshot nach einem Test mit dem Passwort „Hase“, Stand: 25.07.2015

Auch beim Datenschutzbeauftragten des Kantons Zürich (dsb) ist eine solche Passwortprüfung unter **http://review.datenschutz.ch/passwortcheck/check.php** möglich. Zudem erhält man einen detaillierten Prüfbericht mit vielen Kriterien für eine sichere Passwortwahl. Das hier getestete Passwort „willi" fällt eindeutig durch.



dsb
datenschutzbeauftragter kanton zürich

Passwort-Check
Systembeschreibung
Einführung
Systemaufbau
Prüfungsablauf
Statistik

Datenschutz-beauftragter

SGS
Datenschutz mit Qualität

Passwort-Check

Resultat

Das von Ihnen eingegebene Passwort ist schwach.

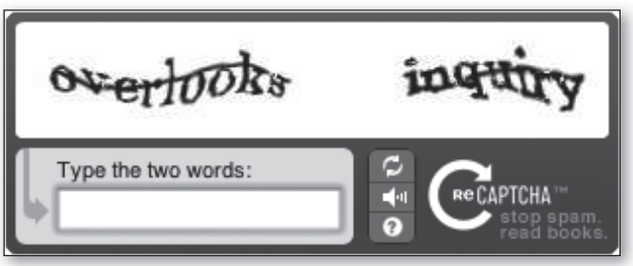
Prüfung an folgenden Bewertungskriterien:

Bewertungskriterien	Spezifikationen	Abzüge	Messwert
Optimale Passwortlänge ist 10 Zeichen	pro fehlendes Zeichen	-5	-25
Fehlende Kleinbuchstaben	a-z	-20	ok
Fehlende Grossbuchstaben	A-Z	-20	-20
Fehlende Interpunktions- und Sonderzeichen	-+.,;:_#/*%&?${}[]() usw.	-20	-20
Fehlende Zahlen	0-9	-20	-20
Leerzeichen, Umlaute oder nicht druckbare Zeichen enthalten	öäüéàèÖÄÜÉÀÈç usw.	-20	ok
identische Zeichen in Folge	ab dem 3. Zeichen	-20	ok
Zeichenfolgen auf der Tastatur	ab dem 3. Zeichen	-20	ok
ABC- und Zahlenreihen	ab dem 3. Zeichen	-20	ok
Passwort durch Wortliste erleichtert erulerbar	deutsch & englisch	-20	-20
Qualität des Passworts in Punkten	**Schwellwert >= 80**	**nicht erfüllt (0)**	

Quelle: Eigener Screenshot nach einem Test mit dem Passwort „willi", Stand: 25.07.2015

Captchas - Mensch oder Maschine?

Für viele Anbieter im Internet stellt sich das Problem, erkennen zu müssen, ob sich ein Mensch oder eine Software (automatisch) anmeldet. Diese bekannten Zerrbilder mit Zahlen- oder Buchstabenkombinationen, die inzwischen bei zahlreichen Anmeldeprozeduren eingegeben werden müssen, heißen „Captchas" (Completely Automated Public Turing test to tell Computers and Humans Apart) und sollen sicherstellen, dass sich ein Mensch und keine Software („Bot") anmeldet. Da auch diese nicht mehr 100%ig sicher sind und auch die Software zur Erkennung der verzerrten Buchstaben immer besser wird, gehen manche Firmen dazu über, Bilder zu zeigen, die wirklich nur Menschen unterscheiden können. Dabei gilt es immer die Balance zu halten zwischen Sicherheit auf der einen und Benutzerfreundlichkeit auf der anderen Seite.



Quelle: captcha.net[10]

Links und weiterführende Informationen

Webseiten

www.gesetze-im-internet.de/tmg/
Telemediengesetz (TMG) im Wortlaut

www.gesetze-im-internet.de/bdsg_1990/index.html
Bundesdatenschutzgesetz (BDSG) im Wortlau

http://ec.europa.eu/justice/data-protection/index_de.htm
Informationen der Europäische Kommission zum Schutz personenbezogener Daten

www.europe-v-facebook.org
Die Initiative hilft bei der Antragstellung zur Herausgabe der gesammelten Daten durch Facebook

www.bsi-fuer-buerger.de
Das Bundesamt für Sicherheit in der Informationstechnik mit Tipps zu Onlineshopping, Passwörtern usw.

www.datenschutz.de
Virtuelles Datenschutzbüro mit weiterführenden Informationen

www.bfdi.bund.de
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Endnoten

[1] BUNDESDATENSCHUTZGESETZ (BDSG). *§ 3 Weitere Begriffsbestimmungen.* Aufgerufen am 25.07.2015 unter http://www.gesetze-im-internet.de/bdsg_1990/__3.html

[2] TELEMEDIENGESETZ (TMG). Aufgerufen am 25.07.2015 unter http://www.gesetze-im-internet.de/tmg/BJNR017910007.html

[3] EUROPÄISCHE Kommission. (2012, 25. Januar). *Pressemitteilung: Kommission schlägt umfassende Reform des Datenschutzrechts vor, um Nutzern mehr Kontrolle über ihre Daten zu geben und die Kosten für Unternehmen zu verringern.* Aufgerufen am 25.07.2015 unter http://europa.eu/rapid/press-release_IP-12-46_de.htm?locale=en

[4] INITIATIVE D21. (2010, 08. Oktober). *D-21 Qualitätskriterien für Internetangebote.* Aufgerufen am 25.07.2015 unter http://www.initiatived21.de/wp-content/uploads/2013/01/D21_Qualitaetskriterien_2011.pdf

[5] INITIATIVE D21. (2013). *Empfohlene Anbieter nach den Qualitätskriterien des Monitoring Board* (Absatz 3). Aufgerufen am 25.07.2015 unter http://internet-guetesiegel.de/qualitaetskriterien

[6] SCHERSCHEL, F. (2013, 04. Dezember). *00000000: Passwort für US-Atomraketen.* heise.de. Aufgerufen am 25.07.2015 unter http://www.heise.de/security/meldung/00000000-Passwort-fuer-US-Atomraketen-2060077.html

[7] SPLASH Data. (2015, 20. Januar). *„123456" Maintains the Top Spot on our Annual „Worst Password" List.* Aufgerufen am 25.07.2015 unter http://splashdata.com/splashid/worst-passwords/

[8] BUNDESAMT für Sicherheit in der Informationstechnik (BSI). (2015). *Wie mache ich meinen PC sicher? Passwörter* (Absatz 1). Abgerufen am 20.07.2015 unter https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html;jsessionid=2C6B2738194C1EE070C80B38F56FA240.2_cid369

[9] BUNDESAMT für Sicherheit in der Informationstechnik (BSI). (2015). *Wie mache ich meinen PC sicher? Passwörter.* Abgerufen am 20.07.2015 unter https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html;jsessionid=2C6B2738194C1EE070C80B38F56FA240.2_cid369

[10] CAPTCHA.NET. (2015). *CAPTCHA: Telling Humans and Computers Apart Automatically* (Absatz 2). Aufgerufen am 25.07.2015 unter http://www.captcha.net

Arbeitsblatt	**AB 1**	**AB 2**
Titel	**Informationelle Selbstbestimmung – was ist das denn?**	**Sichere Passwörter – wie geht das?**
Kompetenzen	Die Schülerinnen und Schüler wählen aus Beispielen aus, welche Daten aus Sicht einer „informationellen Selbstbestimmung" schützenswert und welche unproblematisch zu veröffentlichen sind.	Die Schülerinnen und Schüler beurteilen ein System zur Erstellung sicherer Passwörter und setzen es mit einem eigenen Beispiel um.
Methoden	Stichwortliste, Plakat, Einzelarbeit, Unterrichtsgespräch	Passwortsystem erfinden, Passwort-Check, Einzelarbeit, Unterrichtsgespräch.
Material	Arbeitsblatt, großes Papier, bunte Stifte	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	nein	ja

Hinweise für die Durchführung

AB 1: Informationelle Selbstbestimmung – was ist das denn?

Der Hinweis auf „informationelle Selbstbestimmung" dient als Einstieg und könnte vielleicht später noch vertieft werden (s. „Lust auf mehr"). Die Schülerinnen und Schüler sollen hier verschiedene Stichwörter zu persönlichen Angaben ausschneiden und bewerten. Dazu kleben Sie die Stichwörter auf, je weiter links desto problematischer wäre eine Angabe, je weiter rechts desto problemloser. Dabei gibt es sicherlich Dinge, die man nie ohne Weiteres weitergeben sollte (z. B. Handynummer) und die Dinge, die von Fall zu Fall weder hochproblematisch noch ungefährlich sind (z. B. Postleitzahl) sowie Fakten, die ohne Personenbezug unwichtig sind (z. B. Schuhgröße). Hier könnten Sie weitere Beispiele einfügen, die von den Schülerinnen und Schüler genannt werden.

Der zweite Arbeitsauftrag ist je nach Altersstufe nicht ganz einfach zu beantworten, denn die Interessen hinter der Datensammelwut sind für Schülerinnen und Schüler nicht immer einsichtig. Hier hilft der Hinweis auf die kommerziellen Interessen, z. B. für gezielte Werbung. Zum Schluss soll das Wichtigste in Form eines Plakats festgehalten werden.

AB 2: Sichere Passwörter – wie geht das?

Mit diesem Arbeitsblatt sollen sich die Schülerinnen und Schüler dem Thema Passwortschutz spielerisch über den Einstieg „Geheimsprache" nähern, der hier mit einer Nummerierung des Alphabets gemacht ist.
Schreiben Sie das Beispiel an die Tafel und die Lösung / den „Schlüssel" auf eine zugeklappte Seite. **Hier ist ein Beispiel für eine Geheimsprache:**

160119192315051820051 8 14090513011219 2205181801200514

Und die dazugehörige Lösung, also der „Schlüssel": **a01 b02 c03 d04 e05 f06 g07 h08 i09 j10 k11 l12 m13 n14 o15 p16 q17 r18 s19 t20 u21 v22 w23 x24 y25 z26**

Lösung: Passwörter niemals verraten

Tipp:
Immer 2 Zahlen zusammen nehmen und den Buchstaben davor wählen
(Bsp: 16 = p; 01= a)

Ihre Schülerinnen und Schüler erfinden sicherlich eine schwierigere Geheimsprache (s. Arbeitsauftrag). Die Tipps für gute Passwörter können auch die jüngeren Schülerinnen und Schüler nachvollziehen, vielleicht sollten Sie die einzelnen Punkte verdeutlichen. Der letzte Punkt dient der Überprüfung, wobei selbstverständlich das Ziel sein sollte, dass niemand das Passwort „knacken" kann. Hier ist der Spagat wichtig zwischen der Notwendigkeit, sich Passwörter gut merken zu können und ihrem Schutz.

Erfahrungsgemäß brauchen die Schülerinnen und Schüler ein wenig Unterstützung bei der „Geheimsprache“ des folgenden Arbeitsauftrages. Hier sollen sie für sich ein System entwickeln, mit dem die Wörter gut zu merken sind. Das Beispiel auf dem Arbeitsblatt kann als Modell für die Erstellung und Memorierung von Passwörtern dienen. Danach können sie sehr schnell einsehen, dass man mit diesem System viele verschiedene, gute Passwörter erstellen kann, denn man braucht nur den Ausgangsnamen verändern (eigener Name, Name der Mutter, des Vaters, der Haustiere etc.). In diesem Fall ist auch eine kleine Notiz „Hund“ nicht schlimm, denn niemand kennt das System.

Lösung:

Merken	Passwort	Beschreibung
Mein Hund heißt:	Naischa	Leicht zu merken.
Alle Vokale in Großschreibung:	nAIschA	Die Selbstlaute sind groß geschrieben, alles andere klein.
Meine Telefonnummer lautet 765499; immer abwechselnd ein Buchstabe und ein Zahl:	N7A6I5s4c9h9A	Die Telefonnummer ist eingebaut.
Das Ganze immer in Klammern, damit der Hund nicht wegläuft:	(N7A6I5s4c9h9A)	Es wurden Klammern gesetzt.

Mit der Adresse **https://checkdeinpasswort.de** steht ein Tool zur Verfügung, sein Passwort zu testen. Dabei sollte den Schülerinnen und Schülern klar gemacht werden, dass man nie sein tatsächliches Passwort dort eingibt, denn trotz der Seriosität dieses Anbieters sollte man im Internet nie auf einer unbekannten Webseite sein richtiges Passwort eingeben.

Lust auf mehr?

- Im Zusatzmodul „Ethik macht klick – Werte-Navi fürs digitale Leben“ finden sich weitere Materialien zum Thema unter Baustein 1 Projekt 6 „Aktiv werden“: **http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Ethik/LH_Zusatzmodul_medienethik_klicksafe_gesamt.pdf**
- Das Recht auf informationelle Selbstbestimmung könnte ein schöner Aufhänger zu einer Fortführung des Themas sein. Dabei sind sowohl historische Fragen interessant – erinnert sei an das „Volkszählungsurteil“ des Bundesverfassungsgerichts, in dem erstmals dieses Recht fixiert wurde – als auch ganz aktuelle. Die Datensammelwut lässt heutzutage eine fast lückenlose „Beobachtung“ zu, siehe Kapitel 8_3 „Digitaler Fußabdruck“.
- Hacker versuchen ständig Passwörter zu knacken. Sie gehen dabei ausgesprochen listig vor. Die Schüler können sich über folgende Methoden informieren: Programmierbare Tastatur auf einem USB-Stick, „Rainbow“-Tabellen, Passwortlisten aus Wörterbüchern, Passwortlisten aus gestohlenen Passwortlisten, Software-Manipulationen, Vor- und Nachnamen ausprobieren, Kombinationen mit dem Namen des Angebots (z. B. youtube123), Ersatz von Buchstaben mit ähnlichen Ziffern (z. B. N3isch3).

Informationelle Selbstbestimmung – was ist das denn?

*Du hast das Recht auf **„informationelle Selbstbestimmung"**. Dieses Recht sagt: Du hast das Recht zu wissen, wer was wann über dich weiß. Normalerweise ist das kein Problem, denn natürlich muss deine Schule dein Geburtsdatum, deinen Namen und deine Adresse wissen und auch im Sportverein musst du all dies angeben. Aber muss deine Schule auch wissen, welche Haustiere du hast oder dass dein Lieblingsverein der FC Schalke 04 ist?*

Im Internet ist die Sache noch schlimmer! Bei vielen Internetseiten musst du dich anmelden und wirst alles Mögliche gefragt.

Arbeitsaufträge:

1. Überlege genau, welche persönlichen Dinge du problemlos von dir weitergeben kannst. Unten findest du eine Stichwortliste. Bei welchen Dingen musst du unbedingt deine Eltern fragen? Schneide die Stichworte aus und sortiere sie entlang dieser Linie (je weiter links, desto problematischer, je weiter rechts, desto weniger problematisch ist eine Angabe).

Immer Eltern fragen — **kein Problem**

Name	Geburts-datum	Spitzname	Alter	Wohnort	Straße
Postleitzahl	Handy-nummer	Telefon-nummer	Größe	Name der Mutter	Name des Vaters
Schuhgröße	Einkommen der Eltern	Geschwister-zahl	Vorname	Taschengeld-höhe	Name des Freundes
Foto von dir	Lieblings-tier	Lieblings-essen	Lieblings-Sportverein	Haustiere	Haarfarbe

2. Diskutiert gemeinsam im Klassenverband darüber, warum die Menschen, die diese Internetseiten machen, all das wissen wollen.

3. Überlegt auch, wie ihr euch das nächste Mal bei einer solchen Anmeldung verhalten könnt! Ihr findet sicherlich gute Tipps! Fasst diese auf einem Plakat zusammen!

Sichere Passwörter – wie geht das? (1/2)

„Statt vom Computerzeitalter sollte man lieber vom Passwortzeitalter sprechen", stöhnt Jasmin beim Abrufen ihrer E-Mails. „Ich verwende immer das gleiche: Nicolo – so heißt mein Meerschweinchen und das vergesse ich niemals". „Danke für die Information", antwortet ihr jüngerer Bruder, „Ich habe mir ein todsicheres System ausgedacht". „Lass mal hören!" … „Liebste Schwester – dann wäre es kein todsicheres System mehr!"

Gute Passwörter erfüllen folgende Bedingungen:

- *Gute Passwörter sind mindestens 12 Zeichen lang!*
- *Gute Passwörter enthalten sowohl Klein- und Großbuchstaben als auch Zahlen!*
- *Gute Passwörter enthalten Sonderzeichen (-+.,:_#/*%&?$\{\}[]()!*
- *Gute Passwörter bestehen nicht aus echten Wörtern oder Namen!*
- *Gute Passwörter sind trotzdem gut zu merken!*

Erfinden wir doch einfach eine Geheimsprache:

Die Kunst der Geheimsprache wird seit Jahrtausenden gepflegt.
Früher war sie nur für Könige und Generäle interessant,
aber im Computerzeitalter brauchen wir alle eine Geheimsprache.
Wir brauchen sie für die vielen Passwörter.
Übrigens … Kennwörter ist nur ein anderer Name für Passwörter!

