WORKSHOP
INTERNET & SICHERHEIT

Schwerpunkte des Workshops in der Übersicht

- Einstieg in das Projekt und Kennenlernen, Klärung von ersten Fragen
- Mediennutzungsverhalten von Jugendlichen (Einblicke und Austausch)
- Medienkompetenz heute? – Welche Themen sind den Jugendlichen wichtig
- Thematischer Block: Internet und Sicherheit
- Soziales Lernen und Kommunikationstraining (TN präsentieren ihre Gruppenergebnisse in Kleingruppen und im Plenum)

Aufbau

Dauer	Schwerpunkt /Thema	Methode	Material	Variante / Materialvariante	Kompetenzorientierte Zuordnung / Kompetenzen
45 Min.	Begrüßung, Organisation Überblick über den Tag und die Module Einstieg in das Projekt Warming- Up und Kennenlernen	Input mit Folien „Soziometrische Übung“ „Gemeinsamkeiten“	Kreppband, Eddings (Namensschilder) Folien AB 1.2 AB C.2	 AB C.2 a (mit Gesprächsanlass)	Die TN lernen sich untereinander kennen und erschließen sich verschiedene Übungen zum Sozialen Lernen
30 Min.	Ausbildung Medienscouts: „Wünsche, Erwartungen, Herausforderungen und Befürchtungen“ Besprechen der Ergebnisse im Plenum Filmclip: „Medienscouts NRW – Schülerfilm“ Einblicke in das Projekt und die Arbeit der Medienscouts (Film von Langer und Kabus)	Kartenabfrage in Schulgruppen mit anschließendem Austausch und Ergebnissicherung (Cluster der Karten) **Alternative:** Sammlung über mentimeter als Wortwoken.	Karteikarten AB 1.3 2 Stellwände, Stecknadeln	Kartenabfrage: Lehrerinnen und Lehrern und Schülerinnen und Schülern werden getrennt Gemeinsamer Austausch	Herausfinden, welche Wünsche, Erwartungen, Herausforderungen und Befürchtungen die TN an das Projekt herantragen
45 Min.	Einblicke in das	Plakatgestaltung in	Flipchartpapier,	Plakatgestaltung mit	Die Schülerinnen und Schüler

	Mediennutzungsverhalten bzw. in die Medieninteressen der Jugendlichen	Kleingruppen **Alternative:** Erstellung einer Pinnwand bei padlet. Mit Bildern aus dem Internet. Achtung: Bildrechte beachten.	bunte Stifte, Kreppband	ausgedruckten Logos und Bildern aus Zeitschriften Zusätzlich: Kleber und Scheren Trennung von Lehrerinnen und Lehrern und Schülerinnen und Schülern Für Lehrerinnen und Lehrer: Input und Austausch z.B. über JIM-Studie	reflektieren ihr eigenes Mediennutzungsverhalten
20 Min.	Pause				
15 Min.	Fortsetzung: Einblicke Mediennutzungsverhalten bzw. Medieninteressen der Jugendlichen	Austausch über die Plakate Rundgang **Alternative:** Gemeinsamer Austausch über die erstellten Pinnwände.	fertige Plakate		Die TN präsentieren ihre Erarbeitungen Die Lehrerinnen und Lehrer erhalten einen Einblick in das Mediennutzungsverhalten der Jugendlichen
45 Min.	Medienkompetenz heute Erste Sammlung: Welche Themen sind den Schülerinnen und Schülern wichtig?	Brainstorming in Kleingruppen Austausch und Cluster an Stellwand	Medienkompetenz heute: AB 1.8 Papier und Stifte	Einstieg über Clip z.B. Wo ist Klaus?	Die TN reflektieren welche Themen für sie in ihrer Arbeit als Medienscouts relevant werden könnten
15 Min.	Überleitung zum Thema „Internet und Sicherheit“ Ausblick auf Phase nach der Mittagspause	Input	Folien		
45 Min.	Mittagspause				

20 Min.	Wake-Up Methode	„Lügengeschichten“	Papier, Kreppband und Stifte		
15 Min.	Hinführung zum Thema „Internet und Sicherheit“ durch einen Teaserclip Vorstellung des Arbeitsauftrags Themen- und Rollenvergabe	kurzer Input Themen- und Rollenvergabe über Lose	Clip (Auswahl von AB 1.4) Vergabe von Thema und Amt für Stationen	Variante 1: Arbeit in Schulteams Variante 2: Arbeit in gemischten Gruppen dann Gruppenaufteilung auch durch Losverfahren	
60 Min.	Internet und Sicherheit: Arbeit in Gruppen Inkl. Plakatgestaltung <u>Stationen:</u> Station A: Technischer Schutz Station B: Passwörter Station C: E-Mail und Spam Station D: Suchen im Netz Station E: Wikipedia Station F: Datenschutz und Privatsphäre Station G: Chat und Instant Messenger Station H: Videoportale (z.B. YouTube) Station I: Vergisst das Internet? Station J: Werbung und Abzocke Station K: Pornografie Station L: Urheberrecht	Recherche und Plakatgestaltung in Kleingruppen (je 30 Min.) **Alternative:** Erstellung von Plakaten über Padlet.	Übergreifender Arbeitsauftrag PC mit Internetzugang für jede Gruppe gedrucktes Material (Klicksafe und Co.) Gestaltungmaterial für die Plakate Stationen: AB 1.5 Beschriftung der Stationen	Strukturierung der Plakatgestaltung durch vorgegebene Gliederung z.B. durch Symbole Vorgabe Präsentationsform offener gestalten (z.B. PowerPoint mit Vorgabe max. 3 Folien, Präsentation über „digitale Pinnwand“ im Internet…)	Die TN stellen die Formen, Funktionsweisen, Hintergründe und Zusammenhänge des Mediums dar Die TN erörtern Chancen und Risiken und eigene Handlungsmöglichkeiten
15 Min.	Pause				
30 Min.	Erklärung der Präsentationsmethode	„One stay, four stray“ mit Wechsel der	Kreppband, Stecknadeln Laufzettel: AB 1.8		Die TN präsentieren ihre Erarbeitungen

	Präsentation der Gruppenergebnisse	Präsentierenden Jede und jeder sollte sich mind. 5 Themen anschauen			
15 Min.	Verteilung Hausaufgabe, Tagesrückblick, Auswertung (Zielscheibe) und Abschluss		Hausaufgabe: AB 1.7 Zielscheibe: AB D.2 Zielscheibe	Bei größerem Zeitpuffer Feedback durch Blitzlicht Ausblick auf WS 2	
Im Anschluss	Einsammlung der Materialien durch die Gruppen (Ordner, Klicksafe Material und Co., Fotos von den Ergebnissen des Tages)				

Organisation und technische Vorbereitung WS digitale Spiele

Technische Vorbereitung WS Smartphones

Soll die Präsentation der Gruppenergebnisse mit unterschiedlichen Medien umgesetzt werden und/ oder sollte es die Möglichkeit für die TN geben, die kreativen Möglichkeiten des Smartphones selbst auszuprobieren, müssen folgende Vorbereitungen bedacht werden:

- Sicherstellen, dass das Internet nach Möglichkeit „frei“, also ohne Sperren nutzbar ist.
- Alle notwendigen Passwörter und Gastzugänge zur Internetnutzung an der Schule sollten vorhanden sein.
- Auch der Dozentenrechner muss nach Möglichkeit über eine Internetanbindung verfügen.
- Es ist zu klären, ob WLAN zur Verfügung steht und ob die TN sich mit ihren Smartphones hier anmelden dürfen (Anmeldedaten).
- Zugänge zu den „digitalen Pinnwänden“ anlegen, mit der Möglichkeit für die TN, selbst zu posten. Der oder die Workshopleitende sollte sich die Möglichkeit vorbehalten, Inhalte wieder zu löschen. Die Adressen müssen dann zu Beginn der Arbeitseinheit über Beamer und auf einem Paper ausgeteilt werden. Hier muss auch noch einmal verdeutlicht werden, dass direkt im Internet gepostet wird. Zwar ist die Adresse der „Pinnwand“ so nicht bekannt, dennoch müssen urheberechtliche Gesichtspunkte eingehalten werden (Verbreiten von Bildern etc.); in einigen Fällen können die Rechte der veröffentlichten Inhalte auch an die Seitenbetreiber übertragen werden. Hier empfiehlt sich eine „Vorab-Recherche“ der AGB. Wenn eine digitale Mindmap verwendet wird und/oder eine Onlinepräsentation erstellt werden soll, sollten auch hier Zugänge angelegt und die Passwörter im WS bereitgestellt werden.
- Soll es die Möglichkeit, ein Quiz (online) anzulegen, welches über eine App gespielt wird, müssen auch hier Zugänge angelegt werden. Dabei ist auf die Nutzungsrechte zu achten: handelt es sich um ein Angebot das kostenfrei im Bildungskontext nutzbar ist?
- Bei der Auswahl an Apps, mit denen man Bilder bearbeiten kann, müssen im Vorfeld die weiteren Nutzungsrechte an den Bildern geklärt werden. Hier sollte auch, wie bei allen anderen Angeboten, darauf geachtet werden, dass nach Möglichkeit keine In-App-Käufe möglich. TN sollten zusätzlich über die sichere Nutzung aufgeklärt werden.
- Einige Ergebnisse müssen eventuell zur Präsentation auf den Dozentenrechner übertragen werden. Hierfür ist ein USB-Stick erforderlich. Für Ergebnisse, die auf Smartphones erstellt werden, sollten zur Übertragung die entsprechenden Kabel verwendet werden. Die TN sollten dies als „Hausaufgabe“ beim vorhergegangenen WS erfahren haben.
- Eine Erinnerung per Mail an die Schulteams bzw. die begleitenden Pädagoginnen und Pädagogen einige Zeit vor dem WS ist hier sinnvoll.
- Die genaue Zuteilung, welche Gruppe mit welcher Präsentationsmöglichkeit arbeitet, sollte im Plenum benannt werden.
- Eine Liste mit den passenden Webadressen und Zugängen kann dann zusammen mit den Arbeitsblättern ausgeteilt werden.

Organisation

Kreis / Stadt:	
Datum und Ort:	
Anzahl der TN:	
Koordination & Kontakt:	
Ansprechperson vor Ort & Kontakt:	
Team & Kontakte:	
Räume:	
Arbeitsblätter:	AB 1.2 (1x für Referierende) AB C.2 (pro TN 1 Blatt) oder AB C.2a (pro TN 1 Blatt) AB 1.3 (1x für Referierende für das Cluster) AB 1.4 (1x für Referierende) AB 1.8 (1x pro Gruppe) AB 1.5 (1x) AB 1.6 (1x pro Teilnehmende) AB 1.7 (1x pro Gruppe) AB D.2 (1x oder 1x pro Arbeitsphase)
Material:	Folien (liegen nicht als Vorlage vor): Ablauf des Projektes und Ablauf des Tages Einstieg und Hintergrund und Ziele Medienscouts Mediennutzungsverhalten (Variante) Schülerfilm Clip: Wo ist Klaus? (Variante) Clip für Überleitung zum Thema Internet und Sicherheit bzw. AB 1.4 (Links zu den Filmen) Dokument Digitale Präsentationsmethoden Flipchartpapier Kreppband Moderationsstifte Karteikarten Stecknadeln Stifte Papier Scheren und Kleber
Sicherung der Arbeitsergebnisse:	Während des WS können Fotos von den TN, den Arbeitsprozessen, den Arbeitsergebnissen, den Präsentationen usw. erstellt werden. Zum Abschluss des WS gilt es zu klären, wer diese Sicherung der Ergebnisse/ die Dokumentation an das Projektbüro weiterleitet und wer diese Inhalte sichert. Das kann auch Aufgabe der Koordination der Stadt/des Kreises sein, sofern diese beim WS anwesend sind. Die Übernahme durch das Medienscouts-Team wäre eine weitere Möglichkeit.

SOZIOMETRISCHE ÜBUNG ZUM KENNENLERNEN

ABLAUF

Die Schülerinnen und Schüler sollen sich anhand unterschiedlicher Aspekte in einer Reihe, bzw. in Gruppen im Raum sortieren. Nach der Sortierung lassen sich genauere Fragen zur jeweiligen Thematik stellen, um einen tieferen Einblick zu erhalten.

Als lange Reihe:

- nach Größe
- nach Alter
- nach Entfernung Wohnort – Schule

In verschiedene Ecken:

- ich nutze Instagram
- ich nutze Whatsapp
- ich nutze YouTube
- weder noch

Als lange Reihe:

- Zeit pro Woche am Smartphone
- Zeit am Computer
- Zeit mit der Familie

In verschiedenen Ecken:

- Nutzung von PC/Smartphone und Internet vor allem
    - zum Spielen
    - zur Kommunikation mit Freunden
    - zum Arbeiten für die Schule
    - anderes

Gerätebesitz (ggf. SuS und LuL getrennt):

- Laptop/Netbook
- Tablet
    - Zuhause
    - im eigenen Besitz
- Smartphone

ZIEL

Die zukünftigen Medienscouts lernen sich untereinander kennen. Durch den Bezug zur Nutzung von digitalen Medien und sozialen Netzwerken wird der Einfluss von Medien in den Alltag der Jugendlichen verdeutlicht.

ZEITLICHER RAHMEN
ca. 30-60 Minuten

TEILNEHMERZAHL
min. 6 TN, nach oben offen

WÜNSCHE, ERWARTUNGEN, HERAUSFORDERUNGEN UND BEFÜRCHTUNGEN

ABLAUF

Die Schülerinnen und Schüler und Lehrerinnen und Lehrer schreiben entweder in Kleingruppen sortiert nach Schulen oder getrennt sortiert nach Schülerinnen und Schülern und Lehrerinnen und Lehrern ihre Wünsche, Erwartungen, Herausforderungen und Befürchtungen auf Moderationskarten. Diese werden am Ende geclustert und an einer Pinnwand aufgehängt.
Digitale Alternative: Die Wünsche, Erwartungen, Herausforderungen und Befürchtungen können auch digital mithilfe von mentimeter gesammelt werden.