Arbeitsaufträge:

1. Erfinde eine eigene Geheimsprache, in der auch Zahlen vorkommen können.
2. Zeige sie deiner Nachbarin/deinem Nachbarn und lasse sie „entschlüsseln"!

Sichere Passwörter – wie geht das? (2/2)

Und wie soll man sich so etwas merken? Wie kann man sich **IwidB_65uhJ** merken?
Das funktioniert am besten über ein System, hier ist ein Satz abgekürzt:
„Ich wohne in der Bunsengasse _65 und heiße Jan".

Wie funktioniert folgendes System? Findest du es heraus?

Merken	Passwort	Beschreibung der Veränderung
Mein Hund heißt:	Naischa	
?	nAIschA	
Meine Telefonnummer lautet 765499	N7A6I5s4c9h9A	
?	(N7A6I5s4c9h9A)	

3. Beschreibe das System oben! Probiere es mit zwei anderen Wörtern aus (zum Beispiel mit deinem eigenen Namen oder deinem Haustier)!

4. Erfinde ein eigenes System, wie du gute Passwörter machst und sie dir trotzdem merken kannst! Dann kannst du auch ein Stichwort notieren (oben dürfte man „Hund" notieren, oder?)

5. Ausnahmsweise darfst du dein System NICHT mit den anderen austauschen! Denke an Jasmin und ihren jüngeren Bruder!

Teste es im Internet unter: **www.checkdeinpasswort.de**

Denke daran, dass du nicht dein echtes Passwort verwendest!

Was wir immer tun sollten: Mindestschutz!
8_1 Kritisches Surfverhalten und Passwörter
8_2 WLANs und fremde Rechner
8_3 Digitaler Fußbabdruck
8_4 Datensicherung und -löschung

WLANs und fremde Rechner

Freie, also kostenlose, WLANs finden sich immer häufiger in Cafés, Restaurants, Bahnhöfen oder Flughäfen. Anstelle von WLAN wird auch häufig die Bezeichnung „Wi-Fi" genutzt, wobei es sich hierbei eigentlich um einen Markennamen zur Zertifizierung handelt.[1] Mit Laptops und vor allem mit Smartphones ist die Versuchung groß, diese Möglichkeit der schnellen Datenübertragung zu nutzen. Diese Angebote werden aber problematisch, wenn es um den Schutz der eigenen Daten geht.

Quelle: Wayda Dreamscape:
free_wi_fi_spot/flickr.com/cc-by-2.0

Auf freie Netzwerke kann jedermann zugreifen. Häufig wird eine Anmeldung gefordert, diese kann aber anonym ablaufen. Es gibt jedoch keine Möglichkeit die Nutzer zu beschränken oder zu identifizieren. Technisch kommt hinzu, dass die WLAN-Access-Points (also die Geräte, die das WLAN über mehrere Stationen zur Verfügung stellen) eine Funktion namens „Wireless Isolation" haben, die einen Datenaustausch zwischen den Geräten der Nutzer unterbindet. Bei öffentlichen WLANs ist diese Einstellung jedoch meist ausgeschaltet, mit der Folge, dass zusätzlich eine Gefahr von anderen Nutzern des Netzwerks ausgehen kann.

Noch krimineller wird es, wenn Angreifer ein öffentliches Netzwerk nur vortäuschen und als Hotspot-Anbieter ausgeben. Alle Daten, die übertragen werden, wandern zunächst über ihre Computer: Von Datenschutz kann dann also keine Rede mehr sein.

Probleme
Neben Störungen wie Netzausfällen oder einer mangelhaften Verbindungsqualität, gibt es zwei grundlegende Probleme beim Datenschutz in öffentlichen WLANs:

- der Übertragungsweg über Funk ist u. U. nicht sicher und kann „abgehört" werden
- der Zugang zum Funknetz (und damit auf die angeschlossenen Computer) ist u. U. nicht sicher: es kann „eingebrochen" werden

Aus der Praxis
Für viele Schülerinnen und Schüler ist dies schwierig zu verstehen, weil es in Widerspruch zu ihrem täglichen Nutzungsverhalten steht und sie vielleicht noch keine negativen Konsequenzen dieses Verhaltens bemerkt haben. Trotzdem sollte versucht werden, sie für eine sichere Nutzungsweise zu sensibilisieren.

Übertragungsweg über Funk
Alle Daten, die den kabellosen Weg von einem Computer zum Nächsten finden sollen, werden in ein Funksignal umgesetzt. Logischerweise kann jeder, der dieses Funksignal auffängt und dieselbe „Sprache" spricht, dieses nutzen. Der aktuelle Übertragungsstandard heißt IEEE 802.11n, IEEE steht dabei für Institute of Electrical and Electronics Engineers. Die Reichweiten der handelsüblichen Funknetze sind nicht größer als 100 bis 300 Meter bei optimalen Bedingungen (ohne Hindernisse wie Beton o. ä.). Mit etwas handwerklichem Geschick, ein wenig technischen Verständnis und einer entsprechendem Anleitung (z. B. aus dem Internet) kann die Reichweite aber erhöht werden: neben professionellen technischen Geräten lässt sich z. B. auch für wenige Euro eine Richtfunkantenne bauen, die die 500m-Grenze überwinden kann. Damit kann ein Funknetz leicht abgehört werden, auch wenn der Täter nicht zu sehen ist!

Deshalb wurden zur Absicherung des Datenverkehrs Verschlüsselungsverfahren entwickelt, die die Datenübertragung sicherer machen sollen. Ein älteres System heißt „WEP" (Wired Equivalent Privacy, zu Deutsch etwa „eine dem Kabelanschluss vergleichbare Privatsphäre"). Die neuere Technik „WPA" „Wi-Fi Protected Access", bzw. die inzwischen verbesserte Version „WPA2" ist zu bevorzugen.[2] Zusätzlich sollte ein Pre-Shared-Key (PSK) eingesetzt werden. Mittels WPA wird das Signal verschlüsselt versendet, mit dem PSK erhalten der Sender und der Empfänger bei jeder neuen Anmeldung einen neuen Schlüssel für die Entschlüsselung des Signals. Damit ist ein nicht unüberwindbarer, aber doch grundlegender Schutz in der Datenübertragung gewährleistet.[3]

Bei einem eigenen WLAN (auch in der Schule) sollten einige grundlegende Sicherheitsmaßnahmen ergriffen werden:

- Verschlüsseln mit WPA, besser WPA2.
- Einen eigenen und sicheren Netzwerkschlüssel vergeben (s. Kapitel 8_1 Passwörter).
- Den Namen des WLANs (den „Service Set Identifier", kurz SSID) ändern und „unauffällig" benennen (also nicht mit dem Namen der Schule beispielsweise).
- Ausschalten der WLAN-Geräte bei Nichtnutzung (ein Zeitmanagement machen, beispielsweise durch Zeitschaltuhren).
- Regelmäßige Updates der Geräte durchführen.

Folgen eines ungesicherten Funknetzes

Wird ein privates (oder möglicherweise schulisches) Netzwerk nicht abgesichert, ist somit einerseits das Abhören der übertragenen Daten für Fremde ein Leichtes, andererseits muss jedoch auch für möglicherweise durch Dritte entstandenen Schaden gehaftet werden. Im Klartext bedeutet dies: Den Besitzer der WLAN-Verbindung trifft zumindest eine Teilschuld, wenn ein Fremder sich illegal Filme, Musik etc. über diese aus dem Internet herunterlädt.

Der Bundesgerichtshof hat dies in einem Urteil vom 12. Mai 2010 festgestellt: „Privatpersonen können auf Unterlassung, nicht dagegen auf Schadensersatz in Anspruch genommen werden, wenn ihr nicht ausreichend gesicherter WLAN-Anschluss von unberechtigten Dritten für Urheberrechtsverletzungen im Internet genutzt wird."[4] Erwähnt sei aber auch, dass es durchaus politische Bemühungen gibt, diese sogenannte „Störerhaftung" für offene WLANs zu verändern, damit es mehr offene WLANs in Deutschland gibt und das Risiko für Anbieter vermindert wird.[5]

„Schwarz-Surfen"

Der ein oder andere konnte vielleicht schon einmal beobachten, dass jemand mit einem Laptop auf den Knien im Auto saß. Es ist jedoch nicht nur ein Hobby, wenn „Schwarz-Surfer" auf der Suche nach ungesicherten Funknetzen sind. Ob dies strafbar ist, ist eine spannende Frage und nicht einfach zu beantworten. Es ist auf jeden Fall strafbar, wenn Schutzmechanismen (wie die Verschlüsselung) umgangen werden. Wie sieht dies bei einem offenen Funknetz aus, das nicht abgesichert ist? Das Gesetz spricht von Daten, die besonders gesichert sein müssen:

§

Der § 202a StGB bezüglich des Ausspähens von Daten besagt:

„(1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft .

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden."[6]

Eindeutiger wird die Frage im Telekommunikationsgesetz (TKG) unter § 89 beantwortet:

„Mit einer Funkanlage dürfen nur Nachrichten, die für den Betreiber der Funkanlage, Funkamateure im Sinne des Gesetzes über den Amateurfunk vom 23.6.1997 (BGBl. I S. 1494), die Allgemeinheit oder einen unbestimmten Personenkreis bestimmt sind, abgehört werden. Der Inhalt anderer als in Satz 1 genannter Nachrichten sowie die Tatsache ihres Empfangs dürfen, auch wenn der Empfang unbeabsichtigt geschieht, auch von Personen, für die eine Pflicht zur Geheimhaltung nicht schon nach § 88 besteht, anderen nicht mitgeteilt werden." [7]

Schülerinnen und Schülern sollte also dringend davon abgeraten werden, es als ein Kavaliersdelikt zu betrachten, in fremde Funknetze einzubrechen.

Folgende Tipps für die Nutzung fremder Netzwerke sollten beherzigt werden:

- *WLAN-Funktion nur einschalten, wenn diese auch benötigt wird.*
- *Keine vertraulichen Daten abrufen.*
- *Keine sensiblen Anwendungen wie Online-Banking oder Online-Shopping nutzen. Auch die Anmeldung in Sozialen Netzwerken oder das Versenden von E-Mails kann problematisch werden.*
- *Datei- und Verzeichnisfreigabe deaktivieren.*
- *Die automatische Anmeldung an bekannten Hotspots deaktivieren. Hier besteht die Gefahr, dass bekannte Netzwerk-Namen automatisch angenommen werden, wie beispielsweise „FreeWiFi".*

Jedes Gerät geht heute online

Handys, Spielekonsolen, Drucker, Fernseher: immer mehr Geräte können eine Verbindung zum Internet aufbauen. Was für viele schon selbstverständlich ist, birgt unter dem Aspekt des Jugendschutzes einige Probleme. Früher war der Internetzugang von Kindern (und vielleicht auch Jugendlichen) einfacher zu beschränken als heute. Jede mobile Spielekonsole wie der New Nintendo 3DS oder die Sony PlayStation hat eine Online-Funktion. Mit diesen Geräten haben Kinder einen Internetzugang, der – anders vielleicht als beim heimischen PC – nicht unter der Kontrolle von Erwachsenen steht.

Fremde Rechner

Besondere Vorsicht ist geboten bei allen Rechnern, die von mehreren Personen genutzt werden, wie z. B. in der Schule. Hier sollten einige Tipps beherzigt werden:

- Alle temporären Dateien im Browser löschen.
- Wenn möglich, den Papierkorb und die temporären Dateien von Windows löschen.
- Immer den Browser nach der Nutzung schließen.
- Wenn möglich, den Computer nach der Nutzung immer herunterfahren.
- Keine persönlichen Daten eingeben, insbesondere keine Passwörter.
- Keine sensiblen Seiten – wie z. B. das Online-Banking – aufsuchen.
- Vorsicht bei der Nutzung von E-Mail Diensten walten lassen (u. U. später das Passwort ändern).

Links und weiterführende Informationen

Webseiten

www.bsi.bund.de/DE/Publikationen/Broschueren/broschueren_node.html
Übersicht zu relevanten Broschüren des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

www.verbraucher-sicher-online.de/artikel/ohne-eigenen-computer-surfen-das-internet-cafe
Onlineartikel zur sicheren Nutzung von Internet-Cafés

www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungWLAN-LAN/WLAN/Sicherheitstipps/sicherheitstipps_node.html
Sicherheitstipps des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Nutzung von privatem WLAN

http://irights.info/artikel/ein-netz-voller-fallgruben-stoererhaftung-datenschutz-meldepflicht-faq/24641
Online-Artikel zu häufigen Fragen zum Thema freie WLAN Netze

Endnoten

[1] WI-FI Alliance. (2015). *Certification.* Aufgerufen am 25.07.2015 unter http://www.wi-fi.org/certification

[2] ELEKTRONIK *Kompendium. (2015). WLAN-Sicherheit.* Aufgerufen am 25.07.2015 unter http://www.elektronik-kompendium.de/sites/net/1403011.htm

[3] ELEKTRONIK *Kompendium. (2015). Authentifizierung im Netzwerk.* Aufgerufen am 25.07.2015 unter http://www.elektronik-kompendium.de/sites/net/1710241.htm

[4] BUNDESGERICHTSHOF. (2010, 12. Mai). *Haftung für unzureichend gesicherten WLAN Anschluss* (Absatz 1). Aufgerufen am 25.07.2015 unter http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2010&Sort=3&nr=51934&pos=0&anz=101

[5] HEISE, C., & Bunse, V. (2015, 20. August). *Deutschland verpasst den Anschluss.* zeit.de. Aufgerufen am 21.08.2015 unter http://www.zeit.de/digital/internet/2015-08/digitale-agenda-bundesregierung-breitband-wlan

[6] STRAFGESETZBUCH (StGB). *§ 202a: Ausspähen von Daten* (Absatz 1). Aufgerufen am 25.07.2015 unter http://www.gesetze-im-internet.de/stgb/__202a.html

[7] TELEKOMMUNIKATIONSGESETZ (TKG). *§ 89: Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen* (Absatz 1). Aufgerufen am 25.07.2015 unter http://www.gesetze-im-internet.de/tkg_2004/__89.html

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Online – was soll nicht in fremde Hände**	**Euer Funknetz – ist es sicher?**
Kompetenzen	Die Schülerinnen und Schüler kennen die Bedeutung von Verlauf, Cookies, Passwörtern und Cache im Zusammenhang mit einem Browser. Sie können Einstellungen verändern und gespeicherte Daten löschen.	Die Schülerinnen und Schüler organisieren ein Interview mit einem Funknetz-Betreiber und werten es nach einem Fragenkatalog zur WLAN-Sicherheit aus.
Methoden	Internet-Recherche, Partnerarbeit, Unterrichtsgespräch	Interview, Recherche, Fragenkatalog, Checkliste, Einzelarbeit, Partnerarbeit, Unterrichtsgespräch
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	Ja (evtl. zur Recherche der Fach-Fragen)

Hinweise für die Durchführung

AB 1: Online – was soll nicht in fremde Hände	Verlauf, Cookies, Passwörter und Cache sind Stichworte, bei denen die Browser Daten über das Surfverhalten speichern. Im „Verlauf", auch „History" oder „Besuchte Seiten" o. ä. genannt, werden die Seiten gespeichert, die aufgerufen wurden. Dies hat den Vorteil, dass man einmal besuchte Seiten schneller wiederfindet. Es hat den Nachteil, dass jeder mit Einblick in das System sehen kann, welche Seiten ich aufgerufen habe. Die „Cookies" sind kleine Dateien, die die Anbieter von Internetseiten auf den Computern hinterlassen können (mehr darüber in den Sachinformationen). Sie enthalten Informationen darüber, auf welchen Seiten man war, wie lange, was man genau gesucht hat etc. Leider wird oft die Möglichkeit genutzt, Passwörter von Browsern verwalten zu lassen. Der Sinn dahinter ist, dass man es beim Aufruf einer passwortgeschützten Seite nicht einzugeben braucht. Leider mit einer großen Unsicherheit, denn der Browser stellt eine potenzielle Sicherheitslücke dar, wie viele Beispiele der Vergangenheit zeigen. Der „Cache" schließlich ist eine Art Zwischenspeicher auf dem eigenen Computer, wo Dateien wie Internetseiten mit Text, Bildern, Videos usw. abgelegt werden. Dies soll ein schnelleres Surfen ermöglichen, da diese Daten nicht erneut aus dem Internet geladen werden müssen. In Zeiten des Breitbands eigentlich nicht mehr so wichtig. Alle diese Daten ermöglichen es, Informationen über mein Surfverhalten zu erhalten. Bei problematischen Dingen (zum Beispiel illegale oder strafbare Downloads) kann darüber sogar strafrechtlich Relevantes erkannt werden. Alle Browser ermöglichen aber eine Löschung der Daten oder gar ein „privates Surfen" (oder ähnlich genannt), bei dem die Daten nicht gespeichert werden. Entsprechende Anleitungen finden sich sicherlich auf YouTube. Das Arbeitsblatt beinhaltet viele Rechercheaufgaben, ausreichend PCs für die Schülerinnen und Schüler sind hier notwendig.