Mögliche Fragen:

- Welche Wünsche bringe ich mit für die Ausbildung?
- Was sind meine Erwartungen an die Ausbildung?
- Was muss heute passieren, damit ich am Ende des Tages nach Hause gehe und sage, dieser Tag hat sich gelohnt?
- Wie können die Referierenden dabei unterstützen?
- Was sind die Herausforderungen, die sich bei der Ausbildung stellen werden?
- Was soll auf gar keinen Fall während der Ausbildung passieren?
- Was sind Befürchtungen, die ich bei der Ausbildung habe?

Ziel

Die Antworten werden besprochen und ggf. noch einmal näher nachgefragt durch die Referierenden, um Unklarheiten zu beseitigen. Die zukünftigen Medienscouts und Beratungslehrkräfte werden sich verschiedener Dinge bewusst und die Referierenden können darstellen, was sie während der Ausbildung verwirklichen können und nehmen Ängste.

ZEITLICHER RAHMEN
ca. 30-60 Minuten

TEILNEHMERZAHL
min. 6 TN, nach oben offen

1.4 SEITE 1

WORKSHOP
INTERNET & SICHERHEIT

HINFÜHRUNG ZUM THEMA „INTERNET & SICHERHEIT“ – VIDEOS ZUM EINSTIEG

Arbeitsaufträge

1. Bitte schaue dir das Video an.
2. Notiere danach kurz in Stichworten deine Eindrücke/Gedanken/Ideen in die rechte Spalte.
3. Welches Problem wird dargestellt? Bitte sprich mit der Gruppe darüber.
4. Wie fandest du den Film? Formuliere deine Meinung!

„Wo ist Klaus? http://www.klicksafe.de/spots	
Surfen. Aber sicher! **Spot der polizeilichen Kriminalprävention** https://www.youtube.com/watch?v=RMxyZsA2AKg	
Sheep Spot **„Oben ohne Pelz – Problematische Fotos im Netz“** https://www.youtube.com/watch?v=tVY5X1-cbVo	
Sheep Spot **„Der verheimlichte Freund – Grooming“** https://www.youtube.com/watch?v=frq3nj81GAM	
Sheep Spot **„Weiße Schafe – Rassismus im Netz“** https://www.youtube.com/watch?v=LSVlAZld0Ew	

1.4 SEITE 2

WORKSHOP
INTERNET & SICHERHEIT

HINFÜHRUNG ZUM THEMA „INTERNET & SICHERHEIT“ – VIDEOS ZUM EINSTIEG

“Let’s figtht it together (EU-Spot) https://www.klicksafe.de/spots/	
„Prinzessin“ (EU-Spot) http://www.klicksafe.de/spots Sprache: Rumänisch, Untertitel: Englisch	
„Think before you post“ (EU-Spot) http://www.klicksafe.de/spots	
„Watch your Web“ (Partner-Spots) „Das Internet vergisst nichts“ „Im Internet ist man nicht immer ungestört" „Virtuelles ist real” http://www.klicksafe.de/spots	
„Cybersex“ (EU-Spot) http://www.klicksafe.de/spots	

Arbeitsblätter zu den Themen:

Inhalt

Allgemeines Vorgehen 2
Thema B: Passwörter 5
Thema C: E-Mail und Spam 7
Thema D: Suchen im Netz - Suchmaschinen 8
Thema E: Wikipedia 9
Thema F: Datenschutz und Privatsphäre 10
Thema G: Chats 11
Thema I: Vergisst das Internet? 15
Thema J: Werbung und Abzocke 16
Thema K: Pornografie 17
Thema L: Urheberrecht 18
Thema M: Sexting 19
Thema N: Cybergrooming 20

Allgemeines Vorgehen

Schritt 1: Recherche und Stichpunkte (Zeitrahmen bitte beim Referierenden erfragen)
Ihr braucht dafür pro Gruppe 1 Rechner, Material von klicksafe, Stifte und Block und untenstehende Linkliste

Schritt 2: Erstellung eines Plakats -wenn es nicht anders vorgeben wird- (30 Min)
Ihr braucht dafür Flipchartpapier, Moderationsstifte, Klebestift, Symbole als Kopien

1. Arbeitsauftrag:
Bitte bearbeitet folgende Themen und beantwortet dabei die Fragen mit eigenen Worten. Bereitet das Thema so vor, dass eure Mitschülerinnen und Mitschüler es von euch lernen können!

2. Arbeitsauftrag:
Bitte erstellt ein Plakat zu eurem Thema, sodass die anderen Schülerinnen und Schüler von euch lernen können.
Digitale Alternative: Ihr könnt auch eine digitale Pinnwand bzw. ein digitales Plakat mit euren Ergebnissen mit Padlet erstellen.

Für die Strukturierung eures Plakats könnt ihr folgende Symbole nutzen:

Symbole:

Probleme

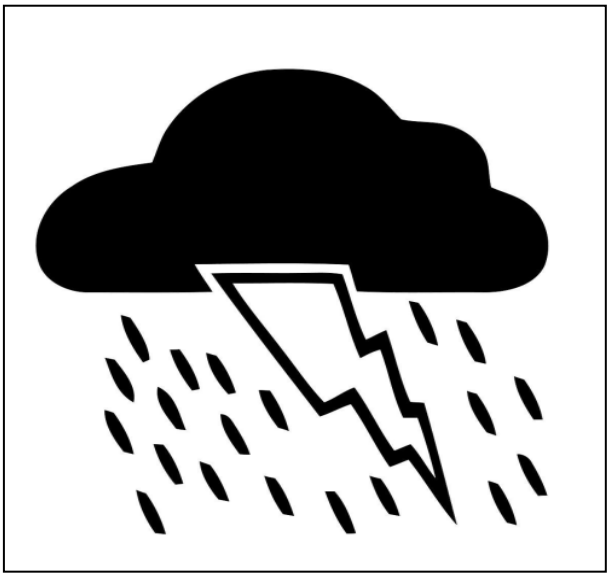
Lösungen

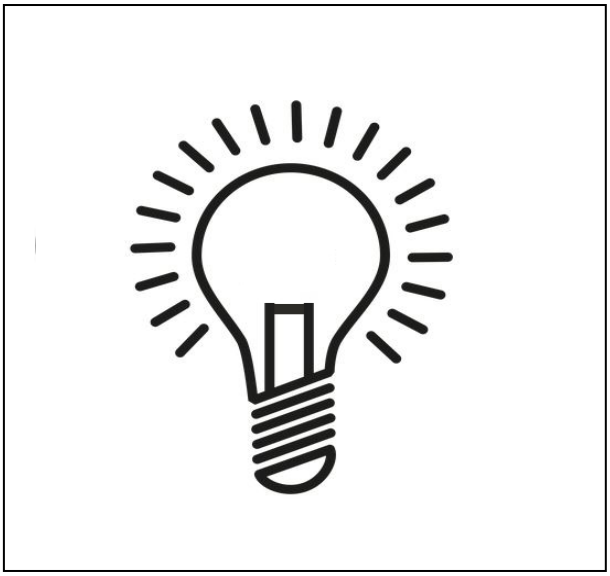
Wichtig zu merken

Tipps für die Bearbeitung:
Lest euch die Fragen durch und teilt sie unter euch auf. Verabredet dann eine Zeit, wann ihr eure Ergebnisse austauscht.

Bevor ihr im Internet oder in den anderen Materialien nachschaut, überlegt erst einmal, ob ihr die Antwort nicht auch selbst wisst. Ihr könnt sie dann anschließend überprüfen.

Symbole als Vorlagen:





Thema A: Technischer Schutz

FRAGEN ZU VIREN UND WÜRMERN:

- Was sind Viren und was sind Würmer?
- Was können sie im Computer anrichten?
- Wie kann man Viren und Würmer verhindern?
- Wie kann man den Virusbefall am Smartphone verhindern?

Fragen zum Windows-Update:

- Wie funktioniert ein automatisches Windows-Update?
- Warum ist es wichtig regelmäßig ein Windows-Update zu machen?

Frage zum Browser:

- Warum ist es wichtig, immer einen aktuellen Browser zu benutzen?

LINKSAMMLUNG:

Klicksafe	https://www.klicksafe.de/themen/schutzmassnahmen/den-pc-schuetzen/
Bundesamt für Sicherheit in der Informationstechnik	https://www.bsi.bund.de/DE/Home/home_node.html
Handysektor	https://www.handysektor.de/artikel/virusbefall-so-schuetzt-du-dein-handy/

MATERIAL:

Titel	**Seiten / Arbeitsblätter / Hinweise**
Klicksafe-Lehrerhandbuch „Knowhow für junge User“	205 - 209 (Schadsoftware)
	229 - 231 (Browser)

TIPP: Bei Unsicherheiten und weiteren Fragen, wende dich an das Team von www.fragzebra.de!

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

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]

Thema B: Passwörter

FRAGEN ZU PASSWÖRTERN

- Was ist ein schwaches und was ist ein starkes Passwort?
- Warum ist ein starkes Passwort wichtig?
- Welche Tipps gibt es für starke Passwörter?
- Wie kann man sich ein Passwort merken?
- „Check Dein Passwort“ (www.checkdeinpasswort.de) Was ist das für eine Seite?
- Wie kann man ein Passwort knacken?

LINKSAMMLUNG

Klicksafe	https://www.klicksafe.de/themen/schutzmassnahmen/den-pc-schuetzen/
Bundesamt für Sicherheit in der Informationstechnik	https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Passwoerter.html
Check Dein Passwort	https://checkdeinpasswort.de

MATERIAL:

Infos:
„PASSWORT-TIPPS“
„PASSWORT-LISTEN“
(als Kopie in eurem Arbeitsmaterial)

Titel	**Seiten/Arbeitsblätter/Hinweise**
Klicksafe-Lehrerhandbuch „Knowhow für junge User“	231 - 240
Klicksafe-Zusatzmodul „Ich bin öffentlich ganz privat – Datenschutz und Persönlichkeitsreche im Web“	29 - 30

den Profil kombiniert werden können. ***Wenn dir das nicht gelingt, wirst du über kurz oder lang zum „gläsernen Menschen".***

• Die Rechte der anderen achten
Wenn du Daten oder Fotos von anderen veröffentlichst, solltest du dich immer fragen, ob du mit der Veröffentlichung entsprechender Daten und Infos einverstanden wärst, wenn sie dich betreffen würden. Wenn das nicht der Fall ist, lass es. Du riskierst eine Abmahnung, Klage und möglicherweise sogar strafrechtliche Verfolgung, wenn du es trotzdem tust. Das ist ein Zeichen von Respekt. Außerdem kann Cyber-Mobbing im schlimmsten Fall zu einem Schulverweis führen. Am besten ist, du fragst vorher direkt bei den Leuten nach!
Jeder hat eine Privatsphäre, nicht nur du. Auch die der anderen muss geachtet und ihre Rechte dürfen nicht verletzt werden. Egal ob im Internet oder in der wirklichen Welt.

• Auf Nummer sicher gehen
Seit es das Internet gibt, geht es auch um die Frage, wie sicher die einzelnen Internet-Anwendungen eigentlich vor „Angriffen" von außen sind. Diese Frage stellt sich auch bei den Sozialen Netzwerken. Die Antwort ist ernüchternd: ***Wie viele Webseiten übertragen auch Soziale Netzwerke nicht immer verschlüsselt! Grundsätzlich kann jeder, der im gleichen (technischen, nicht sozialen) Netzwerk ist wie du, den Datenverkehr im Klartext mitlesen.***
Zu Hause ist die Gefahr noch relativ gering, in fremden Netzwerken wie Internetcafés, Schulen und besonders in ungesicherten WLAN-Netzen dagegen nicht absehbar. Zurzeit verschlüsselt nur XING den gesamten Datenverkehr mit seinen Nutzern. Bei manch anderem Netzwerk ist dagegen sogar die Anmeldung unverschlüsselt. Ein Angreifer kann so direkt deinen ganzen Zugang übernehmen und in deinem Namen Nachrichten schreiben und Schlimmeres tun. Verwendest du das Passwort auch für andere Dienste (z. B. für das E-Mail-Postfach oder beim Internet-Shopping), kann der Schaden noch viel größer werden.

• Räum hinter dir auf!
Wenn du dein Netzwerk nicht mehr nutzen möchtest, solltest du deine Mitgliedschaft beenden und deine Profildaten löschen. Bei einigen Netzwerken ist dies mit wenigen Mausklicks erledigt, bei anderen ist es aufwändiger. Bei facebook etwa ist ein reguläres Löschen des Zugangs gar nicht erst vorgesehen, sondern nur ein Deaktivieren oder Entfernen der Daten. Der Aufwand lohnt sich. Du erschwerst damit das Auffinden deiner Daten. Außerdem bekommst du so immerhin die Chance, dass sie irgendwann von allen Servern und aus allen Caches (Zwischenspeichern) verschwinden. ***Im richtigen Leben machst du ja auch das Licht aus und die Tür zu, wenn du gehst.***

• Wehr dich!
Wenn dich ein unfreundlicher Zeitgenosse beleidigt oder ohne deine Einwilligung Bilder von dir einstellt, dann gilt: Auf Beleidigungen nicht antworten. Denn das ist genau das, was der Angreifer erwartet und erreichen will. Melde den Eintrag dem Betreiber deiner Community. Hol dir Hilfe bei deinen Eltern oder Lehrern. Informiere eventuell Beschwerdestellen, wie etwa **www.jugendschutz.net**. Bei Cyber-Mobbing und massiven Eingriffen in Persönlichkeitsrechte gibt es aber nur eins: die Polizei einschalten. Angriffe sind aber auch auf ganz andere Art möglich, etwa wenn der Netzwerkbetreiber deine Daten entgegen der Nutzungsvereinbarungen weitergibt oder diese Vereinbarungen eigenmächtig ändern will. ***Der Weitergabe deiner Daten kannst du widersprechen und deren Löschung verlangen. Gegen nachteilige Änderungen der Nutzungsbedingungen hilft oft auch ein öffentlicher Protest.***

1 *Ein Grundrecht auf Datenschutz*
2 *Datenschutz im WWW – Ein Überblick über Gesetze*
3 *Big Data*
4 *Datenmissbrauch*
5 *Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung*
6 *Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen*
7 Wie erreiche ich Passwortsicherheit?
8 *Praktische Tipps für Lehrerinnen und Lehrer*
9 *Links, Literatur und Anlaufstellen*

7. Wie erreiche ich Passwortsicherheit?

Um z. B. Kreditkartenbetrug vorzubeugen, sollte man sich trotz verschärfter Vorkehrungsmaßnahmen (z. B. SSL-Zertifikate, erkennbar am Vorhängeschloss in der Browserleiste) zusätzlich einmal mit der eigenen Passwortsicherheit auseinander setzen. Der Zugang zu IT-Systemen wird i. d. R. nämlich über einen Authentisierungsmechanismus geregelt, der im einfachsten Fall eine Benutzerkennung und ein Passwort abfragt. Hierbei sind im IT-System Referenzdaten hinterlegt, gegen die die Eingabe beim Anmeldeprozess verifiziert wird. Zum Schutz der Referenzdaten werden diese zumeist verschlüsselt. Dennoch kann durch Ausprobieren von Zeichenkombinationen ein Passwort ermittelt werden.
Das Ermitteln von Passwörtern wird als „Wörterbuchattacke" (bei Nutzung von Wortlisten) oder „Brute-Force-Attacke" (beim systematischen Ausprobieren aller möglichen Zeichenkombinationen) bezeichnet.

Beispiele:
Ein lediglich 4-stelliges Passwort, das ausschließlich aus Kombinationen der Ziffern von „0" bis „9" besteht (z. B. PIN der EC-Karte) kann in maximal 10.000 verschiedenen Kombinationen auftreten. Wäre es für einen Angreifer möglich, das verschlüsselte Passwort zu lesen, könnte – bei Kenntnis des Verschlüsselungs- oder Hashalgorithmus – das Passwort in maximal 10.000 Versuchen ermittelt werden.

Beispiel 2:
Ein 6-stelliges Passwort, das aus den Buchstaben von „A" bis „Z" und den Ziffern von „0" bis „9" besteht (z. B. Zugangspasswort vieler Internetprovider) kann 2.176.782.336 Kombinationen umfassen. Die Rechnerleistung der heute am Markt erhältlichen Standard-PC, ist ausreichend, um in einem Zeitraum von ca. 3 Tagen alle Kombinationen auszuprobieren.

Beispiel 3:
Im Internet sind verschiedene Listen erhältlich, die Zeichenfolgen einem bestimmten Hashwert zuordnen. Diese als „Rainbow Tables" bezeichneten Listen sind nach verschiedenen Bereichen gegliedert. So gibt es Tabellen, die beliebte Vornamen enthalten. Andere Tabellen enthalten IT-Begriffe, Science-Fiction-Terminologie oder Sportarten. Untersuchungen aus den USA haben gezeigt, dass bei Kenntnis einer Person und deren Neigung durch Auswahl der geeigneten Rainbow Table die Ermittlung der Passwörter deutlich beschleunigt werden kann. Z. B. ist es wahrscheinlich, dass eine fußballbegeisterte Person ein entsprechendes Passwort wählt.

Beispiel 4:
Beliebte Passwörter sind Namen von Freunden, Ehegatten, Haustieren, Sportlern, Schauspielern, Urlaubsorten, weiterhin Geburts- oder sonstige Jahrestage, Kfz-Kennzeichen oder triviale Zeichenfolgen wie z. B. „qwert", „123456" oder „Montag, Dienstag, …". Solche Passwörter können leicht mithilfe automatisierter Routinen ermittelt werden.

Nach der Phishing-Attacke auf Hotmail-Konten analysierten Sicherheitsspezialisten die veröffentlichten Passwörter. Von 9843 Accounts mit Passwörtern (knapp 200 hatten gar keines!) hatten 64 das gleiche Passwort, nämlich „123456".
(Quelle: www.tecchannel.de/sicherheit/news/2022779/phishing_attacke_auf_yahoo_und_googlemail, Stand: 7.10.09, 16.20 Uhr)

Fazit: Gute Passwörter erfüllen mehrere Kriterien!

1. leicht zu merken
2. schwer zu erraten
3. nach kompliziertem Schema aufbauen
4. aus Buchstaben (in Groß- und Kleinschreibung), Ziffern und Sonderzeichen
5. viele Stellen

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]

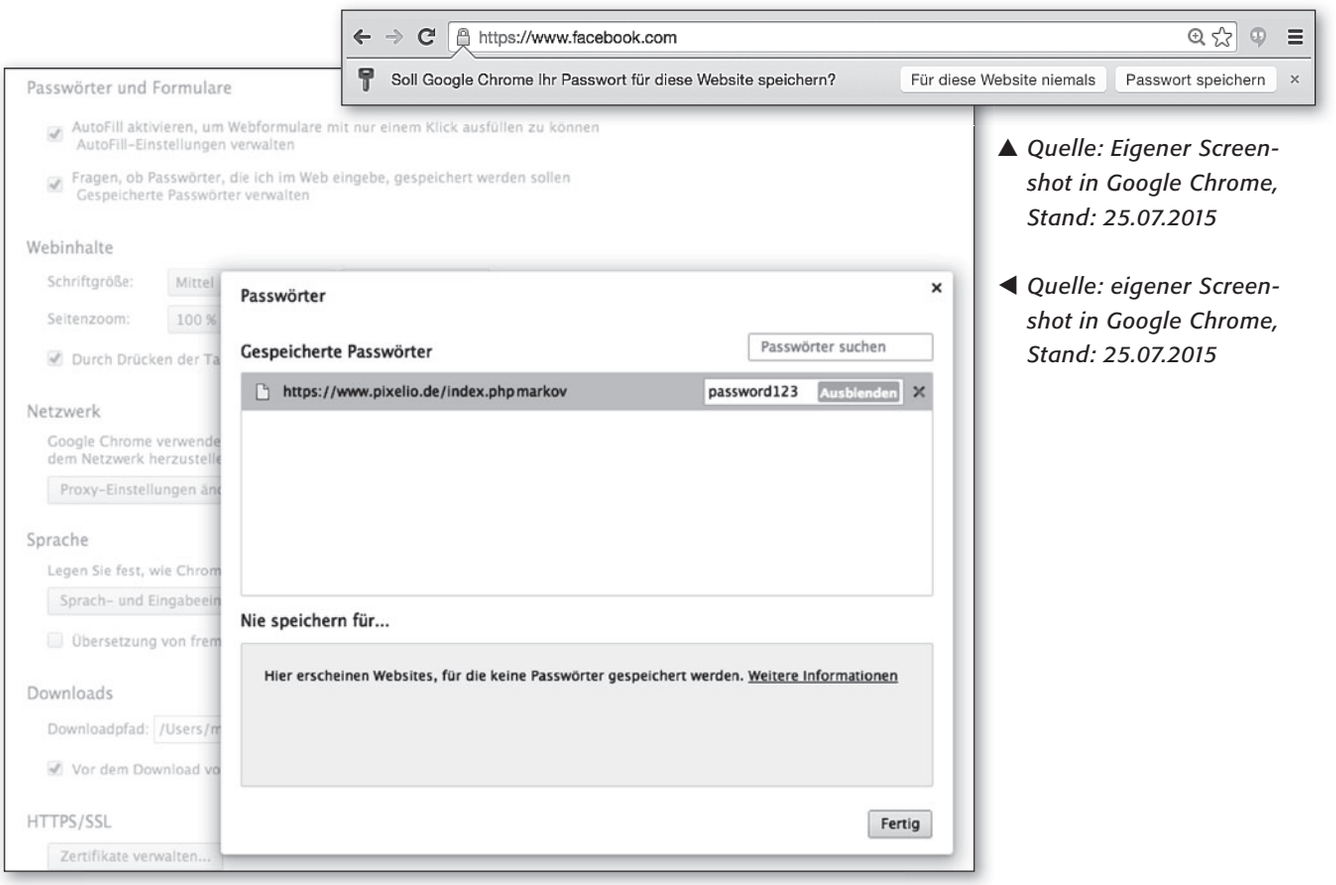
Was wir immer tun sollten: Mindestschutz!
8_1 Kritisches Surfverhalten und Passwörter
8_2 WLANs und fremde Rechner
8_3 Digitaler Fußbabdruck
8_4 Datensicherung und -löschung

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.

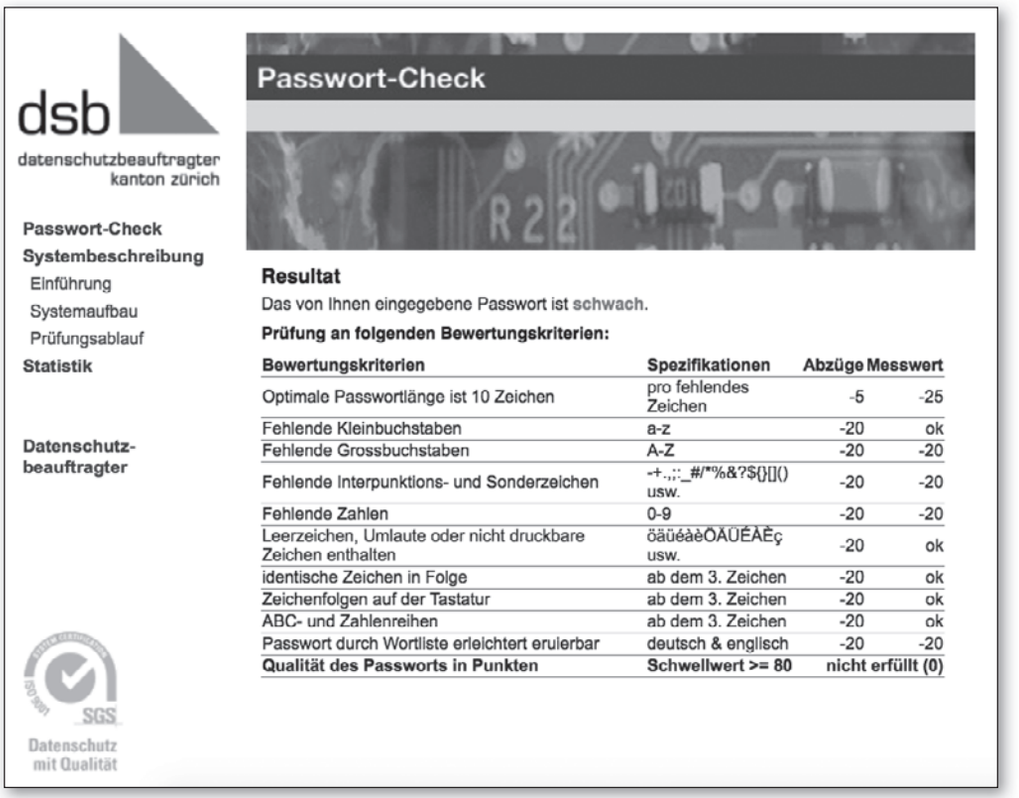
Aus der Praxis

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.

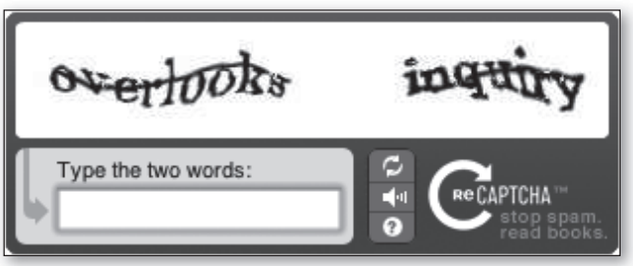
Prüfung an folgenden Bewertungskriterien:

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!

PASSWORT-TIPPS

BEISPIEL PASSWORTERSTELLUNG

Nutze einen Satz, den du dir gut merken kannst. Z.B. „Ich heiße Miriam Mustermann und esse gerne Nudeln“, kürze ihn ab (IhMMuegN) und ergänze ihn mit Zusatzzeichen -z.B. dein Geburtstag oder Ähnliches plus Sonderzeichen (#18IhMMuegN08#).

Für die unterschiedlichen Accounts könntest du dann noch Abkürzungen ergänzen (#18IhMMuegN08#_eb z.B. für ebay).

PASSWORTWECHSEL

In unregelmäßigen Abständen sein Passwort zu ändern, erhöht den Schutz des eigenen Accounts deutlich. Nie dasselbe Passwort für mehrere Accounts verwenden!

URL-BEOBACHTEN

Vor der Passworteingabe immer nachsehen, ob man auf der richtigen Webseite ist und nicht auf einer Seite, die nur genauso aussieht.