AB 2: Euer Funknetz – ist es sicher?

Möchten Sie einen sehr eindrucksvollen Einstieg gestalten, dann nennen Sie die Funktion „Persönlicher Hotspot" Ihres Handy mit einem üblichen WLAN-Namen, zum Beispiel der Restaurant-Kette McDonalds oder Subways … und schalten es ein. Sofort taucht auf den Handys der Schüler dieses WLAN auf mit der Frage, sich zu verbinden. Wäre (DAS sollten Sie natürlich NICHT tun) nun das WLAN offen, wären die Handys mit dem Netz verbunden und ließen einen Zugriff zu.

Bei diesem Arbeitsblatt sind Erwachsene nötig. Die Schülerinnen und Schüler sollen anhand eines Fragenkatalogs die Sicherheit eines Funknetzes kontrollieren, indem sie einen Betreiber eines Funknetzes (das kann auch der Nachbar sein) interviewen. Als Sicherung sollen sie eine Checkliste erstellen, die die Frage beantwortet: „Worauf muss ich achten, wenn ich in ein Funknetz gehe?"

Die Möglichkeit, das Interview auch per Video zu führen ist sicherlich motivierend und mit einem Handy leicht zu bewerkstelligen. Wenn das Einverständnis der interviewten Person vorliegt, sollen die Schülerinnen und Schüler das Ergebnis präsentieren.

Lust auf mehr?

- Das Thema WLAN ist immer wieder spannend und wird immer aktueller, was sich auch den Bemühungen vieler Kommunen erkennen lässt, kostenlose WLAN-Zugänge zum Beispiel vor Touristenattraktionen zur Verfügung zu stellen.

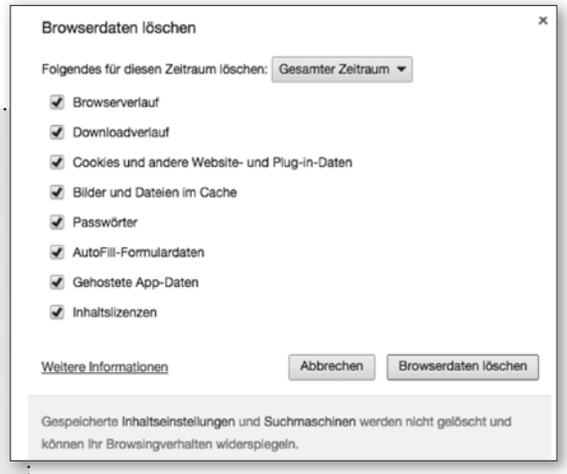
Hier finden Sie ein gutes Video vom WDR in der Sendung „Service-Zeit" zum Thema:
http://www1.wdr.de/fernsehen/ratgeber/servicezeit/sendungen/unsichere-hotspots-100.html

Online – was soll nicht in fremde Hände?

Arbeitest du an einem Computer, den mehrere Personen benutzen? Zu Hause oder in der Schule? Dann solltest du einige Dinge unbedingt wissen. Deine Browser (vom englischen „to browse“: blättern, schmökern), wie zum Beispiel der **Internet Explorer, Google Chrome, Safari** oder der **Mozilla Firefox**, sind ganz schön speicherwütig. Daten über dein Internet-Surfen werden von ihnen automatisch gespeichert. Vor allem Folgende:

- **Verlauf (oder auch Chronik)**
  Hier werden deine besuchten Seiten gespeichert. Der nächste Benutzer kann also sehen, welche Seiten du aufgerufen hattest.
- **Cookies**
  Cookies (vom englischen „Kekse“) sind kleine Dateien, die von Internetseiten auf deinem Computer abgelegt werden können. Darin kann stehen, wann du das letzte Mal auf der Seite warst, welche deine Lieblingsseite ist und vieles andere.
- **Passwörter**
  Die Browser ermöglichen es, Passwörter zu speichern, sodass du sie beim Aufrufen einer Internetseite nicht mehr eingeben musst. Diese Passwörter sind also auf dem Computer gespeichert.
- **Cache**
  Der „Cache“ ist ein Speicherplatz auf deinem Computer. Darin legt der Browser ganze Internetseiten ab, um darauf beim nächsten Aufruf schneller zugreifen zu können. Das war besonders notwendig, als es noch keine schnellen Internetverbindungen gab. Also sind ganze Seiten inklusive aller Bilder, Videos und Texte auf deinem Computer gespeichert.

Tipp: Die Browser ändern sich ständig, aber wenn du eine aktuelle Anleitung suchst, wie du die gespeicherten Daten löschen kannst, dann gib doch bei YouTube folgendes als Suchbegriffe ein: „browser daten löschen“. Hier findest du sicherlich eine Anleitung für deinen Lieblings-Browser!



Quelle: Screenshot klicksafe

Arbeitsaufträge:

1. Überlege und schreibe auf, warum diese Daten nicht in fremde Hände fallen sollten:

a. Verlauf

.....

b. Cookies

.....

c. Passwörter

.....

d. Cache

.....

2. Schaue nach, wie und wo du sie löschen kannst!

3. Kannst du einstellen, dass diese Daten automatisch beim Schließen gelöscht werden? Oder kannst du einstellen, dass die Daten gar nicht gespeichert werden (dies wird oft „privates Surfen“ oder ähnlich genannt)? Erkläre deiner Nachbarin/deinem Nachbarn, wie dies geht!

4. In deinem Handy passiert übrigens genau das gleiche. Abhängig von deinem Betriebssystem (zum Beispiel iOS, Android oder Windows) speichert dein Handy viele Daten darüber, wo du wann auf welchen Seiten im Internet warst. Findet euch in kleinen Gruppen mit dem gleichen Betriebssystem zusammen. Recherchiert, wie ihr die Spuren beim Internet-Surfen löschen könnt und probiert es aus! (Aber Vorsicht: Es gibt auch Einstellungen, alle Daten, also auch Adressen, Telefonnummern und Fotos etc. auf dem Handy zu löschen!)

Euer Funknetz – ist es sicher?

Funknetze oder auf Englisch „WLAN" – sind der absolute Renner in der digitalen Welt. Man findet sie mittlerweile überall: In Restaurants, auf Flughäfen, in Fußgängerzonen und im Fußballstadion – und vielleicht auch bei dir Zuhause?
Doch gerade bei Funknetzen kann viel passieren. So kann jemand in das Funknetz „einbrechen" und zum Beispiel alles lesen, was in deinem Computer / Handy gespeichert ist oder jemand kann das Funknetz „abhören" und möglicherweise die Passwörter stehlen, die man eingibt. Und weil es auch um deine Daten geht, darfst du mal jemandem (Mitschülerin / -schüler, Lehrerin / Lehrer, Nachbarin / Nachbar in deiner Straße …), der ein Funknetz zu Hause hat, ein paar unangenehme Fragen stellen.

Arbeitsaufträge:

1. Führe das Interview durch und notiere die Antworten in der dritten Spalte! Die richtigen Antworten findest du in der zweiten Spalte! Du darfst das Interview auch per Video (mit dem Handy) führen und der Klasse zeigen, wenn die interviewte Person das Einverständnis dazu gegeben hat.

Ist das Funknetz einbruchssicher? Wenn ja, wie?	Hier müssen die Begriffe WEP (ein altes, schlechtes System) oder WPA (gut!) fallen.	
Sendet es automatisch seinen Namen aus? (SSID genannt)	Jedes Funknetz hat einen Namen, der normalerweise ausgesendet wird. Dadurch kann z. B. Windows melden „Funknetz erkannt". Dies kann man abstellen, was sicherer ist, denn nun kann sich niemand automatisch einwählen.	
Ist der Name (SSID) verändert worden oder hat es noch den Standardnamen?	Normalerweise haben die Funknetze schon Namen wie die Firma (zum Beispiel „Netgear"). Besser ist ein eigener Name!	
Ist die Funkübertragung verschlüsselt?	Wie oben, hier gibt es zwei Systeme: WEP (schlecht) und WPA (gut!). Wer nicht verschlüsselt, der kann „abgehört" werden und riskiert, dass zum Beispiel seine Passwörter entschlüsselt werden.	
Mit welchem Passwort?	Wer sein Passwort verrät, hat nichts von Sicherheit kapiert ;-). Sofort ändern lassen!	
Benutzt es den MAC-Filter?	Jeder Computer (genauer die Netzwerkkarte) hat eine Kennung aus 12 Zahlen oder Buchstaben. Diese ist eindeutig und man kann ein Funknetz so einrichten, dass nur die bekannten Kennungen (die man vorher eingeben muss) hineindürfen.	

2. Klärt danach offene Fragen und erstellt schriftlich eine Checkliste auf der Rückseite des Arbeitsblattes, was ihr beachten müsst, wenn ihr in ein Funknetz geht.

3. Lies die Tipps sorgfältig. Arbeite mit einem Partner zusammen und erstelle dir einen kleinen Merkzettel mit Symbolen, der die genaue Größe deines Handys haben sollte!

- *WLAN immer ausschalten, wenn es nicht benötigt wird (spart auch Akku)*
- *Unterwegs kein Onlinebanking, Onlineshopping und auch kein facebook über das fremde WLAN!*
- *Datei- und Verzeichnisfreigabe in den Geräten deaktivieren*
- *Automatische Anmeldung an bekannten Hotspots deaktivieren! Hier gibt es böse Menschen, die öffentliche WLANs mit gleichem Namen vortäuschen, in Wahrheit aber Daten stehlen!*

Was wir immer tun sollten: Mindestschutz!
8_1 Kritisches Surfverhalten und Passwörter
8_2 WLANs und fremde Rechner
8_3 Digitaler Fußbabdruck
8_4 Datensicherung und -löschung

Digitaler Fußabdruck

Bei der großen Masse an täglichen Internetnutzern, verschwinden die Datenspuren einer einzelnen Person doch sicherlich so schnell, dass sich die meisten so gut wie anonym durch das Internet bewegen können. Und das Surfverhalten einer Privatperson erscheint auch eher uninteressant. Oder? Weit gefehlt: Unsere digitalen Datenspuren im Internet „Fußabdruck" zu nennen, ist eine fahrlässige Verharmlosung.
Es handelt sich eher um ganze Trampelpfade voller Daten.

Die zwei Links zeigen, was sich durch den harmlos wirkenden Aufruf einer Internetadresse über den Nutzer in Erfahrung bringen lässt:

www.anonym-surfen.com/anonym-surfen-test/

www.dein-ip-check.de/

Im Jahre 2013 machte der ehemalige Mitarbeiter der amerikanischen National Security Agency (NSA) Edward Snowden publik, in welchem Maße sein ehemaliger Arbeitgeber und damit die Vereinigten Staaten von Amerika (und übrigens auch Großbritannien) Internet-Daten auf Vorrat speichern. Unter dem Titel „NSA-Affäre" bzw. „NSA-Skandal" brachte er das Thema Datenschutz und staatliche Überwachungsmöglichkeiten der Telekommunikation in die politische und öffentliche Diskussion.[1]

Trotzdem bleibt der Ausflug ins Internet nur ein Teil des digitalen Trampelpfades. Beispielsweise weiß der Provider (also der Telekommunikationsanbieter) durch das Mitführen des Handys, wo sich seine Kunden gerade befinden. Durch die Zahlung mit EC-Karte wird dokumentiert, mit welcher Karte wo wie viel bezahlt wurde, bei der Nutzung von Kreditkarten oder einer Payback-Karte, sogar was gekauft wurde. An Bahnhöfen und Flughäfen stehen Videoüberwachungskameras, die eine Identifikation ermöglichen, jede Mautbrücke in Deutschland fotografiert das Nummernschild. Panopti.com veranschaulicht die „schöne neue Welt der Überwachung" und inwieweit der gläserne User schon Realität geworden ist:
www.panopti.com.onreact.com

Anonymität im Netz ist eine Illusion

Der Eindruck der Anonymität im Internet ist eine Illusion. Nutzer sind durch eine eindeutige Adresse (die sog. IP-Nummer) identifizierbar. Diese Nummer erhält jeder Rechner, der sich in das Internet einwählt. Der Internet-Provider erfasst diese Daten. Der Handy-Anbieter erfasst die sogenannten Verbindungsdaten (also nicht den Inhalt eines Gesprächs, aber die Information wann es wo wie lange mit wem geführt wurde). Das deutsche Bundesverfassungsgericht hat am 2. März 2010 die bis dahin angewendete Vorschrift zur Vorratsdatenspeicherung für nichtig erklärt.[2] Alle Provider mussten alle Daten löschen und durften diese Daten nur solange speichern, wie sie beispielsweise zur Abrechnung benötigt werden, also nur wenige Tage. Auch der europäische Gerichtshof hat in einem wichtigen Urteil im April 2014 die Praxis der Speicherung von Daten ohne konkreten Anlass gekippt.[3] Aller Kritik zum Trotz verabschiedete der Bundestag im Oktober 2015 erneut ein Gesetz zur umstrittenen Vorratsdatenspeicherung, das Telekommunikationsunternehmen verpflichtet, Daten ihrer Nutzer zu speichern.[4]

Cookies als Datensammelkrake

Die Betreiber von Webseiten speichern fast unbemerkt die Daten der Besucher, um damit Kundenprofile zu erstellen. Über kleine Dateien (sog. „Cookies") weiß der Anbieter sogar, wann die Nutzer das letzte Mal die Seite besuchten und welche Angebote sie besonders verlockend fanden.[5] In der Regel enthalten Cookies folgende Informationen:

- die eigene Lebensdauer
- den Namen des Servers, der den Cookie gesetzt hat
- die Unique-ID: eine einmalig vergebene Nummer, über die der Anbieter das Setzen des Cookies beim zweiten Aufruf wiedererkennen kann
- Inhaltsdaten, also alle anderen Informationen, die gespeichert sind, z. B. die Produkte, die der Nutzer sich im Online-Shop angesehen hat

Verantwortlich für die „Auto-Vervollständigen"-Funktion, beispielsweise bei der Eingabe von Anmeldedaten, sind „Flash-Cookies". Diese sind streng genommen keine Browser-Cookies, sondern Speicherungen des Programms „Adobe Flash Player"[6]. Diese Cookies können bis zu 25mal größer sein als „normale" http-Cookies, haben vor allem keine Laufzeitbegrenzung und sind browserunabhängig. Damit ist es also egal, mit welchem Browser ein Nutzer im Internet unterwegs ist, der Flash-Cookie ist schon da.[7] Es ist zudem etwas schwieriger diesen zu löschen. Dies funktioniert zwar nicht durch Einstellungen am Browser, aber beispielsweise über den online erreichbaren Einstellungsmanager des Adobe Flash Players: **www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager.html**

Die Cookie-Nachfolger
Neu ist eine andere Methode, die auf Cookies verzichtet und etwas lyrisch „Canvas-Fingerprinting" genannt wird. Etwas vereinfacht beschrieben, wird der Browser tatsächlich aufgefordert ein „Gemälde" (= engl.: „canvas") anzufertigen. Dieses kann auch als Code in Form von Zahlen und Buchstaben dargestellt werden und ist abhängig von einigen individuellen Merkmalen des Gerätes wie Betriebssystem, Browser, Grafikkarte, Grafiktreiber und installierte Schriftarten. Damit ist diese sehr einmalige Kombination ein gutes Merkmal der Wiedererkennung. Wird beim nächsten Mal die Seite mit „Canvas-Fingerprinting" aufgerufen, weiß der Anbieter von ihrem vorherigen Besuch. Diese Technik ist zur Zeit sehr schwierig zu unterbinden und wird schon als Cookie-Nachfolger bezeichnet.[8] Die Universität Leuven aus Belgien veröffentlicht eine Liste der Webseiten, die diese Technik benutzen: **https://securehomes.esat.kuleuven.be/~gacar/sticky/index.html#**

Der gläserne Nutzer ist längst Realität.