PASSWORT-LISTEN: Recht gute Passwörter sind rot markiert

Trotzdem wurden **alle** diese Passwörter geknackt!

chuanshan	One2thr33	Ladycocca1
awes0m3	Delaneybug7	w1nbl00d
Mrminky1	40lei401	Niecie
Ashliej1	ih8laura	Safedriver1
bhuvanbhuvan	Vetemune!	p@$sw0rd
W3bsites	Slatem3	Pulpfict1
Abethebabe1	sejasiap	2oauiodr
513hvandmit	Livefr33	Crossbike7
bondsrus	182953c99vk416	Lugan0
krcdkrcd	k101875k	Paraloft
irq7pozitron	F0rmu1a	Rdxcft67
Krafle76	xxrahmixx	P4ss10n
rekabnala	sandepsandep	CRAZ66Y
All4them	Katoes1	Newstreet1
kaszyca2	Katiekitty	ymenemcm
Kaylaliz3	Gayatrii1	Huntingman3
Kimballl1	This1again	bjerager1
zheshimimi	Angu1lla	marjan!!!
jrzygrl	FINALFELIZ	udahlupA

Thema C: E-Mail und Spam

FRAGEN ZU E-MAIL UND SPAM:

- Welche Probleme kann es für Kinder beim E-Mailing geben?
- Wie viele E-Mail-Adressen sollte man haben und warum?
- Was sind Spam-Mails und welche problematischen Inhalte können sie haben?
- Wie kann man sich vor Spam-Mails schützen?
- Woher kommt der Name „Spam“?
- Was ist eine „Zehn-Minuten-E-Mail-Adresse“ und wozu gibt es sie?

LINKSAMMLUNG:

Klicksafe	https://www.klicksafe.de/themen/kommunizieren/spam/
Internet ABC	https://www.internet-abc.de/kinder/lernen-schule/lernmodule/e-mail-und-newsletter-post-fuer-dich/

MATERIAL:

Titel	**Seiten/Arbeitsblätter/Hinweise**
Klicksafe-Lehrerhandbuch „Knowhow für junge User“	201 - 204 210 - 211

TIPP: Bei Unsicherheiten und weiteren Fragen, wende dich an das Team von www.fragzebra.de!

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/

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 …

Thema D: Suchen im Netz - Suchmaschinen

FRAGEN ZU SUCHMASCHINEN:

- Wie erkennt man Werbung bei Google?
- Welche speziellen Suchmaschinen für Kinder gibt es?
- Wie finde ich mit einer Suchmaschine genau das, was ich suche?
- Welche Tipps und Tricks gibt es?
- Was kann passieren, wenn Kinder mit Google suchen?
- Welche Suchmaschinen außer Google gibt es?
- Wieso sollte man verschiedene Suchmaschinen benutzen?
- Was sind Cookies und warum sollte man sie man bei der Recherche blockieren?

LINKSAMMLUNG:

Klicksafe	https://www.klicksafe.de/suchmaschinen/
Internet ABC	https://www.internet-abc.de/kinder/lernen-schule/lernmodule/suchen-und-finden-im-internet/
Suchmaschine Frag Finn	www.fragfinn.de
Suchmaschine Blinde Kuh	https://www.blinde-kuh.de/index.html
Konrad-Adenauer-Stiftung (für die Lehrerinnen und Lehrer interessant)	http://www.kas.de/wf/doc/kas_21634-544-1-30.pdf?110118165914 (Studie „Bildung und Unterricht in Zeiten von Google und Wikipedia")

MATERIAL:

Titel	**Seiten / Arbeitsblätter / Hinweise**
Klicksafe-Lehrerhandbuch „Knowhow für junge User"	28 - 37

TIPP: Bei Unsicherheiten und weiteren Fragen, wende dich an das Team von www.fragzebra.de!

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

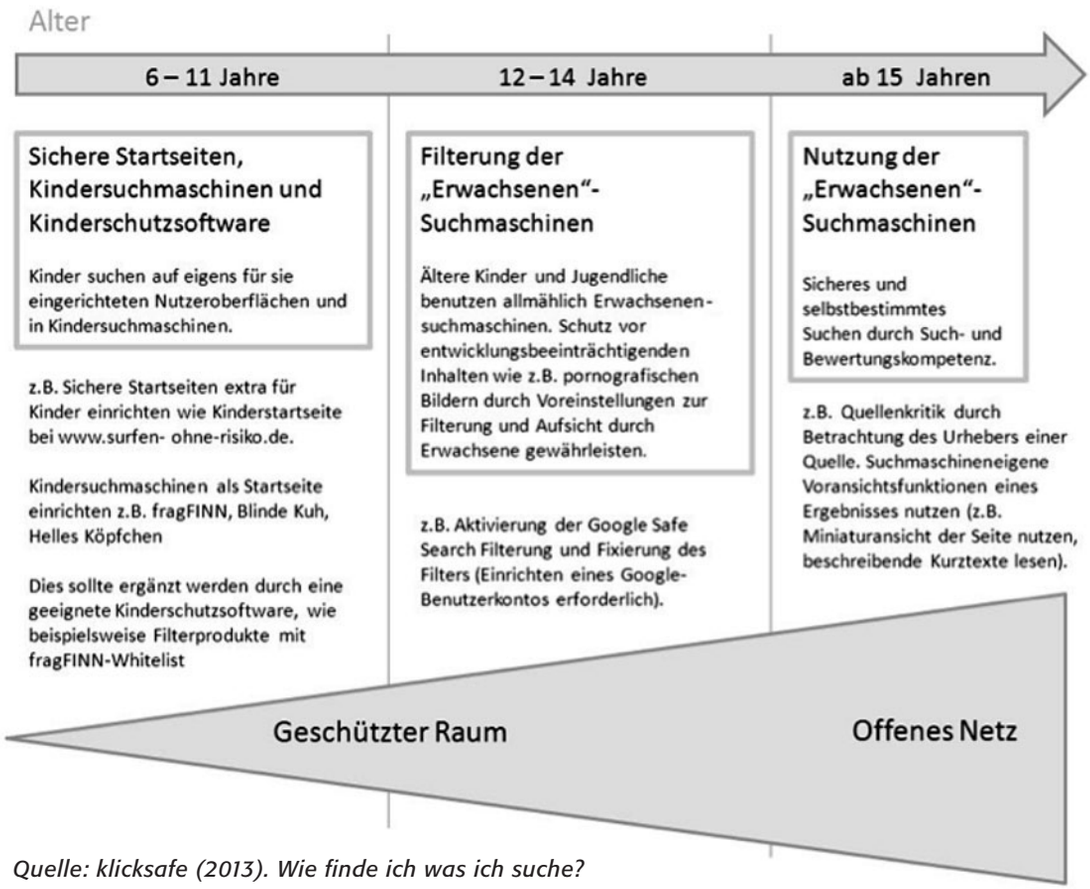
Neben den Websuchmaschinen, die prinzipiell das gesamte öffentlich zugängliche World Wide Web durchsuchen, gibt es eine Vielzahl weiterer Suchmaschinen für spezielle Zwecke, wie Themen- oder Intranet-Suchmaschinen. Andere Suchmaschinen durchsuchen nur eine einzige Domain. So findet z. B. die YouTube-Suchmaschine 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

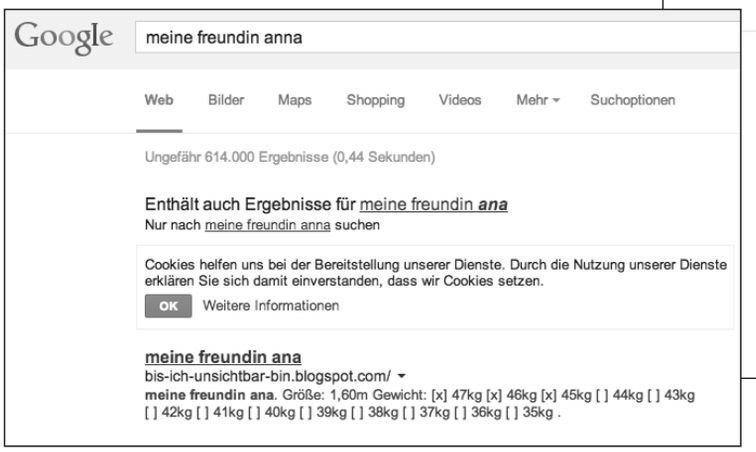
Gerade jüngere Kinder müssen wirksam vor problematischen Inhalten geschützt werden und sollten deshalb (ausschließlich) Kinder-Suchmaschinen wie **www.blinde-kuh.de, www.fragfinn.de** und **www.helles-koepfchen.de** nutzen. Ältere Kinder ab zehn Jahren sollten für die Problematik sensibilisiert werden. 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

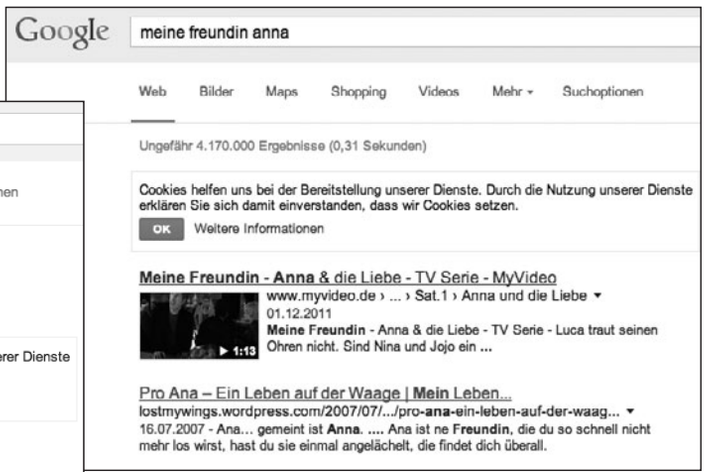
Das Problem beim Jugendschutz

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]

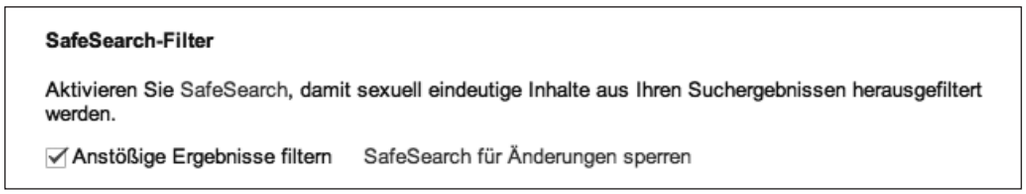
Suchmaschinen und Werbung

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

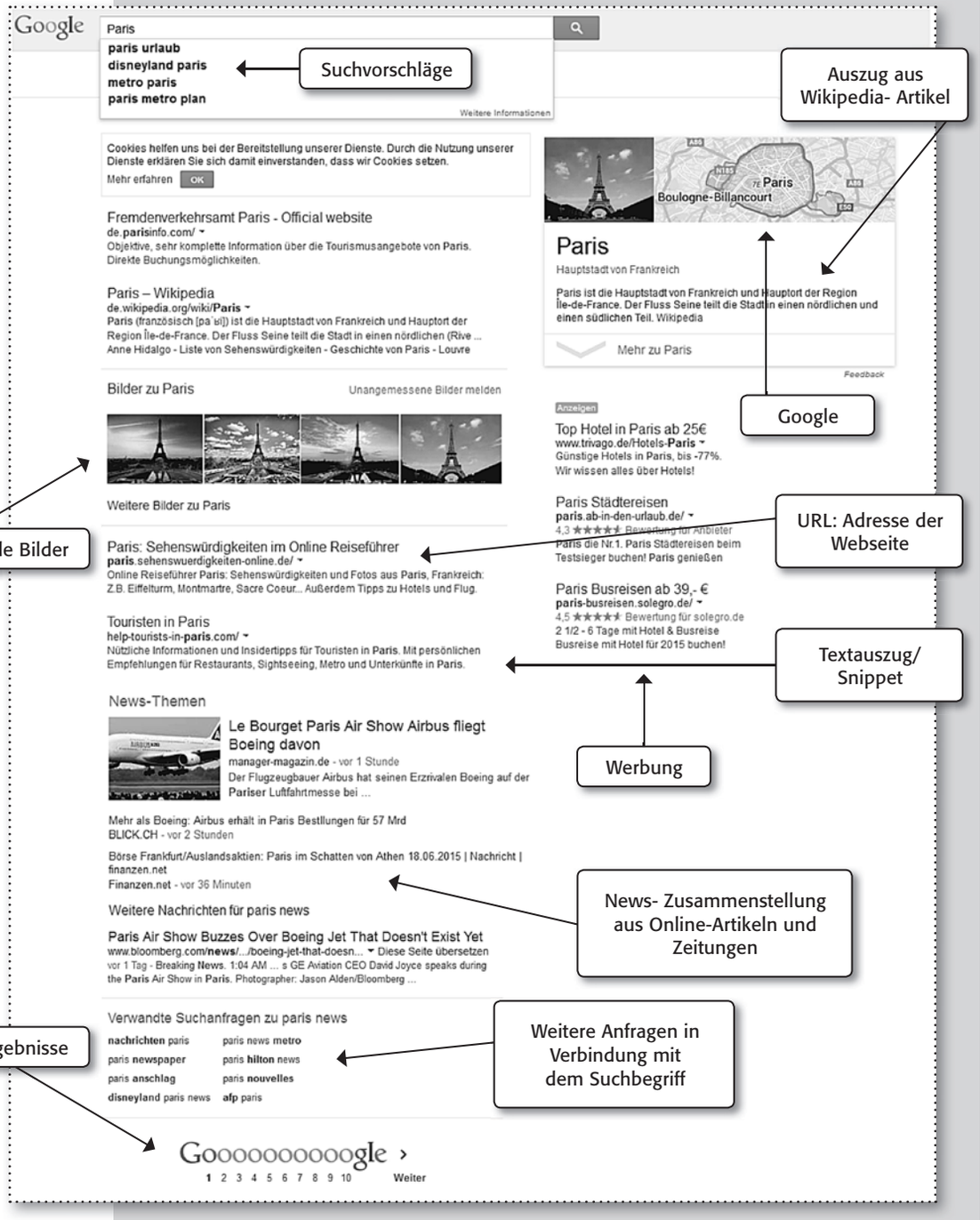
Hinweise für die Durchführung

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**

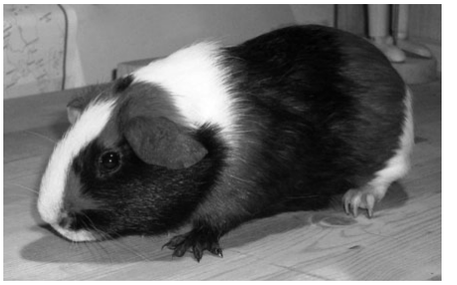
Lust auf mehr?
klicksafe hat ein umfassendes Unterrichtsmaterial zum Thema Suchmaschinen unter **www.klicksafe.de** im Bereich Materialien. Titel: Wie finde ich, was ich suche? Suchmaschinen kompetent nutzen und darüber hinaus Extra-Arbeitsblätter zum Download:
http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Suchmasch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

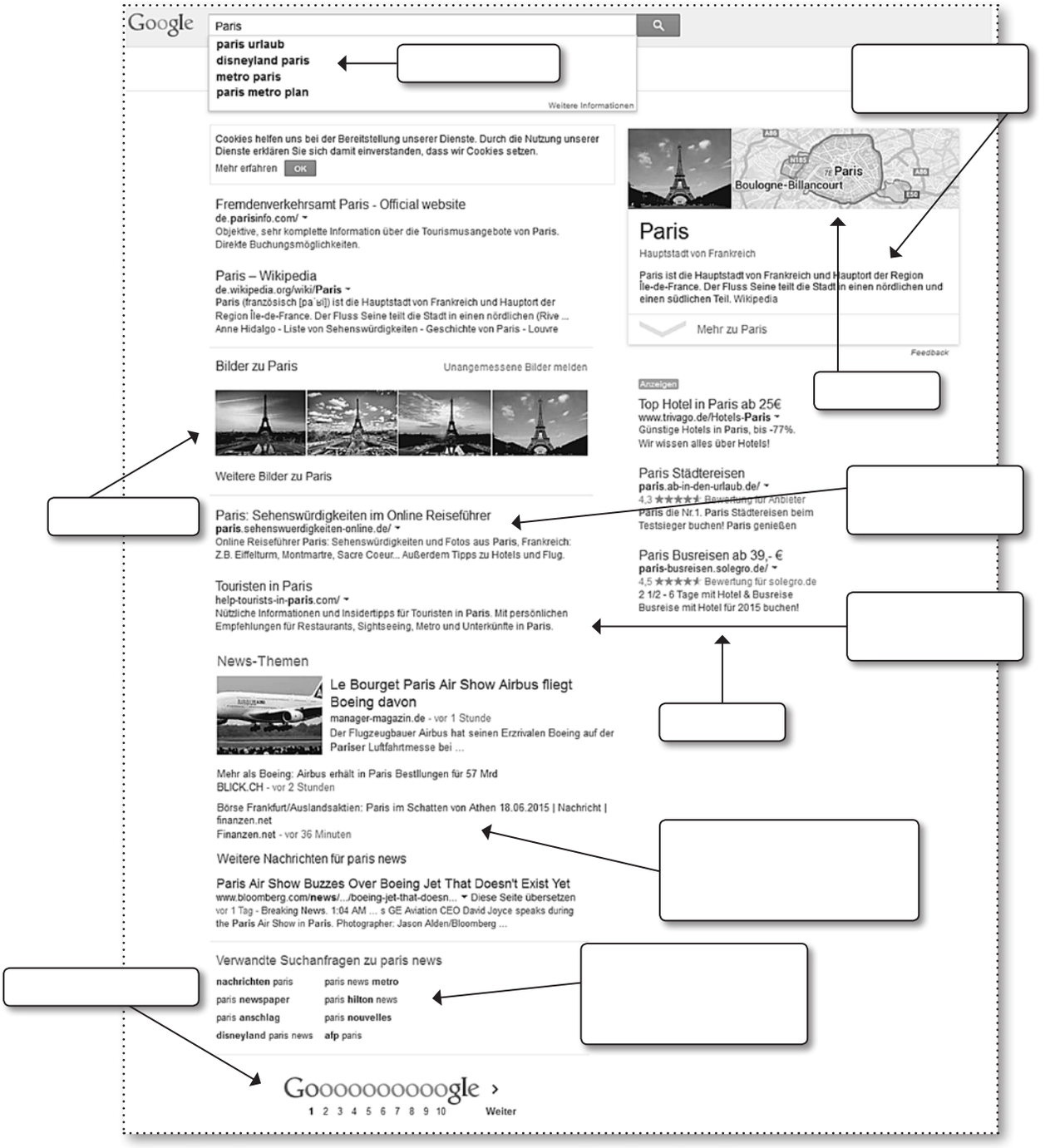
Lies die Vorschau in der Trefferliste genau und überprüfe, ob es auch wirklich das ist, was du suchst. Denn so kannst du Zeit sparen!

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?

1.5 SEITE 9

WORKSHOP
INTERNET & SICHERHEIT

Thema E: Wikipedia

FRAGEN ZU WIKIPEDIA:

- Wie entstand Wikipedia und woher kommt der Name?
- Wie funktioniert Wikipedia, zum Beispiel:
  - Wer darf dort schreiben?
  - Muss man etwas bezahlen?
  - Werden die Inhalte kontrolliert?
  - Was sind die größten Probleme mit Wikipedia? (z.B. in der Schule)
- Schau mal bei „Wikibu“ (http://www.wikibu.ch/) vorbei
  - Was kann man auf dieser Seite herausfinden?

LINKSAMMLUNG:

Klicksafe	http://www.klicksafe.de/wikipedia/
Wikipedia	http://de.wikipedia.org/wiki/Wikipedia http://de.wikipedia.org/wiki/Kritik_an_Wikipedia
Wikibu	http://www.wikibu.ch/ Forschungs- und Entwicklungsprojektes an der Pädagogischen Hochschule PHBern
Konrad-Adenauer-Stiftung (für die Lehrerinnen und Lehrer interessant)	http://www.kas.de/wf/doc/kas_21634-544-1-30.pdf?110118165914 (Studie „Bildung und Unterricht in Zeiten von Google und Wikipedia”)

MATERIAL:

Titel	**Seiten / Arbeitsblätter / Hinweise**
Klicksafe-Lehrerhandbuch „Knowhow für junge User“	38 - 49

TIPP: Bei Unsicherheiten und weiteren Fragen, wende dich an das Team von www.fragzebra.de!

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)?

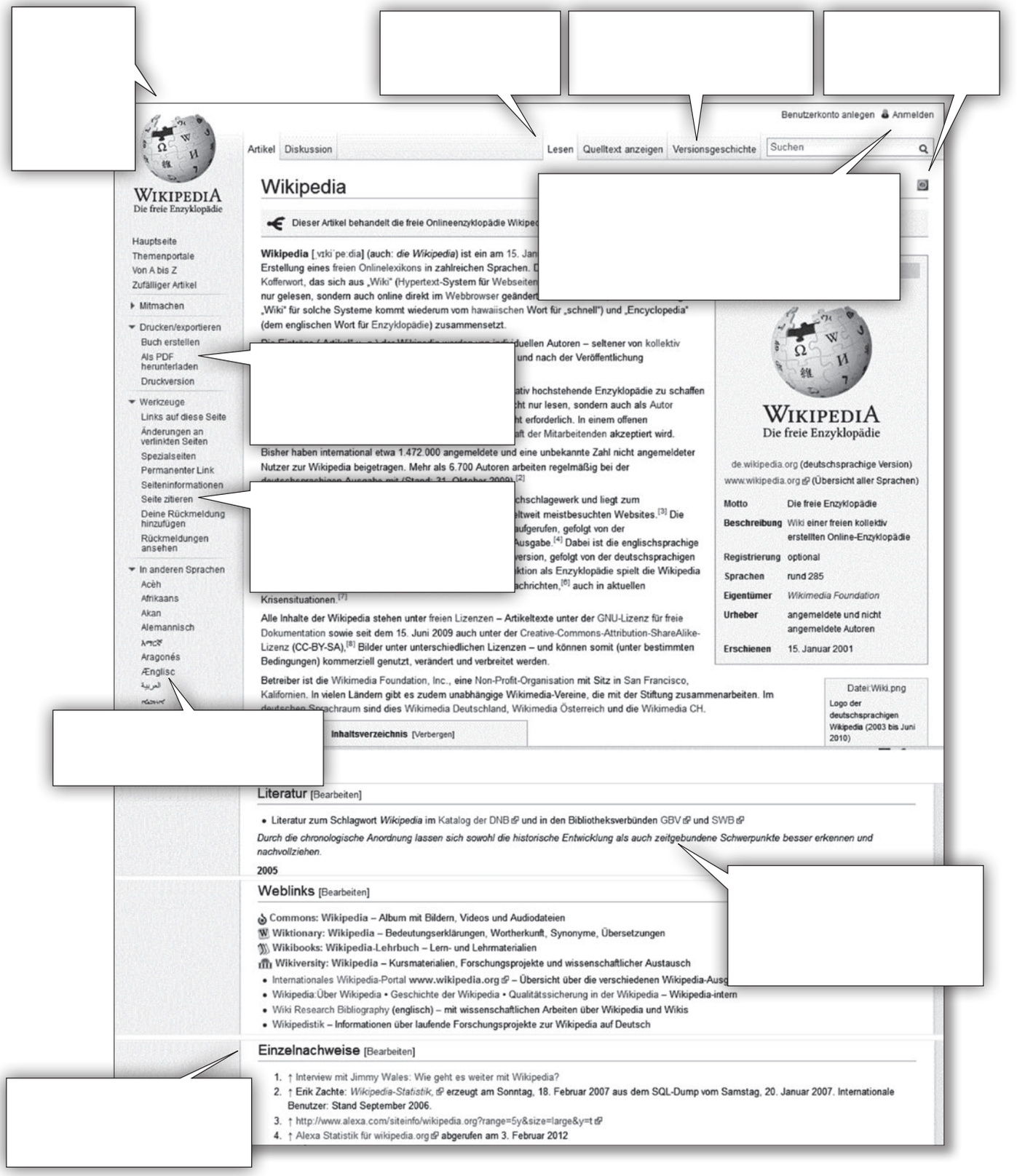
Lust auf mehr?
Methode „Der schnellste Weg“
Die Schülerinnen und Schüler sollen sich mit möglichst wenigen Klicks von einem Wikipedia-Artikel zu einem anderen klicken. Dazu werden vorher 2 Begriffe an die Tafel geschrieben. Die Schülerinnen und Schüler bekommen folgende Aufgabe (hier das Beispiel: von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

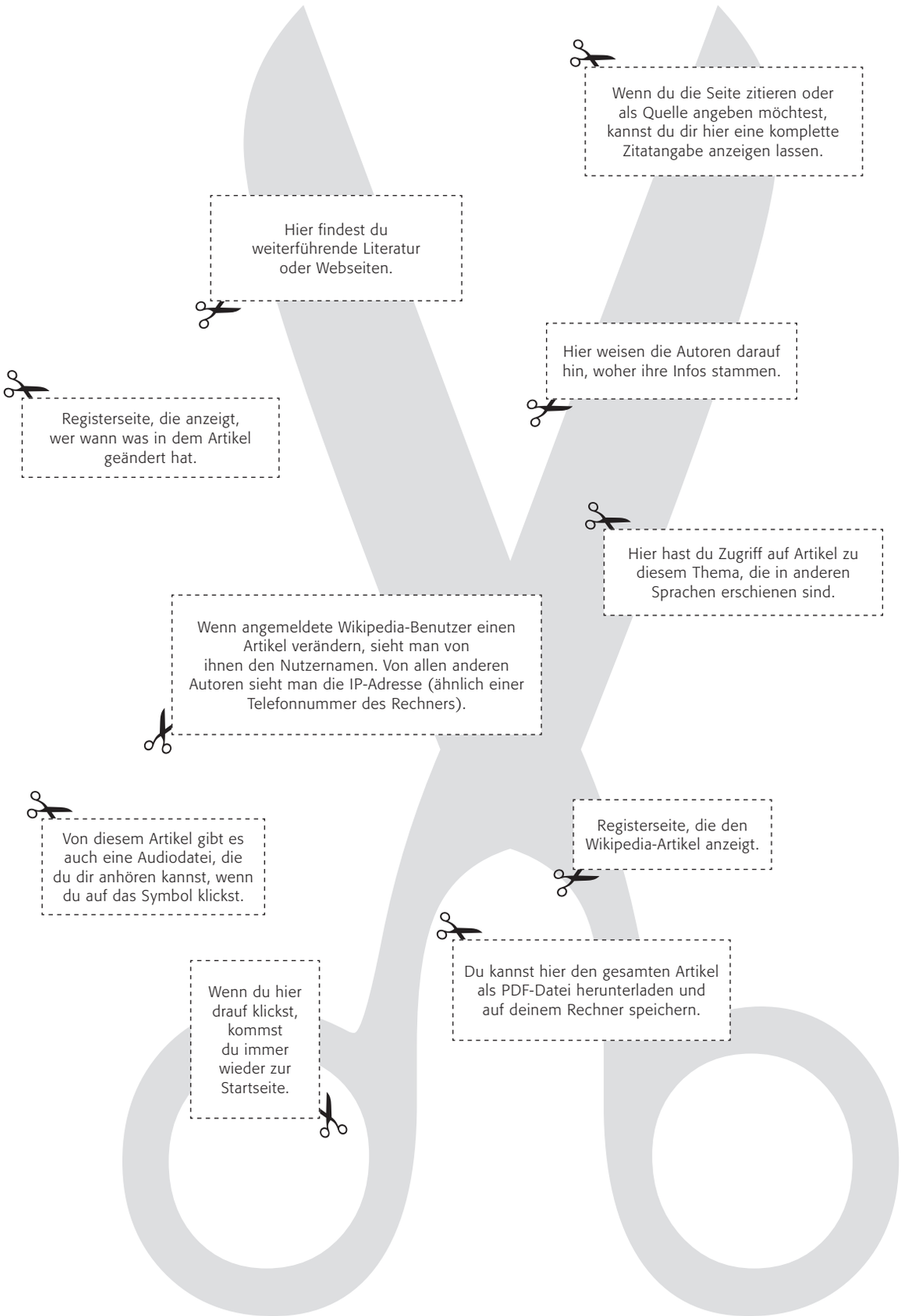
Anderes Beispiel: von Artikel „Harlem Shake“ zu Artikel „Angela Merkel“
Möglicher Weg: Harlem Shake – YouTube – Deutschland – Angela Merkel

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

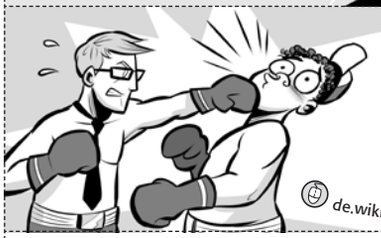
Benutzer, die Seiten absichtlich zerstören – sei es, um einen Artikel oder Teile davon zu löschen oder Unsinn einzufügen.