E-Mail und Browser
E-Mails können auf dem langen Weg durch das Internet abgefangen und gelesen werden. Die Betriebssysteme, die Browser und auch der Flash-Player oder „Silverlight" von Microsoft haben ein riesiges Gedächtnis. Sie speichern, wann sie welche Internetseite aufgerufen, welches Programm sie geöffnet haben und sogar die Inhalte der Internetseite mit Bildern, Texten und Videos. Und Daten im Papierkorb von Windows sind nichts weiter als verschoben und noch lange nicht gelöscht.

Facebook Like-Button
Sein positives Erscheinungsbild mag es zunächst nicht vermuten lassen, doch der bekannte „Gefällt mir"-Button (im englischen Original: „Like"-Button) ist beim Sammeln personenbezogener Daten ganz weit vorne. Zwar ermöglicht er einen durchaus positiv zu bewertenden Ausdruck von Anerkennung auf Knopfdruck, seiner Datensammelwut ist aber kaum zu entgehen.

Der Like-Button ist nicht einfach ein Bildchen mit einem dahinter stehenden Link. Auf der jeweiligen Internetseite wird ein sogenannter iFrame eingebunden. Darin versteckt sich in der eigentlichen Seite, der Code, der direkt von Facebook stammt. Beim Aufruf der Seite wird er automatisch gestartet, ohne dass der Like-Button angeklickt wurde. Im Klartext: Der Like-Button von Facebook wird aktiv beim Aufruf der Seite, nicht erst, wenn er angeklickt wird.[9]

Der Code, der hinter dem Like-Button steckt, sendet die URL (die Adresse) der geöffneten Internetseite an Facebook (Fachleute nennen das „Referer") und zusätzlich den Inhalt eines Cookies, der bei einem früheren Aufruf der Seite gesetzt wurde. Darin kann das Nutzungsverhalten auf dieser Seite gespeichert sein. Theoretisch könnte Facebook schon hier ein Benutzerprofil erstellen, schließlich weiß es, wann diese Seite vom gleichen (evtl. auch anonymen) Nutzer zuvor angeschaut wurde.

Nutzer, die beim Surfen im Internet nicht bei Facebook eingeloggt sind, sind dann nur über die IP-Adresse identifizierbar. Wer sich hinter dieser verbirgt, weiß zwar der Provider, aber nicht Facebook.
Aber Vorsicht: wer gleichzeitig noch in einem anderen Tab oder Fenster des genutzten Browsers bei Facebook eingeloggt ist, wird für Facebook eindeutig identifizierbar.

Ein Beispiel: Ein Nutzer ruft ein Nachrichtenportal mit Like-Button auf und recherchiert über die politischen Ereignisse. Ist zeitgleich Facebook geöffnet, dann weiß Facebook

- wer der Nutzer ist
- welche Seiten dieser aufruft
- über das Cookie das bisherige Nutzerverhalten auf diesen Seiten außerhalb von Facebook

Facebook erfährt also kostenlos eine Menge über das Nutzungsverhalten der Internetnutzer. Geliefert werden diese Daten von allen Seiten weltweit, die den Like-Button (oder andere aktive Facebook-elemente) enthalten. Anders als beispielsweise Google Analytics, kann Facebook diese Daten seinen konkreten Nutzern zuordnen.

Facebook-Nutzer surfen also nicht anonym auf Seiten mit Like-Button, auch wenn dieser nicht aktiv angeklickt wird.

Wenn nun noch der Button angeklickt wird, wird diese Zustimmung („Gefällt mir“) gezählt, taucht auf der Facebook-Seite des Nutzers auf, wird dessen Freunden mitgeteilt und kann von dem Inhalteanbieter zu Werbezwecken benutzt werden: „Willi gefällt das!“ Wem das zunächst harmlos vorkommt: Wer Inhalten von Greenpeace, Robin Wood und Foodwatch zustimmt, könnte u. U. später Probleme mit einer Bewerbung bei Chemie-Unternehmen oder in der Lebensmittelindustrie bekommen.

Aus der Praxis
Die weitreichenden technischen Möglichkeiten solcher harmlosen Spielereien im Internet sind vielen SchülerInnen nicht bewusst. Wichtig ist die Sensibilisierung für die möglichen Folgen von immer detaillierteren Profilen der eigenen Person in fremder Hand. Sind die Wirkmechanismen bekannt, ist die Einsicht für das Gefahrenpotenzial meist nicht weit.

Was tun?
Viele Datenschützer sehen die Praxis des Like-Buttons naturgemäß sehr kritisch. Nicht wenige von ihnen fordern, dass jeder Webseiten-Betreiber von dem Nutzer eine Zustimmung in Form einer Einverständniserklärung erhält, wenn personenbezogene Daten verarbeitet werden. Analog zu einer Datenschutzerklärung bei einer Anmeldung.

Einige Anbieter, wie der Verlag Heise mit dem Computermagazin c´t, sind Vorreiter für andere technische Wege: Sie haben eine 2-Button-Lösung etabliert. Dabei ist der Like-Button zunächst – beim Aufruf der Seite – inaktiv. Mit einem Mausklick auf den Like-Button wird er aktiviert und beim zweiten Mausklick wird er ausgelöst, d.h. der Inhalt erhält den Daumen noch oben, welcher gezählt wird.[10]

Kleine Zusatzprogramme für den Browser, sogenannte „Add-Ons“, verhindern das Laden des Buttons, wie z. B. ShareMeNot:

- für Firefox: **https://addons.mozilla.org/de/firefox/addon/sharemenot**
- für Chrome: **https://chrome.google.com/webstore/detail/sharemenot/peeecebkcdlibcfllbpmmkhggflcppem**

Wer sich schützen will, kann aber auch zwei verschiedene Browser nutzen: Einen für Facebook, den anderen zum Surfen. Zudem können nach jeder Sitzung alle Cookies gelöscht werden. Wem das Löschen aller Datenspuren des Browsers zu mühselig ist, kann auch eine Software dafür benutzen (System-Cleaner, siehe Link-Tipps). Wer sicher sein will, dass die Datenspuren aus Windows verschwinden, muss die temporären Ordner und den Papierkorb löschen. Jedoch sind die Daten leider auch nach dem Löschen im Papierkorb leicht wiederherstellbar. Profis empfehlen ein physikalisches Überschreiben auf der Festplatte, für das es bestimmte Verfahren gibt.

Anonymes Surfen

Weiterhin gibt es Angebote, die das anonyme Surfen im Internet ermöglichen, z. B. CyberGhost **www.cyberghostvpn.com/de** oder VTunnel **www.vtunnel.com**.
Oder man benutzt gleich einen Browser, der keine Daten speichert, wie z. B. Browzar **www.browzar.com** und /oder eine Suchmaschine, die verspricht keine Daten zu speichern: **https://startpage.com**.

Mögliche Probleme

Das anonyme Surfen im Internet hat selbstverständlich zwei Seiten, denn was einmal dem Datenschutz dient, kann beim nächsten Mal missbraucht werden. Durch die immer stärkere Vernetzung aller Lebensbereiche kann so auf technischem Wege auch viel Schaden anonym angerichtet werden. Zudem setzt die Benutzung verschiedener kleiner Helfer zur weitgehend anonymen Fortbewegung im Internet fast immer die Installation von Software voraus, was normalerweise an Rechnern in der Schule oder im Internet-Café nicht möglich ist. Also bleibt nur das Verwischen der Datenspuren per Hand.

Xbox, Smart-TVs und Apps

Auch andere Geräte haben einen enormen Datenhunger. So kann beispielsweise die Spielekonsole „Xbox One" von Microsoft mit Kinect-Erweiterung Gesichter erkennen und per Infrarot den Puls messen, Bewegungen erkennen und theoretisch so analysieren, ob die Nutzer ein Spiel oder einen Film gerade langweilig, lustig oder traurig finden.[11] Interessante Daten für die Anbieter. Sogenannte „Smart TVs", also Fernseher mit einer Internetverbindung, lösen das Dilemma der Einbahnstraße beim Fernsehen. Sie können erkennen (und weitergeben), welches Programm wann geschaut wird, ob schnell umgeschaltet wird etc. Die Sehgewohnheiten werden auf einem silbernen Tablett serviert. Bei den Zusatzfunktionen des Fernsehers werden auch diese Daten gespeichert. Und wie schon in Baustein 3_2 angesprochen, haben viele Apps weitgehende Zugriffsrechte auf die Standort-Daten, die Fotos, den Speicher des Handys oder auch auf Kamera und Mikrofon. Es kann aber Abhilfe geschaffen werden: bei der Xbox One kann der Kinect-Sensor ausgeschaltet oder einfach der Stecker abgezogen werden, die Internetverbindung des Fernsehers kann ausgeschaltet werden und bei den Apps sollten die Rechte stets kontrolliert werden.

Was wir immer tun sollten: Mindestschutz!
8_3 Digitaler Fußbabdruck
Links und weiterführende Literatur
Endnoten

Links und weiterführende Informationen

Webseiten

www.klicksafe.de/service/materialien/broschueren-ratgeber/datenschutz-tipps-fuer-eltern/
klicksafe-Flyer Datenschutz Tipps für Eltern

www.klicksafe.de/service/materialien/broschueren-ratgeber/datenschutz-tipps-fuer-jugendliche-so-sind-deine-daten-im-internet-sicher/
klicksafe-Flyer Datenschutz Tipps für Jugendliche

www.klicksafe.de/service/materialien/broschueren-ratgeber/klicksafe-youthpanel-flyer/
Flyer Tipps fürs digitale (Über)leben von den Jugendlichen des klicksafe Youth Panels

www.klicksafe.de/themen/datenschutz/privatsphaere/tipps-zur-digitalen-selbstverteidigung/
Tipps zur digitalen Selbstverteidigung, die helfen sollen, private Informationen zu schützen

www.computerwoche.de/a/anonym-surfen-so-geht-s,2524084
Hilfreicher Artikel mit Tipps, um beim Surfen anonym zu bleiben

www.chip.de/Downloads_13649224.html?tid1=38985&tid2=0
Übersicht auf Chip.de zu System Cleaner Software

Endnoten

[1] BEUTH, P. (2015). *Alles Wichtige zum NSA-Skandal.* zeit.de. Aufgerufen am 26.07.2015 unter http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal

[2] BUNDESVERFASSUNGSGERICHT. (2010, 02. März). *Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß*. Aufgerufen am 26.07.2015 unter http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011

[3] GERICHTSHOF der Europäischen Union. (2014, 08. April). *Pressemitteilung Nr. 54/14. Der Gerichtshof erklärt die Richtlinie über die Vorratsspeicherung von Daten für ungültig.* Aufgerufen am 26.07.2015 unter http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054de.pdf

[4] BUNDESRAT: Gesetzesbeschluss des Deutschen Bundestages (2015, 16.Oktober): *Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten.* Abgerufen am 8.12.2015, unter: http://dip21.bundestag.de/dip21/brd/2015/0492-15.pdf

[5] HUTHMACHER, J. (2014, 20. Juli). *Hallo, Datenkrake! Wie die Werbeindustrie mit Super-Cookies User-Stalking betreibt.* t3n.de. Aufgerufen am 26.07.2015 unter http://t3n.de/news/personalisierte-werbung-557831/

[6] www.adobe.com/software/flash/about

[7] PLUTA, W. (2010, 03. Mai). *Better Privacy löscht Flash-Cookies.* golem.de. Aufgerufen am 26.07.2015 unter http://www.golem.de/1005/74885.html

[8] BAGER, J. (2013, 21. Oktober). *Fingerprinting: Viele Browser sind ohne Cookies identifizierbar.* heise.de. Aufgerufen am 26.07.2015 unter http://www.heise.de/security/meldung/Fingerprinting-Viele-Browser-sind-ohne-Cookies-identifizierbar-1982976.html

[9] WIESE, J. (2011, 08. September). *Breaking! Facebook Papier erklärt: so funktioniert der Like-Button in Deutschland.* allfacebook.de. Aufgerufen am 27.06.2015 unter http://allfacebook.de/news/breaking-facebook-papier-erklart-so-funktioniert-der-like-button-in-deutschland

[10] SCHMIDT, J. (2011, 01. September). *2 Klicks für mehr Datenschutz.* heise.de. Aufgerufen am 25.6.2015 unter http://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html

[11] CHIP.DE. (2013, 04. November). *Xbox One Kinect: Diese Daten sammelt Microsoft*. Aufgerufen am 25.07.2015 unter http://www.chip.de/news/Xbox-One-Kinect-Diese-Daten-sammelt-Microsoft_65235281.html

Methodisch-didaktische Hinweise

Arbeitsblatt	**AB 1**	**AB 2**
Titel	**Digitale Datenspuren im Alltag**	**Hat das Internet ein Gedächtnis?**
Kompetenzen	Die Schülerinnen und Schüler übertragen ein fiktives Beispiel eines Tages ohne Datenspuren in Form einer Reportage auf die Realität und erfassen, an welchen Stellen der Autor Datenspuren hinterlassen hätte.	Die Schülerinnen und Schüler führen eine Internet-Recherche über das digitale Archiv www.archive.org durch und reflektieren über das Für und Wider der dauerhaften Speicherung digitaler Daten.
Methoden	Textanalyse, Vorlesen, Partnerarbeit	Pro- und Contra-Tabelle, Einzelarbeit, Unterrichtsgespräch, Textanalyse
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	45	90
Zugang Internet/PC	Nein (Ja, bei Recherche zur Qualität der Daten)	ja

Hinweise für die Durchführung

AB 1: Digitale Datenspuren im Alltag

An einem Text, der einen Selbstversuch schildert, einen Tag ohne Datenspuren zu verleben, sollen die Schülerinnen und Schüler erfahren, wie wir alltäglich (digitale) Datenspuren hinterlassen. Danach sollen sie dies auf ihre eigene Situation übertragen.
Mit diesem Arbeitsblatt sollen die Schülerinnen und Schüler für die (digitalen) Datenspuren im Alltag sensibilisiert werden. Ein Einstieg könnte über die Frage erfolgen, wer alles weiß, dass die Schülerin / der Schüler jetzt und hier ist. Etwa: Wer weiß, dass du jetzt hier bist? Neben – hoffentlich – den Eltern könnten dies ihre Mobilfunkanbieter, über die Ortungsfunktionen WhatsApp und Facebook oder ähnliche Anwendungen sein oder sogar die Polizei, wenn auf dem Schulweg eine Kamera zur Überwachung des öffentlichen Raumes installiert ist.
Lassen Sie den Text von einem guten Leser / einer guten Leserin vorlesen oder tun sie es selbst, vielleicht mit etwas Dramatik und Spannung in der Stimme. Die anschließende Phase der ersten Eindrücke könnten Sie wie die Methode „Blitzlicht" durchführen, also Meldungen ohne Kommentare der anderen oder auch die Meldungen direkt zur Diskussion stellen.
Das Beispiel aus der Berufswelt eines Erwachsenen enthält einige Merkmale, die für Kinder und Jugendliche (noch) nicht relevant sind, so Zeiterfassungssysteme, Mautbrücken oder Kreditkarten. Nichtsdestotrotz ist es ein alltägliches Beispiel, das in dieser Form vielleicht den Eltern passieren kann. Die Auflistung der Datenspuren fällt sicherlich leicht, eine genaue Auflistung der erhobenen Daten finden Sie in den Sachinformationen (so werden beim Handy die Verbindungsdaten, aber nicht die Inhalte gespeichert, ebenso beim E-Mailing oder SMS).
Sie könnten den Einstieg wieder aufgreifen und das Beispiel auf die eigene Alltagssituation übertragen lassen und deutlich machen, inwieweit auch Kinder und Jugendliche Datenspuren im Alltag hinterlassen. Die Idee für eine Vertiefung ist als Vorschlag für interessierte Schülerinnen / Schüler zu verstehen und mit einem positiven Ergebnis nur sehr schwierig zu realisieren (es ist fast unmöglich, keine Datenspuren zu hinterlassen!).

AB 2: Hat das Internet ein Gedächtnis?

Das digitale Archiv ist Thema dieses Arbeitsblattes. Darin werden frühere Versionen von Internetseiten gespeichert. Im zweiten Arbeitsauftrag werden die Schülerinnen und Schüler mit der These konfrontiert, dass auch für digitale Daten ein Verfallsdatum eingeführt werden sollte. Dies sollen die Jugendlichen als Pro und Contra gegenüberstellen.
Zum Schluss schließlich wird auf die Tatsache eingegangen, dass viele Jugendliche heute sehr freizügig mit ihren Daten im Internet umgehen. Sie sollen sich vorstellen, wie es wäre, wenn diese Daten (Beschreibungen, Fotos, Videos, Forenbeiträge) in zehn Jahren in die Hände anderer Menschen (angegeben sind Beispiele) fallen. Dies kann sehr peinlich sein.

Lust auf mehr?

- Seit 2014 gibt es auch gegenüber Google ein „Recht auf Vergessen". Der Europäische Gerichtshof entschied, dass Google auf Antrag Suchergebnisse löschen muss (Das Original-Urteil ist hier zu finden: **http://bit.ly/U6yFxH**). Vielleicht gibt dieses Thema Anregung für ein interessantes Referat eines Schülers / einer Schülerin.
- Schon 2008 hat der Journalist Christoph Drösser in der Zeitung „DIE ZEIT" einen Artikel mit dem Titel „Das digitale Alexandria" geschrieben. Die Schüler lesen den Artikel und fassen ihn in eigenen Worten zusammen: **www.zeit.de/2008/04/OdE13-Wissen**

Geht das? Ein Tag ohne Datenspuren?

Der Wecker klingelt. Es ist 6:45 Uhr. Zeit zum Aufstehen, aber da war doch was? Mein Gehirn arbeitet fieberhaft und kämpft gegen den letzten Traum und den Wunsch weiterzuschlafen … ach ja … heute ist der Tag, an dem ich keine Datenspuren hinterlassen möchte. Ich stehe auf. Darf ich das Radio einschalten? Ja, denn niemand erfährt, ob ich es eingeschaltet habe. Darf ich Kaffee kochen? Ja, ein Glück! Ich möchte gerne auf mein Handy schauen und die Nachrichten lesen. Aber das geht nicht, dann wird gespeichert, dass ich sie gelesen habe. Außerdem darf ich mein Handy ja gar nicht einschalten, zum Glück habe ich gestern den Akku rausgenommen. Normalerweise rufe ich auch mein E-Mails ab vor dem Gang ins Büro, aber … das darf ich heute nicht, denn mein Login ins Internet wird notiert. Also los, auf ins feindliche Leben draußen. Ach … M i s t … ich darf das Auto nicht benutzen! Das hatte ich ganz vergessen. Dann werde ich zu spät kommen. Auf den Straßen gibt es Überwachungskameras für den Verkehr und ich möchte ja heute keine Datenspuren in Form von Videos hinterlassen. Und außerdem sendet das Auto ja über die Blackbox Infos über mein Fahrverhalten an meine Kfz-Versicherung. Ich hätte auch nicht auf die Autobahn fahren dürfen – unter Mautbrücken werden die Nummernschilder fotografiert, von jedem Auto! Ich schleiche mich also mit meinem Fahrrad aus dem Haus. Am Bahnhof darf ich nicht vorbeifahren, dort hängt eine Kamera. Endlich im Büro, darf ich die Zeitstempeluhr nicht benutzen (Datenspuren, wann ich wo war!), ich sage später, ich hätte es vergessen. Den Computer darf ich anmachen … oder? Nein, besser nicht, denn auch dort gibt es Protokolldateien im Netzwerk der Firma. Darf ich telefonieren? Auch nicht … M I S T … natürlich weiß die Telefongesellschaft, von welchem Apparat aus wohin wann und wie lange angerufen wird! Mein Handy? SMS? WhatsApp? Keine Chance! Derselbe Datenspeicherwahn. Besser, ich sage, dass ich mich krank fühle, denn arbeiten kann ich sowieso nicht. Ich schleiche also wieder zurück nach Hause, mit Angst davor, gefilmt zu werden. Eigentlich wollte ich noch einkaufen, aber … Kameras in jedem Laden … ich bräuchte auch noch Geld vom Automaten … Daten, Daten, Daten, die gespeichert werden. Meine Kreditkarte? Ein einziger Daten-Horror! Kein Risiko heute. Ich hole mir noch eine Flasche Wasser am Kiosk und zahle in bar. Hatte der Besitzer einen Fotoapparat an der Wand? Oder fange ich schon an zu spinnen? Zu Hause angekommen, schalte ich den Fernseher ein (darf ich …? Bei Satellitenempfang ja, bei Kabelempfang nein – zum Glück habe ich eine Schüssel), ziehe die Vorhänge zu und setze mich auf meine Couch. Ein toller Tag, so ganz ohneDatenspuren, oder?

Arbeitsaufträge:

1. Bitte lest die Reportage laut in der Klasse vor! (Vielleicht gibt es einen tollen Vorleser?!)
2. Was fällt euch dazu ein? Bitte sprecht über eure Eindrücke beim Zuhören.
3. Arbeitet dann in Partnerarbeit. Erstellt eine Liste, wo der Erzähler an einem normalen Tag Datenspuren hinterlässt.

Lust auf mehr?

Kannst du einen Tag verbringen, ohne Datenspuren zu hinterlassen? Schreibe einen Bericht über einen solchen Tag!

Hat das Internet ein Gedächtnis?

Der Amerikaner Brewster Kahle hatte schon zu Beginn des Internets in seiner heutigen Form einen Traum: Er wollte ein digitales Archiv schaffen und das Internet archivieren. Unmöglich? Seit 1996 sammelt sein „Internet-Archiv" (**www.archive.org**), und hatte bis 2014 über 18 Petabyte (das sind 18.000.000.000.000.000 Byte) archiviert, das in vier Rechenzentren auf 20.000 Festplatten gespeichert ist. Sein Internet-Archiv steht (allerdings mit Spiegelservern zum Beispiel in Kairo) in San Francisco und ist mittlerweile offiziell als Bibliothek von Kalifornien anerkannt. Mit einer speziellen Software werden Momentaufnahmen von Webseiten gespeichert. Auf diese Weise sind über 400 Milliarden Seiten (für immer?) zugänglich.

*Mit der „Wayback-Machine" kann man sich z. B. die Seiten von **www.klicksafe.de** anschauen. Über eine Datumsliste kann auf die gespeicherten Seiten zugegriffen werden.*

*Hier findest du eine Video-Dokumentation über das Archiv: **https://vimeo.com/59207751** (auf Englisch).*

Arbeitsaufträge:

1. Begib dich auf eine digitale Zeitreise und rufe frühere Versionen von Webseiten auf. Du darfst private, bekannte oder auch die Schulhomepage nehmen. Vergleiche die alte und die aktuelle Version. Was fällt dir auf?

2. Es gibt immer wieder die Forderung nach einem „Recht auf Vergessen", also der Möglichkeit, digitale Daten auch wieder (endgültig) löschen zu dürfen.
   Lies nun folgende Artikel in der Zeitschrift „Heise" mit einer Pro- und Contra-Diskussion zu diesem Thema und aus der Zeitung „Die Zeit" mit der Idee des „digitalen Radiergummis":

   http://www.heise.de/newsticker/meldung/Pro-Contra-Das-Recht-auf-Vergessen-im-Internet-2189293.html

   http://www.zeit.de/digital/datenschutz/2011-01/radiergummi-vergessen-schoenberger

   Erstelle eine Liste mit den Vor- und Nachteilen eines „Rechts auf Vergessen". Diskutiert diese Forderung anschließend in der Klasse. Bewertet die Argumente und ergänzt eure eigene Liste. Zu welchem Ergebnis kommst du persönlich? Begründe!

3. Stelle dir vor, in zehn oder zwanzig Jahren stoßen folgende Menschen auf die Dinge (z. B. Fotos, Foren-Einträge, Texte, Bilder, Videos), die du heute im Internet hinterlassen hast:

   Welche Folgen könnte das für dich haben! Schreibe sie in einer Tabelle auf!

a. deine Mutter / dein Vater	
b. deine Ehefrau / Partnerin	
c. deine Kinder	
d. dein Arbeitgeber	
e. deine (wichtigen) Kunden	
f. deine Arbeitskollegen	

Was wir immer tun sollten: Mindestschutz!
8_1 Kritisches Surfverhalten und Passwörter
8_2 WLANs und fremde Rechner
8_3 Digitaler Fußbabdruck
8_4 Datensicherung und -löschung

Datensicherung und -löschung

Die Zukunftsfrage

Was passiert eigentlich heute mit einem Datenträger, der vor 20 Jahren z. B. mit Urlaubsbildern beschrieben wurde? Kann er noch problemlos gelesen werden oder scheitert es schon an den passenden Geräten? Kann das Dateiformat noch verarbeitet werden? Genau vor diesem Problem werden Nutzer in Zukunft immer wieder stehen. Große Institutionen wie Museen oder das Bundesarchiv (🌐 w**ww.bundesarchiv.de**) lösen das Problem heute mit großen Computern („Servern") und dem Hin- und Herkopieren der Daten sowie der regelmäßigen Aktualisierung. Für den Normalanwender bleibt auch keine andere Möglichkeit, als wichtige Daten mit neuer Soft- und Hardware zu aktualisieren.

Die Haltbarkeit

Sollte sich jemand dazu entschließen mehrere alte Computer auf den Speicher zu stellen und die 3,5-Zoll-Diskette der 1980er, die CDs, das ZIP-Laufwerk und den USB-Stick der 1990er, die SD-Memory-Card seit dem Jahre 2001, ebenso wie die DVDs oder Blu-ray Discs mit den wertvollen Datenschätzen daneben, so bleibt trotzdem das Problem der eingeschränkten Haltbarkeit.
Nach heutigen Erkenntnissen halten beispielsweise CDs und DVDs, je nach Lagerung, vielleicht nur 25 Jahre, bei Blu-ray-Discs könnten es 50 Jahre und mehr sein. Da diese erst 2002 vorgestellt wurden, wird die tatsächliche Haltbarkeit aber erst ab ca. 2052 festzustellen sein.

Aus der Praxis
Besonders anschaulich wird es, wenn die SchülerInnen einen Zeitstrahl der wichtigsten technologischen Innovationen erstellen sollen. Dieser sollte bis in das Altertum reichen und es sollte sich um maßstabsgerechte Jahresabstände bemüht werden, dann wird die Dynamik seit dem 19. Jahrhundert sehr deutlich!

Flash-Speicher ohne bewegliche Teile

Wie man es auch wendet: digitale Daten müssen auf Speichermedien archiviert werden und dazu lohnt ein Blick auf die Art und Weise, wie diese arbeiten. Vereinfacht gesagt enthalten Festplatten (Hard Disk Drive oder HDD) eine magnetische Platte, die rotiert, und einen Schreib-Lese-Kopf, der darüber fährt und die Daten ausliest. Diese Technik ist unabhängig von der Schnittstelle (also zur Zeit IDE, SATA, SCSI) und kam auch in den Floppy-Disks (den „alten" Disketten) zum Einsatz. Diese Technik ist auf Dauer störanfällig, weil sie viele bewegliche Teile enthält. Besser geeignet zur Datenspeicherung sind sogenannte „Flash-Speicher" (nicht zu verwechseln mit der gleichnamigen Software der Firma Adobe!). Sie finden Einsatz in USB-Sticks und SD-Karten, aber auch als Festplatten-Ersatz in Computern und heißen dann SSD (Solid State Drive). In ihnen befinden sich keine mechanischen Teile und sie behalten die Daten dauerhaft (nach Herstellerangaben etwa 10 Jahre) auch ohne Stromversorgung.[1]

Die Haltbarkeit eines Flash-Speichers ist abhängig von den Schreib- und vor allem den Löschzyklen, die von den großen Herstellern mit mind. 100.000 garantiert werden. Der USB-Stick kann also ohne weiteres 100.000 Mal beschrieben werden. Nutzt man ihn als Datenspeicher, so hält er besagte 10 Jahre ohne Strom und 100.000 Schreibvorgänge lang. Wie lange tatsächlich kann noch keiner sagen, denn die ersten Sticks kamen erst im Jahre 2000 auf den Markt.[2] So oder so: Um das Herumkopieren der wichtigsten Daten kommt man auch mit Flash-Speichern nicht herum.

Was tun?
Wirklich wichtige Daten sollten regelmäßig auch außerhalb des eigentlichen Computers / Handys / Tablets gesichert werden. Dies kann man über Software (Backup- oder Synchronisier-Programme) automatisieren. Dabei ist es keine schlechte Idee, dazu zwei voneinander unabhängige Systeme (zum Beispiel eine herkömmliche Festplatte und einen Flash-Speicher und /oder CD / DVD) zu verwenden. Und es führt kein Weg daran vorbei, diese Daten, vielleicht einmal im Jahr, neu zu überspielen und dem Stand der Technik anzupassen.

Die Routine
Nun ist es sehr schwierig, den richtigen Rhythmus für eine Speicherung zu finden (täglich? wöchentlich? monatlich?) und auch jedes Mal daran zu denken. Sinnvoll ist eine automatisierte Sicherung, für die es wiederum eine Vielzahl kommerzieller Softwareprodukte gibt. Folgende Tipps helfen bei der Datenlagerung:

- Von Zeit zu Zeit überprüfen, ob die Daten mit der vorhandenen Software noch lesbar sind.
- Daten umkopieren und mit der entsprechenden Software in neuere Datenformate überführen. Faustregel: spätestens alle 5 Jahre, besser nach 2 – 3 Jahren.
- Optimale Lagerbedingungen: trocken, kühl (nicht über Zimmertemperatur), kein direktes Sonnenlicht, mehrere Kopien an verschiedenen Orten aufbewahren.
- Die Dokumentation nicht vergessen (z. B. Lagermedium aussagekräftig und mit Datum beschriften)!

Backup-Methoden
Die Experten unterscheiden zwischen verschiedenen Speichermethoden[3]:

- Volldatensicherung (alle Daten werden gespeichert)
- Inkrementelle Datensicherung (nach einer Volldatensicherung werden nur geänderte Daten erneut gespeichert, danach jeweils nur die Dateien, die seit der letzten inkrementellen Sicherung geändert wurden)
- Differenzielle Datensicherung (ähnlich der inkrementellen, es werden jedoch alle, seit der letzten Volldatensicherung geänderten Dateien erneut gespeichert)

Der Vorteil der differenziellen Datensicherung ist, dass im Bedarfsfall nur zwei Versionen der Speicherung benötigt werden: Die Volldatensicherung und die letzte differenzielle Datensicherung. Bei einer inkrementellen Sicherung bedarf es aller Speicherversionen. Eine Wiederherstellung ist bei differenzieller Sicherung unkomplizierter, allerdings benötigt diese Variante auch mehr Speicherplatz.

Wolkige Aussichten
Eine weitere Alternative zur Datensicherung bietet ein gemieteter, online zugänglicher Speicher, auch „Cloud" (engl. „Wolke") genannt. Dieser bietet zudem noch einige Vorteile, wie die ortsunabhängige Verfügbarkeit und automatische Synchronisation mit verschiedenen Geräten. Anbieter von Cloud-Speichern arbeiten mit redundanten Systemen (die Festplatten sind also gespiegelt) und mit allerlei Vorkehrungen gegen Datenverlust (Strom-Sicherungen etc.), so dass i. d. R. davon ausgegangen werden kann, dass die Daten dort erhalten bleiben.

Datensicherheit in der Cloud
Hier stellt sich allerdings das Problem der Datensicherheit. Also: wie gut sind die Daten vor fremden Zugriff geschützt? Cloud-Anbieter haben mitunter Computerstandorte in anderen Ländern, wie den U. S. A., die andere gesetzliche Regelungen haben. Diese erlauben u. U. einen Zugriff auf die gespeicherten Daten, der durch deutsche Datenschutzgesetze nicht möglich wäre.
Ein weiteres Problem ist die Übertragung der Daten auf dem Weg in die Cloud. Hier könnten die Daten „abgefangen" werden. Hochsensibel sind die Hochseekabel, die die Internetdaten beispielsweise über den Atlantik schicken.

Folgende Herausforderungen stellen sich für Cloud-Lösungen:

- Nutzer wissen einfach nicht mehr genau, wo ihre Daten gespeichert sind und kennen keine Administratoren, die einen uneingeschränkten Zugriff darauf haben.
- In einer Cloud können Nutzer Zugriffsrechte an Dritte vergeben, was schnell unübersichtlich werden kann.
- Nutzer wissen nicht, wie die Daten gelöscht werden. Digitale Daten auf Festplatten werden nicht wirklich physisch vernichtet und sind im Zweifelsfall wiederherstellbar. Nicht umsonst ist das sichere Löschen von Daten ein großes Problem.
- Nutzer können nicht einschätzen, wie sicher ihr Speicherplatz vor dem (unberechtigten) Zugriff des Nachbarn ist, von Hacker-Angriffen ganz zu schweigen.
- Sollte die Internetverbindung auf Seiten des Nutzers oder des Cloud-Anbieters ausfallen, gibt es keine Chance auf die Daten zuzugreifen.
- Im Falle einer Insolvenz oder eines Verkaufs mit Zerschlagung des Cloud-Anbieters könnten die Server eventuell beschlagnahmt und / oder verkauft werden, ohne dass Nutzer eine Eingriffsmöglichkeit haben.
- Die unterschiedlichen Gesetze, die andere Zugriffsmöglichkeiten von Polizei und Geheimdiensten ermöglichen, sind meist weit entfernt von den deutschen Datenschutz-Standards.

Was tun?