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".

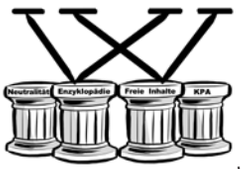
Edit-War („Bearbeitungskrieg")



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.

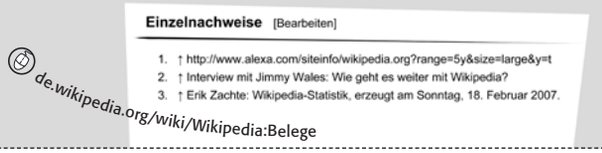
Versionsgeschichte

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

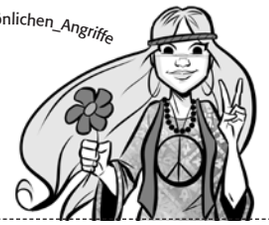


de.wikipedia.org/wiki/Wikipedia:Belege

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.

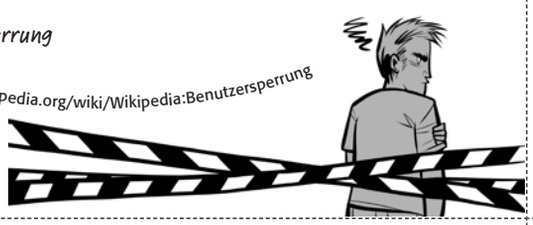
Mentorenprogramm

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

1.5 SEITE 10

WORKSHOP
INTERNET & SICHERHEIT

Thema F: Datenschutz und Privatsphäre

FRAGEN ZUM DATENSCHUTZ:

- Was sind „personenbezogene Daten“?
- Wieso ist Datenschutz wichtig?

FRAGEN ZUR PRIVATSPHÄRE:

- Was ist die „Privatsphäre“?
- Welche Daten sollte man nicht veröffentlichen?
- Welche Dinge sind unproblematisch zu veröffentlichen?

LINKSAMMLUNG:

Klicksafe	https://www.klicksafe.de/themen/datenschutz/datenschutz-grundverordnung/
Internet-ABC	https://www.internet-abc.de/kinder/lernen-schule/lernmodule/datenschutz-das-bleibt-privat/
Virtuelles Datenschutzbüro	https://www.datenschutz.de/

MATERIAL:

Titel	**Seiten / Arbeitsblätter / Hinweise**
Klicksafe-Lehrerhandbuch „Knowhow für junge User“	229 - 231 241 - 247 249 - 263
Klicksafe-Zusatzmodul „Ich bin öffentlich ganz privat – Datenschutz und Persönlichkeitsreche im Web“	siehe Inhaltsverzeichnis besonders die Arbeitsblätter ab Seite 43

TIPP: Bei Unsicherheiten und weiteren Fragen, wende dich an das Team von www.fragzebra.de!

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

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.

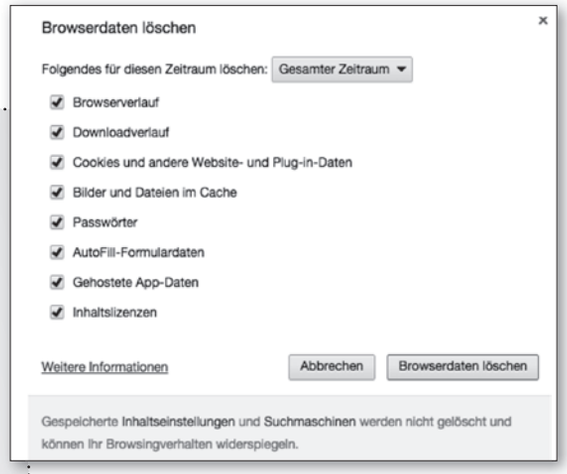
Hier finden Sie ein gutes Video vom WDR in der Sendung „Service-Zeit" zum Thema:
http://www1.wdr.de/fernsehen/ratgeber/servicezeit/sendungen/unsichere-hotspots-100.html

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!)

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

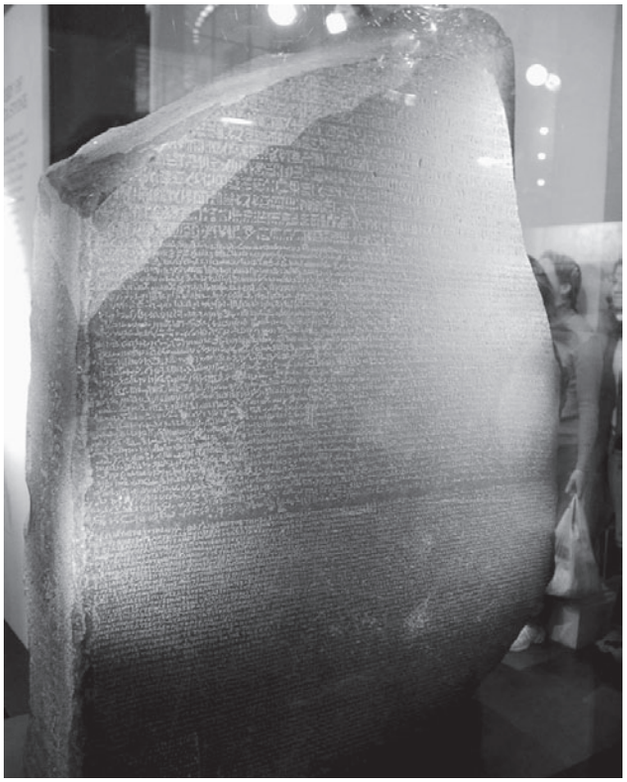
Hinweise für die Durchführung

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!

Thema G: Chats

FRAGEN ZU CHATS (Z.B. IN WHATSAPP, INSTAGRAM, SNAPCHAT)

- Welche Probleme kann es in Chats geben?
- Wie kann man Chats sicher nutzen?
- Was versteht man unter einer „Netiquette“?
  Lest euch u.a. den Text in eurem Arbeitsmaterial durch

FRAGEN ZU GRUPPEN:

- Welche Probleme kann es in Gruppen (z.B. in WhatsApp) geben?
- Wie kann man sicher chatten? Welche Chat-Tipps gibt es?

LINKSAMMLUNG:

Klicksafe	http://www.klicksafe.de/themen/kommunizieren/chat/ http://www.klicksafe.de/themen/kommunizieren/whatsapp/ https://www.klicksafe.de/fileadmin/media/documents/pdf/Themen/Kommunizieren/Cybergrooming/Poster_Cyber-Grooming_2021_final-web.pdf
Handysektor	https://www.handysektor.de/?id=665&tx_kesearch_pi1%5Bsword%5D=instant+messenger https://www.handysektor.de/artikel/messenger-und-sicherheit-wie-sicher-chattest-du https://www.handysektor.de/artikel/10-goldene-regeln-fuer-den-gruppenchat-in-whatsapp https://www.handysektor.de/fileadmin/user_upload/downloads/Wh

	atsApp-Flyer_handysektor.pdf
Chatiquette	http://www.chatiquette.de/

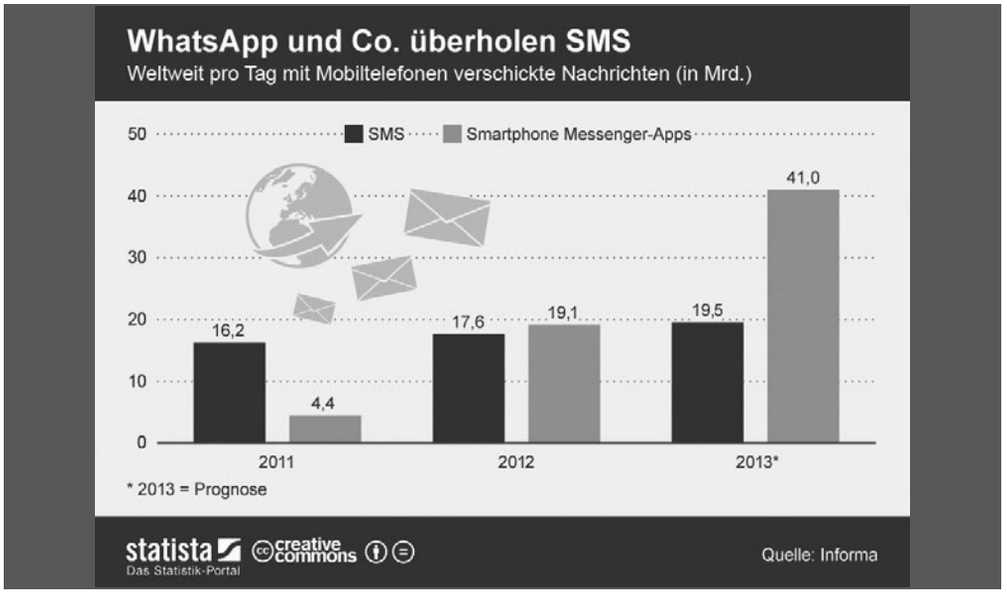
MATERIAL:

Titel	**Seiten/Arbeitsblätter/Hinweise**
Klicksafe-Lehrerhandbuch „Knowhow für junge User“	70 - 75 81 - 82 76 - 78
Chatiquette	Kopie
Klicksafe-Unterrichtseinheit Klassenchat-Regeln	Kopie

TIPP: Bei Unsicherheiten und weiteren Fragen, wende dich an das Team von www.fragzebra.de!

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.

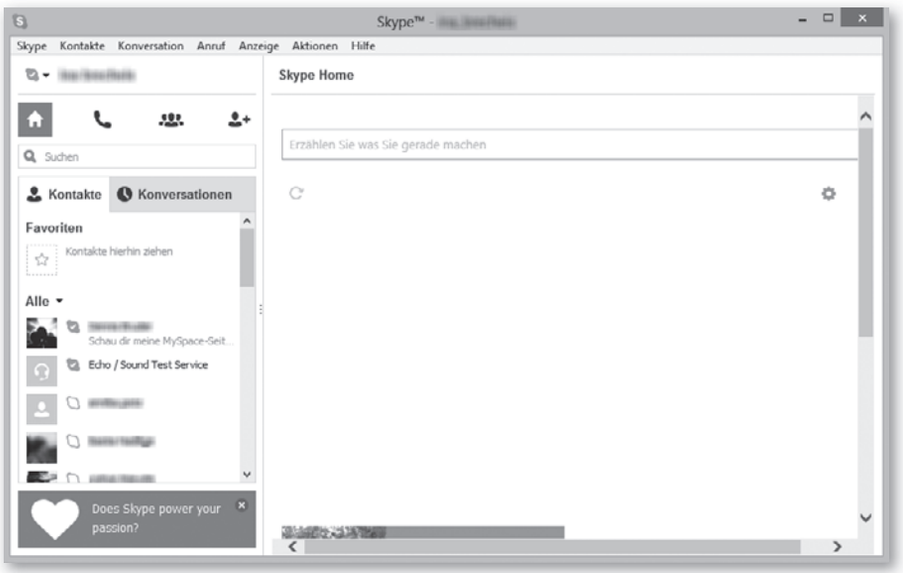
Laufzettel

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.

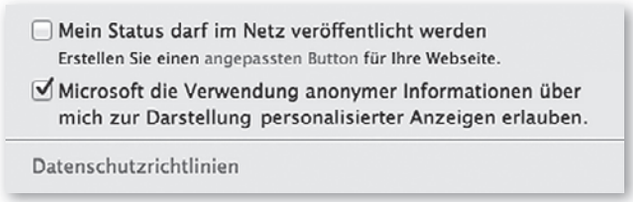
Skypen bietet vielfältige Möglichkeiten. Dazu gehören:

- 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

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.

Netiquette – Wie verhalte ich mich richtig?

Auch bei der schriftlichen Unterhaltung mit Hilfe des Internets, die zum Beispiel über WhatsApp und Co. möglich ist, gibt es, genau wie bei einem persönlichen Gespräch auch ein paar Kommunikationsregeln, die man beachten sollte.

Achte immer darauf, dass deine Posts möglichst eindeutig sind. Die Gefahr von Missverständnissen ist beim Chatten besonders groß, da man den Gesichtsausdruck oder die Tonlage des anderen nicht sehen oder hören kann. Vergewissere dich deshalb immer, ob dein Chatpartner dich richtig verstanden hat. Wenn du unsicher bist, frage nach. Nimm dir die Zeit, deine Nachricht vor dem Absenden noch einmal gut durchzulesen.

Da man die andere Person meistens nicht sieht oder hört, kann es auch vorkommen, dass du sie unabsichtlich mit einer scherzhaften Bemerkung beleidigst. Die Person sieht und hört dein Lachen ja nicht und nicht jede und jeder hat den gleichen Humor wie du. Was dir die Tränen vor Lachen in die Augen treibt, kann die andere Person verletzen. Überlege deshalb genau, was du schreibst. Passende Emojis können helfen Missverständnisse zu vermeiden.