Spezielle Software, wie z. B. „Boxcryptor“[4], ermöglicht eine technisch sehr einfache Verschlüsselung der Daten auf dem Weg zur Cloud und innnerhalb der Cloud. Dies wäre eine einfache Möglichkeit, seine Daten zu schützen. Außerdem sollte bei der Auswahl eines Cloud-Anbieters vor allem bei sensiblen Daten auf einen seriösen Anbieter geachtet werden, am besten einen deutschen mit Servern in Deutschland. Die Daten sollten unbedingt verschlüsselt abgespeichert und übertragen werden.

ISO 27001

Wer auf Nummer sicher gehen möchte, sieht sich nach Unternehmen um, die eine Zertifizierung nach dem ISO-Standard 27001 haben. Darin festgelegt sind zahlreiche Kriterien zur Sicherheit von Informationssystemen und die Anbieter garantieren den IT-Grundschutz.[5] Weitere Informationen dazu bietet das Bundesamt für Sicherheit in der Informationstechnik (siehe Linkübersicht).

Daten sicher löschen

Das Gegenteil der Datensicherung ist ähnlich schwierig: Die Daten sicher zu löschen! Lehrerinnen und Lehrer dürfen nicht ohne weiteres Schülerdaten wie Namen, Noten, Fotos usw. auf den heimischen Rechnern verarbeiten (siehe Baustein 9). Besonders vorsichtig sollte man deshalb mit einem Computer sein, der diese sensiblen Daten enthält (Virenschutz und Firewall und eigene Benutzerkonten für alle Nutzer sollten selbstverständlich sein). Aber was ist mit dem Löschen dieser Daten? Was ist, wenn der Computer ausgedient hat und die Festplatte gelöscht werden muss? Ein einfaches Löschen des installierten Betriebssystems bietet hier nicht die ausreichende Sicherheit, da die Daten nicht physikalisch von der Festplatte gelöscht werden und ein Spezialist sie jederzeit wiederherstellen könnte. Sicherheit bietet die sogenannte „Gutmann-Methode“ (benannt nach ihrem Entwickler, dem neuseeländischen Wissenschaftler Peter Gutmann), bei der die Daten auf der Festplatte 35mal nach einem Zufallsprinzip überschrieben werden. Es gibt einige kostenlose Programme, die diese Aufgabe übernehmen.[6]

Es sollte keine Festplatte, keine Disc und kein USB-Stick in fremde Hände gelangen. Wer seinen Computer verkauft oder weitergibt, sollte die Festplatte vorher ausbauen und physisch zerstören.

Links und weiterführende Informationen

Webseiten

www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzZertifikat/itgrundschutzzertifikat_node.html
Informationen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu ISO 27001

www.it-sicherheit.de/ratgeber/it_sicherheitstipps/tipp/sicheres-speichern-und-lo776schen-ihrer-daten/
Ausführlicher Artikel mit Tipps zum Speichern und Löschen von Daten

Endnoten

[1] BUNDESAMT für Sicherheit in der Informationstechnik (BSI). (2015). *Speichermedien.* Aufgerufen am 25.07.2015 unter https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Datensicherung/Speichermedien/speichermedien_node.html

[2] FEDDERN, B. & Benz, B. (2007). *Flash-Haltbarkeit.* In c't, 02/2007. Aufgerufen am 25.07.2015 unter http://www.heise.de/ct/hotline/Flash-Haltbarkeit-296140.html

[3] BUNDESAMT für Sicherheit in der Informationstechnik (BSI). (2015). *Methoden der Datensicherung.* Aufgerufen am 26.07.2015 unter https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Datensicherung/Sicherungsmethoden/sicherungsmethoden_node.html

[4] www.boxcryptor.com

[5] BUNDESAMT für Sicherheit in der Informationstechnik (BSI). (2015). *ISO 27001 Zertifizierung auf Basis von IT-Grundschutz.* Aufgerufen am 27.07.2015 unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzZertifikat/itgrundschutzzertifikat_node.html

[6] CHIP.DE. (2012, 31. August). *Festplatten löschen: Daten komplett entfernen.* Aufgerufen am 26.07.2015 unter http://www.chip.de/artikel/PC-Cleaner-kostenlos-Computer-saeubern-ganz-einfach-2_46706321.html

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Und in 1000 Jahren?**	**Daten für die Ewigkeit**
Kompetenzen	Die Schülerinnen und Schüler übertragen den Beginn einer Fantasiegeschichte über die Speicherung von Daten auf eine eigene Fortführung der Geschichte.	Die Schülerinnen und Schüler vergleichen die Speichermöglichkeiten ausgewählter Medien und übertragen die Kenntnisse in eine grafische Übersicht.
Methoden	Schreibwerkstatt (versch. Möglichkeiten: Cluster, Fließband-Geschichte, Demokratie, Zeitung), Gruppenarbeit, Textanalyse	Tabelle, Internet-Recherche
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	nein	Ja

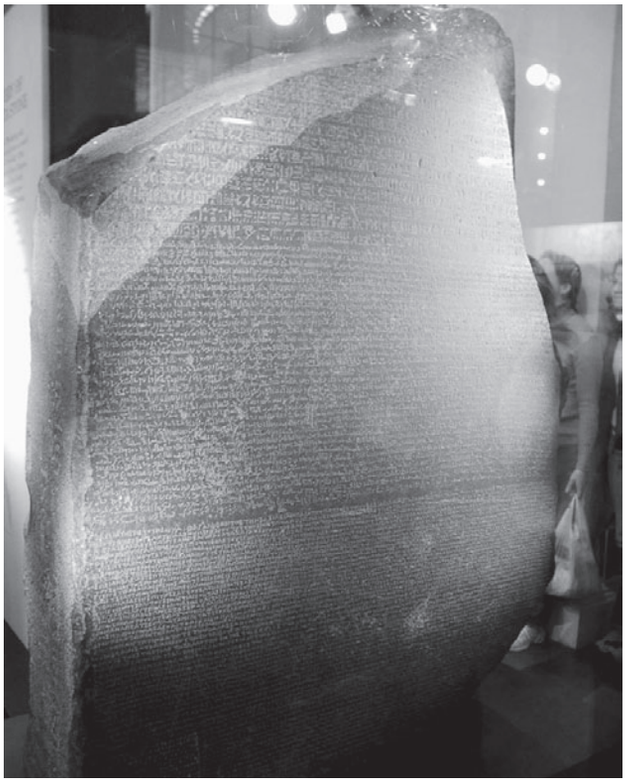
Hinweise für die Durchführung

AB 1: Und in 1000 Jahren?	Mit diesem Arbeitsblatt sollen sich die Schülerinnen und Schüler kreativ mit dem Problem der Datensicherung auseinandersetzen. Den Aufhänger bietet der „Stein von Rosetta" (siehe Informationen auf dem Arbeitsblatt), mit dessen Hilfe die ägyptischen Hieroglyphen übersetzt werden konnten. Die Schülerinnen und Schüler sollen eine Science-Fiction-Geschichte weitererzählen, wenn jemand in 2000 Jahren eine CD von heute findet. Die Methode der „Schreibwerkstatt" soll ein strukturiertes Arbeiten ermöglichen. So ist das „Clustern" eine eher kreativ-chaotische Methode, die sehr viel Spaß macht. Weitaus anstrengender, aber nicht weniger lustig, ist die „Fließband-Geschichte", da dort immer wieder auf die Fortführungen der anderen Gruppenmitglieder reagiert werden muss. In sehr gut funktionierenden Gruppen eignet sich die Form „Demokratie", wo jeder etwas schreibt und gemeinsam entschieden wird. Etwas stringenter ist „Zeitung", da dort die Form einer Zeitungsmeldung eingehalten werden muss. Vielleicht lassen Sie die Gruppen selbst entscheiden, welche Form sie wählen.
AB 2: Daten für die Ewigkeit	Auf der „Sound of Earth" ist folgendes gespeichert: „Der Anfang der Datenspur enthält 115 analog gespeicherte Bilder. Der Rest besteht aus Audiodaten. Dazu gehören gesprochene Grüße in 55 verschiedenen Sprachen (deutscher Text: „Herzliche Grüße an alle") sowie verschiedene Töne wie Wind, Donner und Tiergeräusche. Darauf folgen 90 Minuten ausgewählter Musik, neben ethnischer Musik auch bekannte Titel von Johann Sebastian Bach, Wolfgang Amadeus Mozart, Chuck Berry (mit dem Titel Johnny B. Goode) und anderen. Zusätzlich zu den Grüßen in verschiedenen Sprachen befindet sich neben einer geschriebenen Nachricht des U. N. Generalsekretärs Kurt Waldheim auch noch eine von US-Präsident Jimmy Carter: „This is a present from a small, distant world, a token of our sounds, our science, our images, our music, our thoughts and our feelings. We are attempting to survive our time so we may live into yours." („Dies ist ein Geschenk einer kleinen, weit entfernten Welt, Beispiele unserer Geräusche, unserer Wissenschaft, unserer Bilder, unserer Musik, unserer Gedanken und unserer Gefühle. Wir hoffen, unser Zeitalter zu überleben, so dass wir ihres erleben können.") (Quelle: http://de.wikipedia.org/wiki/Sounds_of_Earth). Man darf gespannt sein, welche Erkenntnisse die Außerirdischen daraus ziehen.

Lust auf mehr?

- Das Thema Daten in der Cloud kann zusätzlich behandelt werden. Lassen Sie die Schüler hierzu recherchieren. Beispielsweise: „Was bedeutet Clouding?", „Welche Dienste bieten es an?", „Wo werden die Daten gespeichert?", „Wo liegen die Risiken?", „Wie können die Daten in einer Cloud zusätzlich geschützt werden?" etc.
- Auf einer ganz anderen Ebene ist die spannende Frage, was aus unserer digitalen Zeit als kulturelles Erbe übrig bleibt … oder – etwas praktischer – was würden wir heute auf eine „Sound of Earth"-CD spielen?

Und in 1000 Jahren?



Der Stein von Rosetta ist knapp 115 Zentimeter groß, wiegt aber über 750 Kilogramm. Er ist rund 2200 Jahre alt, steht im Britischen Museum in London, und noch immer kann man seine Inschrift lesen. Seine Erschaffer haben darin einen Text in drei Sprachen hinterlassen und mit seiner Hilfe konnte man die ägyptischen Hieroglyphen entziffern.

Quelle: http://upload.wikimedia.org/wikipedia/commons/8/89/Rosetta_stone.jpg

Stelle dir das mal mit einer CD von heute vor!
Stelle dir vor, sie wird in 2000 Jahren gefunden!

Arbeitsauftrag:
Schreibe folgende Geschichte weiter!

Minux7 war ein Kind wie alle anderen, sein Computerchip im Kopf unterschied sich kein bisschen von denen seiner älteren Geschwister **Minux1** bis **Minux6** und seiner jüngeren, **Minux8** bis **Minux11**. Aber trotzdem war **Minux7** anders, er hatte diese Liebe zu allen Dingen, die alt waren. Und beim letzten Besuch der Erde war er doch aus der Überlebenskuppel herausgeschlichen und hatte in einem Bernsteinblock ein glänzendes rundes Ding von ungefähr 34 kyrometer (er wusste, das waren früher einmal 12 Zentimeter oder so ähnlich!) gefunden. Ganz undeutlich stand etwas darauf, aber das konnte er beim besten Willen nicht ohne seinen Sprachenchip „1000 Jahre und älter" entziffern. Zurück auf dem Mars wollte er das Rätsel lösen. …

Ihr dürft dazu eine **„Schreibwerkstatt"** durchführen. Findet euch in 4er-Gruppen zusammen und sucht euch eine der folgenden Formen aus:

A **Clustern.** Jeder schreibt spontan auf, was ihm dazu einfällt. Danach werden die Ideen sortiert und gemeinsam wird am Text weitergeschrieben

B **Fließband-Geschichte.** Einer beginnt mit einem Satz, der nächste schreibt weiter und so weiter

C **Demokratie.** Jeder schreibt den nächsten Satz der Geschichte, alle werden vorgelesen und danach wird gemeinsam ausgesucht, welcher am besten ist, dieser wird verwendet. Dann der nächste Satz…

D **Zeitung.** Ihr schreibt die Geschichte wie einen Zeitungsartikel.

Daten für die Ewigkeit?

1977 startete die NASA (die amerikanische Raumfahrtbehörde: National Aeronautics and Space Administration) eine Mission, die auf lange Dauer ausgerichtet war. Innerhalb von 16 Tagen startete sie die beiden Sonden Voyager 2 und Voyager 1 (in dieser Reihenfolge, weil die zweite eine andere Route hatte und schneller war). Der Start innerhalb von wenigen Tagen war kein Zufall – die Planeten standen günstig – um unser Sonnensystem zu erkunden. Am 15.8.2006 hatte Voyager 1 etwa 15 Milliarden km (oder 100 Astronomische Einheiten) zurückgelegt. Etwa 2017 wird die Sonde den interstellaren Raum erreichen.

An Bord beider Voyager-Sonden befindet sich eine Schallplatte aus Gold mit den „Sounds of Earth" (Klänge der Welt) mit Bildern und Tönen von der Erde und eine eingravierte Bedienungsanleitung. Diese Schallplatte hat eine geschätzte Lebensdauer von 500 Millionen Jahren.

„The Sounds of Earth Record Cover – GPN-2000-001978" von NASA/JPL http://grin.hq.nasa.gov/ABSTRACTS/GPN-2000-001978.html. Lizenziert unter Gemeinfrei über Wikimedia Commons - http://commons.wikimedia.org/wiki/File:The_Sounds_of_Earth_Record_Cover_-_GPN-2000-001978.jpg#/media/File:The_Sounds_of_Earth_Record_Cover_-_GPN-2000-001978.jpg

Arbeitsaufträge:

1. Informiere dich darüber, was auf der Schallplatte der Voyager gespeichert ist! Überlege, warum die Menschen dies Außerirdischen mitteilen wollten! (Spezialaufgabe: hättest du es genau so gemacht?)

Hier findest du durchschnittliche Haltbarkeitsdauer verschiedener Datenträger:

■ 5–10 Jahre	Informationen auf Magnetbändern, Magnetplatten, Disketten
■ 20–50 Jahre	Magneto-Optical Disks, WORM, CD-ROM, CD-R
■ 30 Jahre	Recycling-Papier
■ * Jahre	* Wie lange ein USB-Stick haltbar ist, hängt von der Benutzung ab!
■ 50 Jahre	Blu-Ray-Discs
■ 100 Jahre	Chromogene Farbfilme, Diazo- und Vesicular-Mikrofilme
■ 100 Jahre	Holzschliffhaltiges, säurehaltiges Papier
■ 250 Jahre	Chromogene Farbfilme, gekühlt
■ 300 Jahre	Silberhalogenid-Mikrofilme auf Acetat-Basis
■ 400 Jahre	Farbfilme im Farbbleichverfahren (Iifochcrome Micrographic)
■ Mehrere Hundert Jahre	säure- und ligninfreies, gepuffertes „alterungsbeständiges" Papier
■ 1000 Jahre	Pergamente, Papyri, Tontafeln

Quelle: „Archive und ihre kulturelle Überlieferung – Digitale Archive", Prof. Christian Wolff Universität Regensburg

2. Wie lange etwas haltbar ist, ist sehr unterschiedlich. Übertrage die Liste mit den Haltbarkeitsdauern in ein Säulendiagramm (Du kannst auch MS Excel oder OpenOffice.calc dazu nutzen)! Wie sollte man wichtige Daten speichern?

3. Jetzt wird es noch mal schwierig: Was kannst du tun, wenn du eine CD mit Urlaubsfotos noch deinen Enkeln zeigen möchtest? Diskutiert verschiedene Möglichkeiten in der Klasse und haltet die Ergebnisse auf der Tafel fest!

9|1 Spezielle Bestimmungen für die Schule

9|2 Datenschutzbestimmungen für Lehrer

9|3 Mediennutzung und Aufsichtspflicht

Was wir beachten müssen: Regelungen für die Schule!

9

Spezielle Bestimmungen für die Schule

Kommunikation über Soziale Netzwerke
Die Innenministerkonferenz (IMK) der Bundesländer hat sich in einem Bericht vom April 2012 mit dem Datenschutz in Sozialen Netzwerken beschäftigt und darin rechtliche Bede nken an der Nutzung von Facebook durch öffentliche Stellen und damit auch der Schule angemeldet.[1] Neben den dort aufgeführten, eher allgemein gehaltenen Vorschlägen, existieren noch konkretere Bestimmungen, die den Umgang mit Facebook im schulischen Kontext regeln. In folgenden Bundesländern haben die jeweiligen Schulministerien strikte Verbote erlassen:

- **Baden-Württemberg**
  Das Kultusministerium Baden-Württemberg stellt klar: „Aufgrund datenschutzrechtlicher Bestimmungen ist die Verwendung von Sozialen Netzwerken für die dienstliche Verarbeitung personenbezogener Daten generell verboten“[2]. Damit ist sowohl die Kommunikation (z. B. Termine vereinbaren, Lerngruppen einrichten) zwischen Lehrern und Schülern als auch die Kommunikation zwischen Lehrern über Schüler via Facebook verboten. Soziale Netzwerke dürfen aber im Unterricht genutzt werden, um Vorteile und Risiken pädagogisch zu bearbeiten.

- **Bayern**
  Das Bayerische Kultusministerium formuliert: „Die Kontaktaufnahme als „Follower“ dürfte in beide Richtungen grundsätzlich unzulässig sein. Lehrkräfte sollten selbstverständlich nicht „Anhänger“ ihrer Schülerinnen und Schüler sein, die sie zu erziehen und zu bewerten haben. Entsprechende „Freundschaftsanfragen“ könnten Schülerinnen und Schüler praktisch nicht ablehnen. Und auch die Freundschaftsanfrage durch Schülerinnen und Schüler sollten Lehrkräfte zurückweisen.“ [3]

- **Rheinland Pfalz**
  Das Bildungsministerium Rheinland-Pfalz verbietet Facebook-Freundschaften zwischen Lehrern und Schülern, da so das Distanz-Verhältnis zwischen Lehrern und Schülern aufgehoben würde. Zudem dürfen weder Noten, Hausaufgaben etc. über das Soziale Netzwerk mitgeteilt werden, noch dürfen Klassenausflüge darüber geplant werden. Die Begründung: Der Bildungs- und Erziehungs-Auftrag der Schule und die Datenpolitik von Facebook passen nicht zusammen.[4]

- **Schleswig-Holstein**
  Das Ministerium für Bildung und Wissenschaft des Landes Schleswig-Holstein verbietet die Kommunikation zwischen Lehrern und Schülern über schulische Belange via Facebook. Außerdem ist es Schulen nicht erlaubt, eigene Facebook-Seiten, sogenannte Fanpages einzurichten.[5]

In den übrigen Bundesländern ist die Kommunikation zwischen Lehrern und Schülern derzeit (Stand: 2015) nicht generell verboten:

- **Berlin**
  Zur Nutzung von Sozialen Netzwerken wie Facebook gibt es derzeit keine einheitliche Vorgabe, jedoch forderte der Berliner Datenschutzbeauftragte bereits in seinem Bericht für das Jahr 2013 ein generelles Facebook-Verbot zwischen Lehrern und Schülern.[6]

- **Brandenburg**
  Ein komplettes Verbot wird als unnötig angesehen. Vielmehr wird an das Verantwortungsbewusstsein der Lehrer appelliert, mit persönlichen Daten in allen Nutzungskontexten umsichtig umzugehen.[7]

- **Bremen**
  Auch in Bremen wird die Nutzung von Facebook und ähnlichen Netzwerken nicht grundsätzlich verboten. In einer ausführlichen Handreichung des Landesinstituts für Schule Bremen[8], werden jedoch ausführlich verschiedene Vor- und Nachteile aufgezeigt. Die Art der Nutzung kann somit jeder selbst entscheiden. Es wird jedoch empfohlen, stets eine angemessene bzw. professionelle Distanz einzuhalten.

- **Hamburg**
  Lehrern steht es frei, Soziale Netzwerke im schulischen Kontext zu nutzen. Das Thema Soziale Netzwerke erhält in Hamburg zudem besondere Relevanz, da es ein Teil des für allgemeinbildende Schulen verbindlich zu behandelten Medienpasses ist.[9]

- **Hessen**
  In einer Handreichung zum Umgang mit Sozialen Netzwerken in hessischen Schulen, empfiehlt das hessische Kultusministerium, dass die Nutzung Sozialer Netzwerke im Bereich der schulischen und unterrichtsrelevanten Kommunikation nur sehr eingeschränkt und nur unter bestimmten Voraussetzungen erfolgen sollte. Alternativ sollten vielmehr schulinterne Lernplattformen wie bspw. Moodle genutzt werden, um eine rechtlich unangreifbare Kommunikation und Datenverarbeitung zu gewährleisten. Messenger-Dienste wie bspw. WhatsApp sollten aus datenschutzrechtlichen Gründen in der schulischen Kommunikation nicht eingesetzt werden.[10]

- **Mecklenburg-Vorpommern**
  Es gibt keine expliziten Vorgaben für den Umgang mit Sozialen Netzwerken.

- **Niedersachsen**
  Auch in Niedersachsen werden keine verbindlichen Vorgaben an Lehrkräfte gerichtet.

- **Nordrhein-Westfalen:**
  Es gibt kein explizites Verbot der Facebook-Nutzung im schulischen Kontext. In einer Handreichung der Bezirksregierung Münster wird aber darauf hingewiesen, dass auch innerhalb Sozialer Netzwerke zwischen Lehrern und Schülern stets ein dienstliches Verhältnis herrschen muss.[11]

- **Saarland**
  Aus einem Rundschreiben an alle Schulen des Saarlandes geht hervor, dass die Nutzung von Facebook & Co. im schulischen Kontext generell erlaubt ist. Dabei ist jedoch wichtig, dass Schüler und Eltern, die Facebook nicht nutzen, nicht benachteiligt werden dürfen. Das Soziale Netzwerk darf also nicht der einzige Kommunikationsweg bleiben und auch innerhalb des Netzwerkes muss eine professionelle Distanz zwischen Lehrern und Schülern gewahrt werden.[12]

- **Sachsen-Anhalt**
  In einem Hinweisblatt des Landes heißt es hierzu: „Soziale Netzwerke dürfen nicht dazu genutzt werden, um dienstliche oder personenbezogene Informationen über ein solches Netzwerk zu verbreiten. Insbesondere wird von der Nutzung i. S. einer Lernplattform abgeraten." [13]

- **Sachsen**
  Das Sächsische Staatsministerium für Kultus verweist bezüglich der dienstlichen Nutzung von Sozialen Netzwerken an Schulen insbesondere auf die Datenschutzproblematik. Das Einstellen personenbezogener wie schulbezogener Daten in Soziale Netz werke durch die Lehrperson wird als datenschutzrechtlich unzulässig bewertet.[14]

- **Thüringen**
  Es herrscht kein explizites Verbot Sozialer Netzwerke, jedoch weist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit in einer Pressemitteilung darauf hin, dass eine dienstliche Nutzung von Facebook den Datenschutzbestimmungen des Landes Thüringen widerspricht und somit unterlassen werden sollte.[15]

Aus der Praxis
Die dienstliche Kommunikation zwischen Lehrern und Schülern via Facebook und Co. ist nicht nur negativ. Für eine Klassenfahrt lässt sich bspw. mittels eines Messenger-Dienstes für einen bestimmten Zeitraum eine Gruppe erstellen, über die die Schüler dann über kurzfristige Programmänderungen informiert werden können. Vorausgesetzt es werden vorher klare Regeln vereinbart, alle SchülerInnen verfügen über den Messenger-Dienst und es ist im jeweiligen Bundesland erlaubt.
***Wichtig dabei vorher abzuklären:** Datenschutzrechtliche Unbedenklichkeit und zwangloses Einverständnis aller Beteiligten!*

Links und weiterführende Informationen

Webseiten

www.kmk.org/index.php?id=485
Die Seite der Kultusministerkonferenz bietet eine Übersicht über die Schulgesetze aller Bundesländer.

http://li.hamburg.de/medienpass/
Übersichtsseite zum Hamburger Medienpass

www.lis.bremen.de/sixcms/media.php/13/Handreichung_Soziale_Netzwerke_Schule.pdf
Ausführliche Handreichung „Soziale Netzwerke in der Schule" des Landesinstituts für Schule Bremen mit Anwendungsbeispielen.

http://lehrerfortbildung-bw.de/sueb/recht/ds_neu/
Eine umfassende Informationsseite über datenschutzrechtliche Aspekte in der Schule in Baden-Württemberg.

www.datenschutzzentrum.de/schule/praxishandbuch-schuldatenschutz.pdf
Umfassendes Handbuch zum Schuldatenschutz in Schleswig-Holstein.

Endnoten

[1] INNENMINISTERKONFERENZ (IKM). (2012, 4. April). *Ergebnisbericht der Arbeitsgruppe des AK I „Staatsrecht und Verwaltung" zum Datenschutz in Sozialen Netzwerken vom 4. April 2012* (Absatz 2). Aufgerufen am 02.08.2015 unter https://www.datenschutzzentrum.de/internet/20120404-AG-SozNetzw-AK-I-IMK.pdf

[2] IT.KULTUS-BW. (2015, 29. April). *Der Einsatz von „Sozialen Netzwerken" an Schulen.* Aufgerufen am 02.08.2015 unter http://www.kultusportal-bw.de/IT,Lde/Startseite/IT-Sicherheit/soziale+Netzwerke

[3] IT-BEAUFTRAGTER der Bayerischen Staatsregierung. (2012, September). *Der rechtliche Rahmen für den Umgang der Beschäftigten der Bayerischen Staatsverwaltung mit Sozialen Medien* (S. 21). Aufgerufen am 02.08.2015 unter http://www.uni-wuerzburg.de/fileadmin/32040000/_temp_/Weitergabe_Leitfaden_SozialeMedien_-_Rechtlicher_Rahmen_zum_Leitfaden.pdf

[4] DATENSCHUTZ RLP. (2013). *Merkblatt: Lehrkräfte und Soziale Netzwerke (z. B. facebook).* Aufgerufen am 14.07.2015 unter http://www.datenschutz.rlp.de/de/aktuell/2013/images/SMR-Merkblatt-soziale_Netze.pdf

[5] MINISTERIUM für Bildung und Wissenschaft Schleswig-Holstein. (2012, 02. November). *Betrieb von Fanpages auf Facebook und dienstliche Kommunikation über Facebook an Schulen.* Aufgerufen am 14.11.2014 unter http://www.schleswig-holstein.de/DE/Fachinhalte/S/schulrecht/Downloads/Erlasse/Downloads/Facebook.pdf?__blob=publicationFile&v=1

[6] NEWS4TEACHERS.DE. (2014, 2. April). *Berliner Datenschützer will Facebook-Verbot zwischen Lehrern und Schülern auch in der Hauptstadt.* Aufgerufen am 02.08.2015 unter http://www.news4teachers.de/2014/04/berliner-datenschuetzer-will-facebook-verbot-zwischen-lehrern-und-schuelern-auch-in-der-hauptstadt/

[7] KAUFMANN, M. (2013, 24. Juli). *Kein Facebook-Tabu.* maz-online.de. Aufgerufen am 02.08.2015 unter http://www.maz-online.de/Brandenburg/Kein-Facebook-Tabu

[8] LANDESINSTITUT für Schule Bremen. (2013, August). *Soziale Netzwerke in der Schule. Handreichung zur Medienkompetenz.* Aufgerufen am 02.08.2015 unter http://www.lis.bremen.de/sixcms/media.php/13/Handreichung_Soziale_Netzwerke_Schule.pdf

Endnoten

[9] BEHÖRDE für Schule und Berufsbildung. (2013, 8. November). *Digitale Medien. Schulen führen Hamburger Medienpass ein.* Aufgerufen am 02.08.2015 unter http://www.hamburg.de/bsb/pressemitteilungen/4133750/2013-11-08-bsb-digitale-medien/

[10] https://kultusministerium.hessen.de/sites/default/files/media/hkm/handreichung_soziale_netzwerke_-_stand_februar_2015.pdf

[11] SCHEPPING, P., Sieberg, H. & Weichselgärtner, R. (2013, Juni). *„Privat trifft Dienst". Facebook und Co. im schulischen Raum.* Bezirksregierung Münster, Dezernat 46.01 – Lehrerausbildung. Aufgerufen am 02.08.2015 unter http://www.brd.nrw.de/schule/personalangelegenheiten/pdf/2013_10_06_Handreichung_zu_Risiken_und_Grenzen_der_Nutzung_sozialer_Netzwerke_BR_Muenster.pdf

[12] SAARLAND Ministerium für Bildung und Kultur. (2014, 12. Februar). *Rundschreiben an alle Schulen. Umgang mit sozialen Netzwerken.* Aufgerufen am 02.08.2015 unter http://www.saarland.de/dokumente/thema_bildung/Rundschreiben_Soziale_Netzwerke.pdf

[13] KULTUSMINISTERIUM Sachsen-Anhalt. (2014, 19. November). *Hinweise zum Umgang mit sozialen Netzwerken (zum Beispiel Facebook) in den Schulen Sachsen-Anhalts.* Bek. des MK vom 19.11.2014 – 25-5885 (Absatz 5). Aufgerufen am 02.08.2015 unter http://www.mk.bildung-lsa.de/bildung/be-umgang_soziale_netzwerke.pdf

[14] http://www.schule.sachsen.de/download/download_bildung/14_07_verhaltenshinweise_smk.pdf

[15] HASSE, Dr. L. (2013, 29. Juli). *Pressemitteilung. Lehrer in facebook & Co.? NEIN!* Aufgerufen am 02.08.2015 unter https://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/pmtlfdi/pm_lehrer_in_facebook___co.pdf

Datenschutzbestimmungen für Lehrer

Datenschutz im Schulalltag
Die gängige Praxis im Umgang mit Daten im Schulalltag ist nicht immer optimal: Oft gibt es keine persönlichen Büros, die abgeschlossen werden können. Teilweise gibt es keine Dienst-Computer, die ausschließlich zu schulischen Zwecken genutzt werden und zentral von Experten eingerichtet und gewartet werden etc. Häufig bringen Lehrkräfte ihre eigenen ungesicherten Geräte, wie Laptops oder USB-Sticks mit. Auf diesen werden dann zu Hause und unterwegs Klassenlisten, Fotos, Noten etc. verwaltet und gespeichert – schlimmstenfalls in einer Cloud. So kann es leicht vorkommen, dass ein USB-Stick in der Schule vergessen und dann von Schülern gefunden wird. Viele sind sich dieser Gefahren nicht immer bewusst.

Immer daran denken, was schlimmstenfalls passieren kann, wenn Daten (Klassenlisten, Noten, etc.) wirklich einmal in falsche Hände geraten sollten und Risiken minimieren.

Verwaltung von Daten: Was ist erlaubt?
Jedes Bundesland hat seine eigenen Bestimmungen bezüglich der Verarbeitung personenbezogener Daten in der Schule. Allen gemein sind jedoch die folgenden Punkte:

- Private Geräte dürfen nur in Ausnahmefällen zu dienstlichen Zwecken eingesetzt werden.
- Wenn Lehrer personenbezogene Daten von SchülerInnen verarbeiten, ist dies automatisch eine dienstliche Tätigkeit, d. h. es gelten die Landesbestimmungen für den Datenschutz in diesem Falle auch zu Hause und auf privaten Geräten.
- Die Schulleitung muss diese Nutzung (schriftlich) genehmigen, diese Genehmigung kann für maximal fünf Jahre erteilt werden.
- Schülerdaten dürfen nur von den Lehrern verarbeitet werden, die als Klassenlehrer oder Fachlehrer diese Schüler auch unterrichten.
- Es dürfen nur benötigte Daten verarbeitet werden, max. die folgenden:
  - Namen,
  - Geschlecht,
  - Geburtsdatum, Geburtsort,
  - Zugehörigkeit zu einer Religionsgemeinschaft,
  - Klasse, Gruppe oder Kurs,
  - Ausbildungsrichtung bzw. Ausbildungsberuf,
  - Fächer,
  - Art, Datum und Ergebnisse von Leistungskontrollen,
  - Zeugnisnoten und andere Zeugniseintragungen.
- Das Gerät muss so behandelt werden, dass niemand sonst Zugriff auf die Daten haben kann, z. B. durch Passwortschutz und andere Sicherungen.
- Diese Daten dürfen nur verschlüsselt übertragen werden (d. h. bspw. kein unverschlüsselter Versand der Klassenliste per E-Mail).

Die Datenschutzbestimmungen der Länder beziehen nicht immer zu allen Verwendungszusammenhängen Neuer Medien klar Stellung, was durch die fortschreitenden Neuentwicklungen in diesem Feld nicht verwunderlich ist. Bei Unklarheiten ist es aber sicherlich sinnvoll, auf die Nutzung eines bestimmten Dienstes zu verzichten.