Auch in einem Chat ist es wichtig, die andere Person ausreden zu lassen und sie nicht zu unterbrechen. Warte deshalb immer einen Moment ab, ob dein Gegenüber die Nachricht tatsächlich zu Ende geschrieben hat. Ein Chat ist zudem nicht völlig privat und anders als in einem persönlichen Gespräch bleiben deine Nachrichten gespeichert und noch lange Zeit lesbar. Schreibe nichts, was du nicht auch laut in der Öffentlichkeit aussprechen würdest. Schließlich ist es wie in jedem Gespräch wichtig, im Chat fair miteinander umzugehen, sich nicht zu beschimpfen, zu beleidigen und Rücksicht aufeinander zu nehmen. Behandle deine Chatpartnerin oder deinen Chatpartner so, wie auch du behandelt werden möchtest.

1.5 SEITE 14

WORKSHOP
INTERNET & SICHERHEIT

Thema H: Videoportale (YouTube)

FRAGEN ZU YOUTUBE:

- Wieso ist YouTube kostenlos?
- Was muss ich beim Hochladen fremder Inhalte beachten?
- Wo finde ich die Regeln zur Benutzung von YouTube?
- Welche Probleme kann es bei YouTube geben?
- Stichworte: Urheberrecht/Datenschutz/Cybermobbing/Gewalt/Pornografie

LINKSAMMLUNG:

Klicksafe	http://www.klicksafe.de/themen/rechtsfragen-im-netz/urheberrecht/ https://www.klicksafe.de/themen/kommunizieren/youtube/
Handysektor	https://www.handysektor.de/?id=665&tx_kesearch_pi1%5Bsword%5D=youtube
YouTube	http://www.google.com/support/youtube/bin/request.py?contact_type=abuse&hl=de_DE http://www.youtube.com/t/terms

MATERIAL:

Titel	**Seiten / Arbeitsblätter / Hinweise**
Klicksafe „Kosmos YouTube“	siehe Inhaltsverzeichnis

TIPP: Bei Unsicherheiten und weiteren Fragen, wende dich an das Team von www.fragzebra.de!

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

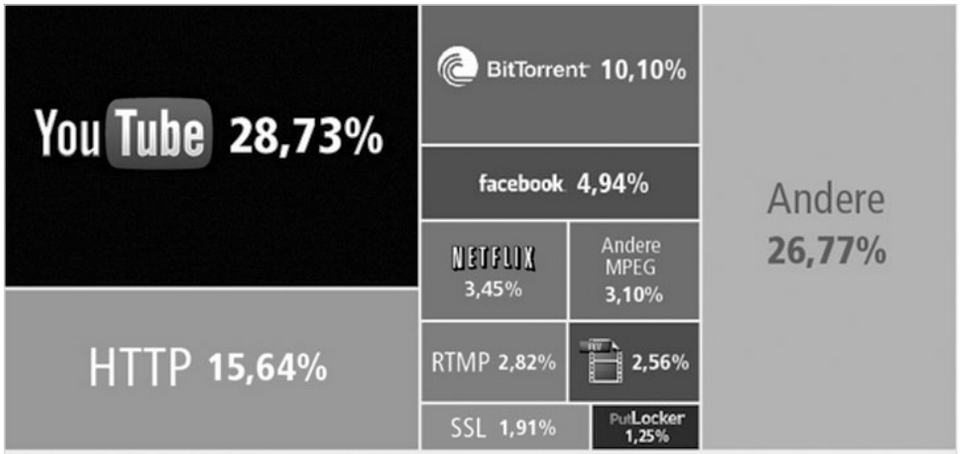
Von Null auf eine Milliarde
YouTube wurde im Februar 2005 von drei ehemaligen PayPal-Mitarbeitern, Chad Hurley, Steve Chen und Jawed Karim, gegründet. Das erste YouTube-Video wurde im April 2005 eingestellt und zeigt Jawed Karim 18 Sekunden lang vor einem Elefantengehege. Rund anderthalb Jahre später, 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.

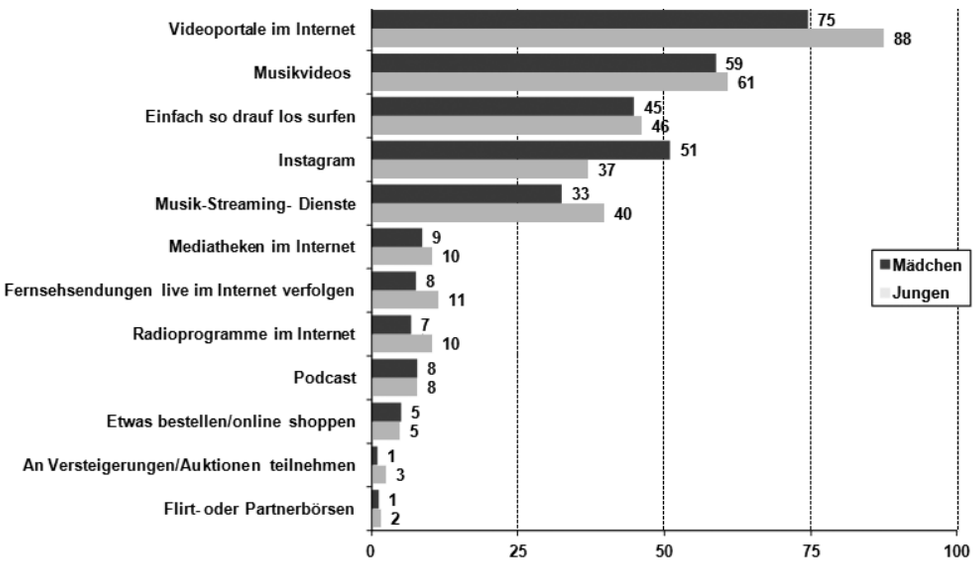
Quelle: Richter (2013)[4]

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/**

1.5 SEITE 15

WORKSHOP
INTERNET & SICHERHEIT

Thema I: Vergisst das Internet?

FRAGEN ZU „VERGISST DAS INTERNET?“:

- Wie und wo kann ein Foto noch gespeichert sein, das ich schon längst gelöscht hatte?
- Wieso kann es problematisch sein, noch Jahre später Fotos und anderes von mir im Netz zu finden?
- Was kann man tun, damit dies nicht passiert?
- Was ist www.archive.org ?
- Was kann ich dort auch nach Jahren wiederfinden?

LINKSAMMLUNG:

Handysektor	https://www.handysektor.de/artikel/comic-das-netz-vergisst-nichts/
Klicksafe	http://www.klicksafe.de/spots/
Archive.org	http://www.archive.org/index.php

MATERIAL:

Titel	**Seiten / Arbeitsblätter / Hinweise**
Klicksafe-Lehrerhandbuch „Knowhow für junge User“	249 - 256 257 - 263
Klicksafe-Zusatzmodul „Ich bin öffentlich ganz privat – Datenschutz und Persönlichkeitsreche im Web“	siehe Inhaltsverzeichnis besonders die Arbeitsblätter 4 (S. 46), 7 (S. 50) und 8 (S. 51-52)

TIPP: Bei Unsicherheiten und weiteren Fragen, wende dich an das Team von www.fragzebra.de!

Arbeitsblatt vom Name:

Was weiß das Netz über mich?

„Karrierebremse Internet" – das stand als Überschrift in der Westdeutschen Allgemeinen Zeitung vom 22.9.2009. In dem Zeitungsartikel steht beschrieben, dass Arbeitgeber das Internet gezielt nach Informationen absuchen, wenn sich jemand für einen Job bewirbt. Und auch der Zeichner Thomas Plassmann hat das Problem in seiner Karikatur „Informationsgesellschaft" beschrieben.

Und diese Suche ist ganz einfach: Du kannst einen Namen „googlen" oder in eine der Personensuchmaschinen wie www.yasni.de oder www.spock.com eingeben. Und schon erfährst du, was das Netz über denjenigen weiß! In diesem Arbeitsblatt darfst du es mal ausprobieren. Du brauchst dafür einen Internetzugang.

Arbeitsaufträge:

1. *Du darfst Detektiv spielen: Finde heraus, was das Internet über dich weiß. Suche nach Informationen zu deiner Person. Fasse die wichtigsten Daten auf einem Steckbrief zusammen. Wenn du nichts über dich findest (gut!), dann suche dir einen Prominenten heraus, vielleicht eine Schauspielerin oder einen Fußballer!*
2. *Welche der gefundenen „personenbezogenen Daten" findest du problematisch, wenn sie im Internet veröffentlicht werden? Suche dir drei Beispiele heraus und erläutere sie deinem Nachbarn!*
3. *Spielt folgendes Rollenspiel: Große Krisensitzung bei Familie Müller. Paula / Paul muss sich in drei Monaten für eine Ausbildungsstelle bewerben. Und Onkel Willi hat sich als Personalchef der Firma Meier mal im Internet umgeschaut … und Paula / Paul hat eine Menge Datenspuren hinterlassen!*

Paula / Paul	Mutter	Vater	Freundin Jana	Onkel Willi
Du gehst recht sorglos mit deinen Daten im Internet um. Deine facebook-Chronik ist öffentlich komplett einsehbar, gegründet hast du die Gruppe „Wir trinken nur Bier an Tagen die mit ‚g' enden. Und Mittwochs." und du hast auch tolle Fotos der letzten Partys und von deinen Freunden veröffentlicht. Außerdem bist du regelmäßig im Blog „Arbeit – Nein Danke!" und schreibst dort Kommentare und, und, und …	Natürlich kennst du Soziale Netzwerke, schließlich brauchst du es für deinen Beruf. Du bist selbst Mitglied bei facebook und du hast dort auch viele Daten von dir veröffentlicht. Dir war nie so ganz klar, dass das auch problematisch werden kann, auch wenn du eigentlich vorsichtig warst bei der Veröffentlichung.	„Was soll nur aus dem Kind werden?" Du bist der Meinung, dass Paula / Paul ohnehin zuviel vor dem Computer hockt. Und du verstehst auch nicht recht, was man dort alles machen kann. Dieses facebook war dir sowieso immer unheimlich.	Du bist ganz vorsichtig mit dem, was du im Netz veröffentlichst und was nicht. Du hast vielleicht 2–3 harmlose Fotos von dir in facebook und bestimmt keine blöden Sachen und auch keine wichtigen persönlichen Daten. Du wusstest schon immer, dass Datenschutz wichtig ist. Aber Paula / Paul wollte ja nie auf dich hören!	Du bist Personalchef bei der Firma Meier. Und du hast in den letzten Jahren immer wieder Job-Bewerber, die alles über sich im Internet stehen haben. Normalerweise lädst du solche Leute gar nicht erst ein – was für ein Bild macht das denn für die Firma? Aber du möchtest deiner Nichte/ deinem Neffen natürlich helfen!

Arbeitsblatt vom Name:

Sicherer werden: Privatdaten-Management

Du hast bis hierhin schon ganz viel über „personenbezogene Daten" gelernt und weißt, was an deren Veröffentlichung problematisch sein kann. Du kennst die Gesetzeslage und weißt, dass das Internet nichts vergisst und auch Arbeitgeber surfen. Doch wie kannst du dich – aus Sicht des Datenschutzes – richtig verhalten? Hier sollst du dir einige Tipps erarbeiten.

TIPPS

	Was ist das Problem?	Tipp
E-Mail	Viele sagen: „E-Mails sind Postkarten, die mit Bleistift geschrieben sind." Das Problem sind die „Authentizität" (ist der Absender echt?) und die Integrität (ist der Inhalt verändert?)	a) Ich schreibe nichts wirklich Privates in E-Mails. b) Ich benutze eine Verschlüsselungs-Software.
WhatsApp	WhatsApp nutzt Handynummern zur Identifizierung und greift deshalb auf das Adressbuch deines Smartphones zu. Die Sicherheit der über WhatsApp übermittelten Daten steht in der Kritik.	a) Ich schreibe nichts wirklich Wichtiges in WhatsApp wie Bankverbindung oder ähnliches. b) Ich gebe meine Handynummer nicht leichtfertig weiter, um mit neuen Bekanntschaften WhatsApp nutzen zu können. c) Ich respektiere die Privatsphäre meiner Freunde im Adressbuch und nutze WhatsApp nicht, wenn diese ihre Daten nicht weitergeben möchten.
facebook	Profilfoto und Titelbild ist für jeden sichtbar. Die Standardeinstellung bei facebook entsprechen nicht den sichersten Optionen. Öffentliche Beiträge können tatsächlich von jedem gesehen werden.	a) Ich überlege mir sehr genau, welche Profil- und Titelbilder ich wähle. b) Ich ändere die Voreinstellungen und wähle immer einen möglichst kleinen Personenkreis als Publikum aus. c) Ich überlege mir sehr genau was ich schreibe und wähle „öffentlich" nur, wenn es wirklich notwendig sein sollte.
Eigene Fotos und Filme	Fotos oder Filme können von deinem Profil oder deiner Seite kopiert und woanders gespeichert werden. Jeder kann sie sehen.	a) Ich veröffentliche keine / nur harmlose Fotos von mir. b) Ich suche regelmäßig in www.yasni.de (und anderen Suchhilfen) nach Fotos von mir. c) Ich schaue die Fotoalben meiner Freunde durch.
Flash-Cookies	Die so genannten Flash-Cookies werden nicht im Browser gespeichert, sondern im Adobe Flash Player.	Ich kontrolliere und lösche diese Supercookies im Einstellungsmanager für den Flash Player.
Internet-Telefonie	Der Inhalt des Telefonats kann abgehört werden.	Ich bespreche nichts wirklich Wichtiges per Internet-Telefonie.
Browser	Deine besuchten Seiten, die Cookies und andere Daten werden gespeichert.	a) Ich ändere die Browser-Einstellungen. b) Ich lösche diese Daten nach jeder Benutzung.
Chat	Alle Daten sind von allen Nutzern einsehbar, du weißt nie genau, wer dein Gegenüber wirklich ist.	a) Ich melde mich mit einem anonymen Nickname an. b) Ich gebe keine Daten (z. B. Adresse, Telefon- oder Handynummer) weiter.
Anmeldungen Websites	Du musst personenbezogene Daten angeben, damit du dich anmelden kannst.	a) Ich gebe nur unwichtige Daten weiter. b) Ich lüge und benutze eine zweite E-Mail-Adresse.
Passwörter	„Schwache" Passwörter können leicht erraten oder geknackt werden.	a) Ich denke mir ein eigenes System für Passwörter aus. b) Ich geben sie nie weiter.
Blogs und Foren	Deine Veröffentlichungen in Blogs und Foren können von allen gelesen werden.	a) Ich schreibe ohne meinen richtigen Namen. b) Ich bin sehr sorgfältig mit dem, was ich schreibe.