Die genauen Datenschutzbestimmungen der einzelnen Bundesländer finden sich hier:

Baden-Württemberg	www.landesrecht-bw.de/jportal/?quelle=jlink&query=SchulG+BW&psml=bsbawueprod.psml&max=true
Bayern	www.gesetze-bayern.de/jportal/portal/page/bsbayprod.psml?showdoccase=1&doc.id=jlr-EUGBY2000rahmen&doc.part=X
Berlin	http://gesetze.berlin.de/jportal/?quelle=jlink&query=SchulG+BE&psml=bsbeprod.psml&max=true&aiz=true
Brandenburg	http://bravors.brandenburg.de/de/gesetze-212992
Bremen	https://bremen.beck.de/default.aspx?typ=reference&y=100&g=BrSchulG
Hamburg	www.landesrecht-hamburg.de/jportal/portal/page/bshaprod.psml?showdoccase=1&doc.id=jlr-SchulGHArahmen&st=lr
Hessen	www.rv.hessenrecht.hessen.de/jportal/portal/t/uom/page/bshesprod.psml?doc.hl=1&doc.id=jlr-SchulGHE2005rahmen%3Ajuris-lr00&documentnumber=1&numberofresults=270&showdoccase=1&doc.part=R&paramfromHL=true#focuspoint
Mecklenburg-Vorpommern	www.landesrecht-mv.de/jportal/portal/page/bsmvprod.psml?showdoccase=1&doc.id=jlr-SchulGMV2010rahmen&doc.part=X&doc.origin=bs&st=lr
Niedersachsen	www.schure.de/2241001/nschg.htm
Nordrhein-Westfalen	www.schulministerium.nrw.de/docs/Recht/Schulrecht/Schulgesetz/Schulgesetz.pdf
Rheinland-Pfalz	http://landesrecht.rlp.de/jportal/portal/t/n9a/page/bsrlpprod.psml?doc.hl=1&doc.id=jlr-SchulGRP2004rahmen%3Ajuris-lr00&documentnumber=1&numberofresults=146&showdoccase=1&doc.part=R&paramfromHL=true#focuspoint
Saarland	http://sl.juris.de/cgi-bin/landesrecht.py?d=http://sl.juris.de/sl/gesamt/SchulOG_SL.htm#SchulOG_SL_rahmen
Sachsen	www.recht.sachsen.de/vorschrift/4192-SchulG
Sachsen-Anhalt	www.landesrecht.sachsen-anhalt.de/jportal/portal/t/1rxx/page/bssahprod.psml?doc.hl=1&doc.id=jlr-SchulGST2013rahmen&documentnumber=1&numberofresults=144&showdoccase=1&doc.part=R&paramfromHL=true#focuspoint
Schleswig-Holstein	www.gesetze-rechtsprechung.sh.juris.de/jportal/?quelle=jlink&query=SchulG+SH&psml=bsshoprod.psml&max=true
Thüringen	http://landesrecht.thueringen.de/jportal/?quelle=jlink&query=SchulG+TH&psml=bsthueprod.psml&max=true&aiz=true

Checkliste
Folgende Checkliste kann helfen, Daten dienstrechtlich korrekt zu verwalten:

- ☐ *Das schriftliche Einverständnis der Schulleitung liegt vor*
- ☐ *Es sind ausschließlich Schülerdaten gespeichert, die wirklich benötigt werden (z. B. Namen, Geschlecht, Noten etc.)*
- ☐ *Alle nicht benötigten Daten sind umgehend mit Spezialprogrammen, sogenannte Datenschreddern, sicher zu löschen (z. B. ArchiCrypt-Shredder, Freeraser, CyberShredder etc.)*
- ☐ *Das Gerät (vor allem auch der USB-Stick) ist mit einem starken Passwort geschützt (d. h. mind. 8 Zeichen, darunter Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen etc.)*
- ☐ *Der Zugriff auf die Daten und Geräte durch Dritte ist ausgeschlossen – auch zu Hause*

Links und weiterführende Informationen

Webseiten

www.kmk.org/index.php?id=485
Übersichtsseite der Kultusministerkonferenz zu den einzelnen Schulgesetzen der Bundesländer. Hier finden sich auch die speziellen Bestimmungen für Privatschulen.

www.lehrer-online.de/persoenliche-daten.php?sid=467780793786545917440597059710 30
Übersichtsseite von Lehrer-Online zu persönliche Daten und Datenschutz.

http://blog.kaspersky.de/zehn-sicherheitstipps-fur-schuler-lehrer-und-eltern/
Sicherheitstipps der Firma Kaspersky

www.content-zwh.de/FAH/datenschutznav/default.htm
Lernprogramm für Beschäftigte im öffentlichen Dienst. Erstellt von der Fortbildungsakademie des Ministeriums für Inneres und Kommunales des Landes Nordrhein-Westfalen in Zusammenarbeit mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

www.ldi.nrw.de/mainmenu_Datenschutz/index.php
Einführung in grundlegende Fragen des Datenschutzes.

Mediennutzung und Aufsichtspflicht

Aufsichtspflicht auch bei der Mediennutzung
Jeder Minderjährige fällt unter die Aufsichtspflicht. In der Schule übernimmt der Lehrer anstelle der Eltern diese Aufsichtsplicht. Ziel ist immer, Schüler vor Schaden jeglicher Art zu bewahren und das muss überall und zu jeder Zeit gewährleistet sein. Deshalb müssen Lehrer in den Pausen Schulhof und Flure beaufsichtigen und dürfen auch die Klassenräume nicht unbeaufsichtigt lassen. Für volljährige SchülerInnen gilt die sogenannte **Fürsorgepflicht**. Die jeweiligen Bestimmungen sind in den Schulgesetzen der Länder geregelt.

Auch in Bezug auf die Mediennutzung in der Schule gelten diese Pflichten. In vorangegangenen Kapiteln wurde aufgeführt, welche Inhalte für die Entwicklung von Kindern und Jugendlichen problematisch oder gar gefährlich sein können. Auch für den Schulalltag gilt es sicherzustellen, dass besonders gefährdende Inhalte für Kinder und Jugendliche nicht zugänglich sind. Ist das dennoch der Fall, kann dies als Form der Unterlassung geahndet werden.

Da es nur schwer möglich ist, die Aufsicht bzw. die sichere Mediennutzung eines jeden Schülers zu gewährleisten, hat sich im Schulalltag bewährt, dass sich die Schüler beaufsichtigt „fühlen" müssen.[1] Diese gefühlte Aufsicht wäre bswp. nicht gegeben, wenn die zuständige Lehrkraft bei Unterrichtseinheiten im Computerraum grundsätzlich in andere Tätigkeiten vertieft ist und so den Schülern das Gefühl gibt, sich frei und ohne Beachtung der Arbeitsaufträge im Internet bewegen zu können.

Für die korrekte Beaufsichtigung der SchülerInnen können die drei folgenden Grundsätze berücksichtigt werden: [2]

- **Vorausschauende Umsichtigkeit**
  Lehrer müssen Gefahren identifizieren und mit den SchülerInnen klare Regeln vereinbaren, um diese zu vermeiden.
- **Ununterbrochene Beständigkeit**
  SchülerInnen müssen sich darauf verlassen können, dass Lehrer ihre Aufsicht grundsätzlich immer ausführen und wahrnehmen.
- **Kontrollierende Nachdrücklichkeit**
  Regeln werden den SchülerInnen immer wieder ins Gedächtnis gerufen, deren Einhaltung wird kontrolliert und Regelverstöße werden angemessen geahndet.

Verletzung der Aufsichtspflicht
LehrerInnen handeln im Schulalltag nicht als Privatpersonen, sondern als Beamte und damit Angestellte des Staates. Bei einer Verletzung der Amtspflicht (also der durch das ausgeführte Amt eines Beamten begründeten Dienstpflicht), haftet daher auch der Dienstherr.[3] Bei Vorsatz oder grober Fahrlässigkeit kann dieser seine Beamten allerdings zur Verantwortung ziehen.

Doch was genau ist unter Vorsatz und Fahrlässigkeit zu verstehen? Das Bürgerliche Gesetzbuch legt in § 823 grundsätzlich fest, dass jeder, der einem anderen schuldhaft Schaden zufügt, diesen auch ersetzen muss. Einen Schaden zu „verschulden", ist jedoch nicht gleichbedeutend damit, ihn zu „verursachen".[4] Um einen Schaden zu verursachen, muss ein Vorsatz, also die Intention vorliegen, jemanden einen Schaden zuzufügen bzw. muss dieser Schaden billigend in Kauf genommen werden (§ 15 StGB)[5].

Wird ein Schaden „verursacht“ kann Fahrlässigkeit vorliegen. Fahrlässig handelt, „wer die erforderliche Sorgfalt außer Acht lässt“[6]. Hier wird in grobe (d. h. Sorgfalt wird bewusst und in schwerem Maße vernachlässigt) oder leichte (d. h. unbewusste) Fährlässigkeit unterschieden.

Die Frage nach grober oder leichter Fahrlässigkeit ist für die Rechtsfolgen einer Aufsichtspflichtverletzung relevant. Folgende Rechtsfolgen können unterschieden werden[7]:

- Bei einem zivilgerichtlichen Verfahren können Schadensersatzforderungen geltend gemacht werden, bspw. wenn im Sportunterricht grundlegende Vorsichtsmaßnahmen wissend außer Acht gelassen wurden.

- Bei einem dienstgerichtlichen Verfahren kann es zu einer Disziplinarstrafe kommen, bspw. nach bewusstem, unerlaubtem Verlassen des zu beaufsichtigenden Bereiches.

- Strafrechtliche Folgen im Sinne einer Verurteilung sind in schwerwiegenden Fällen der Aufsichtspflichtverletzung zu erwarten, bspw. bei einem Badeunfall mit fahrlässiger Tötung.

Internetnutzung sicher gestalten
Es gibt verschiedene Möglichkeiten die Mediennutzung in der Schule für alle Beteiligten sicher zu gestalten:

- **Medienkompetenz**
  Schüler, Lehrer und Eltern sollten um die Chancen und Risiken der Internetnutzung wissen und eigenständig sicher damit umgehen können.

- **Nutzerordnung**
  Mittels einer Nutzerordnung sollten klare Regeln darüber aufgestellt werden, was erlaubt ist und was nicht. Die Ordnung sollte folgende Aspekte umfassen, von allen Beteiligten (Schüler, Eltern) schriftlich bestätigt und ausführlich besprochen werden:

  - Regelung über die Geheimhaltung von Passwörtern
  - Auflistung der verbotenen Nutzungsformen und -inhalte
  - Einhaltung von Datenschutz und Datensicherheit
  - Integrität der Techniken, d. h. kein Eingriff in Soft- und Hardware
  - Umsichtiger Umgang mit den Geräten bis hin zum Ess- und Trinkverbot am PC
  - Klare Regelungen über den Abruf von Informationen / Daten / Programmen aus dem Internet und das Versenden von Informationen über das Internet
  - Wahrung von Urheberrecht und Persönlichkeitsrechten
  - Evtl. Abschnitt zur Aufsicht und außerunterrichtlichen Nutzung

- **Sanktionen bei Missbrauch**
  Verstöße müssen sanktioniert werden. Zur Verfügung stehen im Regelfall die schulischen Disziplinarmaßnahmen bis hin zur strafrechtlichen Ahndung schwerer Verstöße.

- **Technische Kontrolle**
  Der Einsatz von Filtersoftware sowie Servern, die die Zugriffe protokollieren und eindeutige Nutzerkennungen zuweisen, ermöglicht die Kontrolle der Internetaktivitäten.

Aus der Praxis
Um eine sichere Internetnutzung während des Unterrichts zu gewährleisten, hat es sich bewährt, neben technischem Schutz, klaren Regeln etc. den Schülern auch immer mal wieder über die Schulter zu schauen. So sehen sie, dass dem Lehrer nicht vollkommen entgeht, was sie tun (Stichwort: gefühlte Aufsicht).

Exkurs: WLAN in der Schule

Viele Schulen ermöglichen mittlerweile ihren SchülerInnen einen kostenlosen Internetzugang über WLAN – auch außerhalb des Unterrichts, in Pausen und Freistunden. Voraussetzung dafür sind allerdings klare und eindeutige Nutzungsregeln, die als Teil der Schulordnung von der Schulkonferenz beschlossen werden. Diese sollten in schriftlicher Form vorliegen und von Schülern und Eltern unterzeichnet werden.

In den Nutzungsregeln sollte enthalten sein,

- dass der Internet-Zugang nur zu schulischen Zwecken genutzt wird,
- dass alle gesetzlichen Bestimmungen zum Urheberrecht, Jugendschutz, Strafrecht etc. zu beachten sind,
- dass die Schule Nutzungseinschränkungen wie technische Filtersperren, zeitliche Beschränkungen und definierte Zugänge vornehmen darf,
- dass die Schule keine Haftung für die Datensicherheit und -integrität der Geräte der SchülerInnen übernimmt,
- welche Sanktionen bei Missbrauch erfolgen,
- dass die Schule jede Aktivität personenbezogen protokollieren, speichern und verarbeiten darf.

Für den Einsatz von WLAN im Schulgebäude ist es wichtig dafür Sorge zu tragen, dass der Internetzugang nur seitens berechtigter Personen, also SchülerInnen und LehrerInnen, möglich ist. Gewährleistet werden kann dies in technischer Hinsicht bspw. über eine Anmeldung mit Nutzername und Passwort oder / und über MAC-Adressen, die jedes Gerät eindeutig identifizieren. Nur auf diese Weise registrierte Geräte sollten dann auf das Internet zugreifen können.

Links und weiterführende Informationen

Webseiten

www.schulministerium.nrw.de/docs/Recht/Schulrecht/Rechtsfragen-Internetnutzung/index.html
Unter Regelungen > Muster-Nutzerordnung der Computereinrichtung an Schulen findet sich hier ein Musterbeispiel einer Nutzerordnung für den schulischen Einsatz

www.schleswig-holstein.de/DE/Fachinhalte/L/lehrer_innen/Downloads/Muster_Internetnutzung.pdf?__blob=publicationFile&v=1
Musterbeispiel einer WLAN-Nutzungsregelung für Schulen

www.schulrecht-sh.de/texte/i/internetnutzung.htm
Schulrecht von Schleswig-Holstein zur Internetnutzung an Schulen

www.nibis.ni.schule.de/~as-ver/fach/paedagogik/material/aufsichtspflicht.pdf
Ein detailliertes Skript zu Fragen rund um die schulische Aufsichtspflicht

www.schulrecht-rw.de/2_Aufsichtspflicht.pdf
Ein Skript zum Thema Aufsichtspflicht, zusammengestellt für angehende und bereits tätige Lehrende an Grund- und Hauptschulen in Baden-Württemberg

Endnoten

[1] STAATLICHES Seminar für Didaktik und Lehrerbildung Rottweil. (o. A.). *Aufsichtspflicht*. Aufgerufen am 02.08.2015 unter http://www.schulrecht-rw.de/2_Aufsichtspflicht.pdf

[2] Ebd.

[3] GRUNDGESETZ für die Bundesrepublik Deutschland. *Artikel 34*. Aufgerufen am 02.08.2015 unter http://www.gesetze-im-internet.de/gg/art_34.html

[4] BÜRGERLICHES Gesetzbuch. *§ 823 Schadensersatzpflicht.* Aufgerufen am 02.08.2015 unter http://www.gesetze-im-internet.de/bgb/__823.html

[5] STRAFGESETZBUCH. *§ 15 Vorsätzliches und fahrlässiges Handeln.* Aufgerufen am 02.08.2015 unter http://www.gesetze-im-internet.de/stgb/__15.html

[6] BÜRGERLICHES Gesetzbuch. *§ 276 Verantwortlichkeit des Schuldners* (2. Satz). Aufgerufen am 02.08.2015 unter http://www.gesetze-im-internet.de/bgb/__276.html

[7] STAATLICHES Seminar für Didaktik und Lehrerbildung Rottweil. (o. A.). *Aufsichtspflicht*. Aufgerufen am 02.08.2015 unter http://www.schulrecht-rw.de/2_Aufsichtspflicht.pdf

klicksafe.de ist das deutsche Awareness Centre im CEF Telecom Programm der Europäischen Union.

klicksafe sind:

Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz – www.lmk-online.de

Landesanstalt für Medien Nordrhein-Westfalen (LfM) – www.lfm-nrw.de

Neben klicksafe gehören dem Safer Internet Centre folgende Partner an:

internet-beschwerdestelle.de
(durchgeführt von eco und FSM)

jugendschutz.net

Kinder- und Jugendtelefon von Nummer gegen Kummer e.V.

klicksafe wird kofinanziert von der Europäischen Union

klicksafe – Büros

c/o Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz
Turmstraße 10
67059 Ludwigshafen
E-Mail: info@klicksafe.de
Internet: www.klicksafe.de

c/o Landesanstalt für Medien Nordrhein-Westfalen (LfM)
Zollhof 2
40221 Düsseldorf
E-Mail: klicksafe@lfm-nrw.de
Internet: www.klicksafe.de