Ein kleiner Zusatzauftrag für ganz Schnelle:
Wer noch weitermachen möchte: Auch zu folgenden Stichwörtern findet man Datenschutz-Probleme: Handy, Online-Banking, Gesichtserkennung, W-LAN.

Auch das solltest du bedenken … je mehr über dich im Netz zu finden ist … desto mehr finden auch Bösewichter!

Arbeitsblatt vom **Name:**

Arbeitsaufträge:

1. Lies die Tipps sorgfältig durch. Frage nach, wenn du etwas nicht kennst oder nicht verstehst.

2. Welche der Tipps findest du besonders gut und wichtig für dich persönlich? Lege dir eine TOP-5 Liste an und redet in der Klasse darüber!

3. Erstelle dir eine Mind-Map mit den Tipps. Schreibe sie so auf ein großes Blatt Papier, dass du eine gute Übersicht hast. Du darfst die einzelnen Punkte auch mit Bildern verdeutlichen!

Unter **www.watchyourweb.de** findest du nette Video-Clips zum Thema

Eine Aufgabe zum Weiterdenken Zuhause:
Veröffentlichte Daten werden manchmal mit einem Tattoo verglichen. Stimmt der Vergleich? Was glaubst du?

Arbeitsblatt vom Name:

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 meine E-Mails abrufen vor dem Gang ins Büro, aber … das darf ich heute nicht, denn mein Login ins Internet wird von meinem Anbieter protokolliert mit Uhrzeit und der Nummer des Computers, der IP-Nummer. 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! Und das Auto selbst erfasst auch eine ganze Menge Informationen. 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? Keine Chance! Derselbe Datenspeicherwahn. Besser, ich melde mich sofort krank, 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! Und ich zücke tatsächlich immer die Kunden-Karte, wenn ich in meinem Drogeriemarkt Shampoo und Seife kaufe – wenn ich jetzt daran denke, wird mir schwindlig. Die wissen, was ich wie oft einkaufe! Kein Risiko heute. Ich hole mir noch eine Flasche Cola 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 ohne Datenspuren, oder?

Arbeitsaufträge:

1. Bitte lies den Text genau durch und führe danach ein Partnerinterview durch.
2. Liste auf, wo der Autor des Textes Datenspuren hinterlassen hätte.
3. Geht es dir als Schüler/Schülerin eigentlich auch so? Welche Datenspuren hinterlässt du an einem normalen Tag? Werde ein Daten-Detektiv und spüre auf, wo du Datenspuren hinterlässt. Erstelle auch dazu eine Liste und vergleiche sie mit dem Text!

Methode „Partnerinterview"
Zu zweit mit Partner A und Partner B. Beide lesen, und danach fasst Partner A das Wichtigste zusammen, Partner B wiederholt. Dann Wechsel der Rollen – aber Vorsicht! Jeder darf zwei Fehler beim Nacherzählen des Tagesablaufs einbauen, die der andere finden muss!

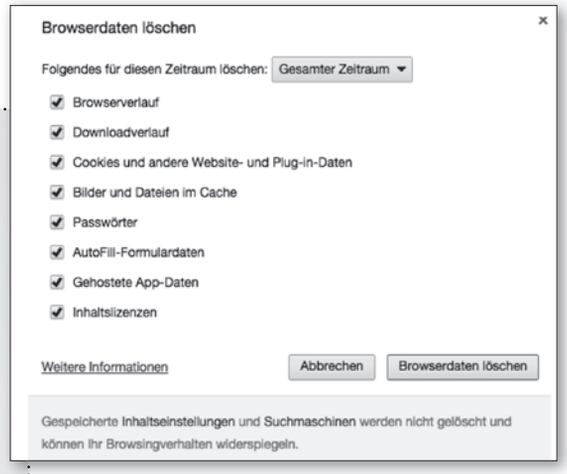
Idee für eine Hausaufgabe:
Kannst du einen Tag verbringen, ohne Datenspuren zu hinterlassen? Schreibe einen Bericht über einen solchen Tag!

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

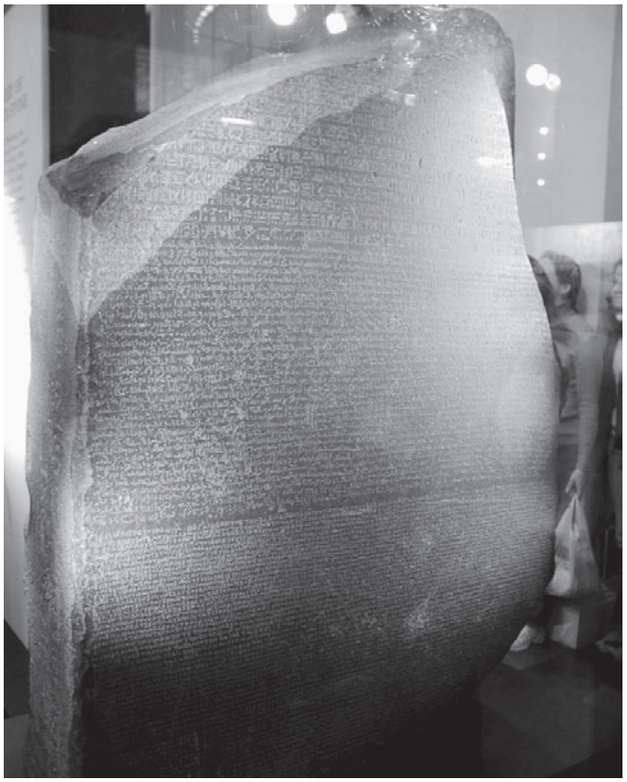
Hinweise für die Durchführung

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!

1.5 SEITE 16

WORKSHOP
INTERNET & SICHERHEIT

Thema J: Werbung und Abzocke

FRAGEN ZU ABZOCKE und WERBUNG:

- Welche unterschiedlichen Werbeformen (z.B. Pop-Up) gibt es im Internet?
- Was bedeutet „personalisierte Werbung“?
- Was bedeutet „Cookie“ im Internet? Was kann man dagegen tun?
- Wie verläuft eine typische Abzocke (= Betrug) im Netz?
- Wie reagiere, wenn ich abgezockt wurde? Welche Tipps gibt es?

LINKSAMMLUNG:

Klicksafe	https://www.klicksafe.de/themen/einkaufen-im- netz/
Handysektor	https://www.handysektor.de/lexikon/eintrag/werbung-pop-ups/

MATERIAL:

Titel	**Seiten / Arbeitsblätter / Hinweise**
Klicksafe-Lehrerhandbuch „Knowhow für junge User“	188 - 197 249 - 250

TIPP: Bei Unsicherheiten und weiteren Fragen, wende dich an das Team von www.fragzebra.de!

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*

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.

1.5 SEITE 17

WORKSHOP
INTERNET & SICHERHEIT

Thema K: Pornografie

FRAGEN ZU PORNOGRAFIE:

- Was ist überhaupt Pornografie?
- Warum kann es für Kinder und Jugendliche problematisch sein?
- Wieso kann es problematisch sein, „sexy Fotos“ von sich ins Netz zu stellen?

LINKSAMMLUNG:

Klicksafe	https://www.klicksafe.de/themen/problematische-inhalte/pornografienutzung/index.html https://www.klicksafe.de/themen/problematische-inhalte/sexting/sexting-worum-gehts/ http://www.klicksafe.de/themen/problematische-inhalte/pornografienutzung/beratung-tipps-und-infos/
Handysektor	https://www.handysektor.de/pornografie/

MATERIAL:

Titel	**Seiten / Arbeitsblätter / Hinweise**
Klicksafe-Lehrerhandbuch „Knowhow für junge User“	S. 137, S. 144
Klicksafe-Zusatzmodul „Let´s talk about Porno“	siehe Inhaltsverzeichnis

TIPP: Bei Unsicherheiten und weiteren Fragen, wende dich an das Team von www.fragzebra.de!

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.

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.	☐	☐

1.5 SEITE 18

WORKSHOP
INTERNET & SICHERHEIT

Thema L: Urheberrecht

FRAGEN ZU URHEBERRECHT:

- Darf man das veröffentlichen: fremde Filme/Fotos/Texte?
- Darf man das veröffentlichen: eigene Filme/Fotos/Texte?
- Was steht im Urheberrecht?
- Was kann bei einem Verstoß gegen das Urheberrecht passieren?
- Was ist eine „Privatkopie“?
- Was kann ich tun, wenn ich eine Abmahnung bekomme?
- Was bezeichnet man als „geistiges Eigentum“?
- Was versteht man unter „Creative Commons“?

LINKSAMMLUNG:

Klicksafe	http://www.klicksafe.de/themen/rechtsfragen-im-netz/urheberrecht/
Handysektor	https://www.handysektor.de/artikel/urheberrecht/
Weitere Infos bei iRights	http://irights.info/
Checked 4you	https://www.checked4you.de/trends-shopping/recht/comic-zu-creative-commons-173547

MATERIAL:

Titel	**Seiten / Arbeitsblätter / Hinweise**
Klicksafe-Lehrerhandbuch „Knowhow für junge User“	145 - 158
Klicksafe-Zusatzmodul „Nicht alles, was geht, ist auch erlaubt. Downloaden, tauschen, online stellen – Urheberrecht im Alltag“	siehe Inhaltsverzeichnis

TIPP: Bei Unsicherheiten und weiteren Fragen, wende dich an das Team von www.fragzebra.de!

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!*

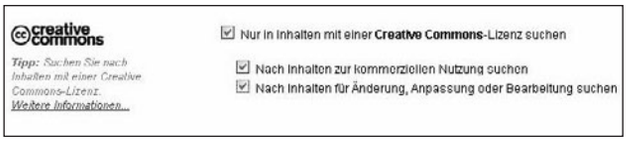


Foto	CC-Lizenz	Autor	Quelle
	by / sa	Thomas Claveirole	http://www.flickr.com/photos/thomasclaveirole/299623633/
	by / nc / sa	affnpack	http://www.flickr.com/photos/affenpack/4635278727/
	by / nd	vince42	http://www.flickr.com/photos/84609865@N00/4998370790/

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)

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.

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

§ 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

1.5 SEITE 19

WORKSHOP
INTERNET & SICHERHEIT

Thema M: Sexting

FRAGEN ZU SEXTING:

- **Was ist Sexting überhaupt?**
- **Warum kann es problematisch werden?**
- **Ist das Weiterleiten von intimen Bildern strafbar?**
- **Ist Sexting erlaubt?**

LINKSAMMLUNG:

Klicksafe	https://www.klicksafe.de/themen/problematische-inhalte/sexting/sexting-worum-gehts/
Handysektor (Video: Dickpicks und Co – Was tun mit Nacktbildern? + Safer Sexting Tipps)	https://www.youtube.com/watch?v=zPrU-zZ8OpI

MATERIAL:

Titel	**Seiten / Arbeitsblätter / Hinweise**
Unterrichtsreihe „Mobile Medien – Neue Herausforderungen“ von klicksafe und Handysektor: Heft 3 Selfies, Sexting, Selbstdarstellung	Siehe Inhaltsverzeichnis

TIPP: Bei Unsicherheiten und weiteren Fragen, wende dich an das Team von www.fragzebra.de!

1.5 SEITE 20

WORKSHOP
INTERNET & SICHERHEIT

Thema N: Cybergrooming

FRAGEN ZU CYBERGROOMING:

- **Was ist Cybergrooming überhaupt?**
- **Ist Cybergrooming strafbar?**
- **Wie kann man Cybergrooming erkennen?**
- **Was kann man gegen Cybergrooming tun?**
- **Ist Cybergrooming verboten?**

LINKSAMMLUNG:

Landesanstalt für Medien NRW (Video: Cybergrooming)	https://www.medienanstalt-nrw.de/medienorientierung/cybergrooming.html

MATERIAL:

Titel	**Seiten / Arbeitsblätter / Hinweise**
Unterrichtsmaterial Landesanstalt für Medien NRW für die Klasse 5 bis 8	Siehe Inhaltsverzeichnis

TIPP: Bei Unsicherheiten und weiteren Fragen, wende dich an das Team von www.fragzebra.de! Auf der Internetseite findest du einen extra Button, mit welchem du Cybergrooming melden kannst!

1.6 SEITE 1

WORKSHOP
INTERNET & SICHERHEIT

LAUFZETTEL

Thema	Raum	Notizen	erledigt
Technischer Schutz			
Passwörter			
E-Mail und Spam			
Suchen im Netz			
Wikipedia			
Datenschutz und Privatsphäre			
Instant Messenger und Chat			

1.6 SEITE 2

WORKSHOP
INTERNET & SICHERHEIT

Thema	Raum	Notizen	erledigt
Videoportale			
Vergisst das Internet?			
Werbung und Abzocke			
Pornografie			
Urheberrecht			

1.7 SEITE 1

WORKSHOP
INTERNET & SICHERHEIT

HAUSAUFGABE

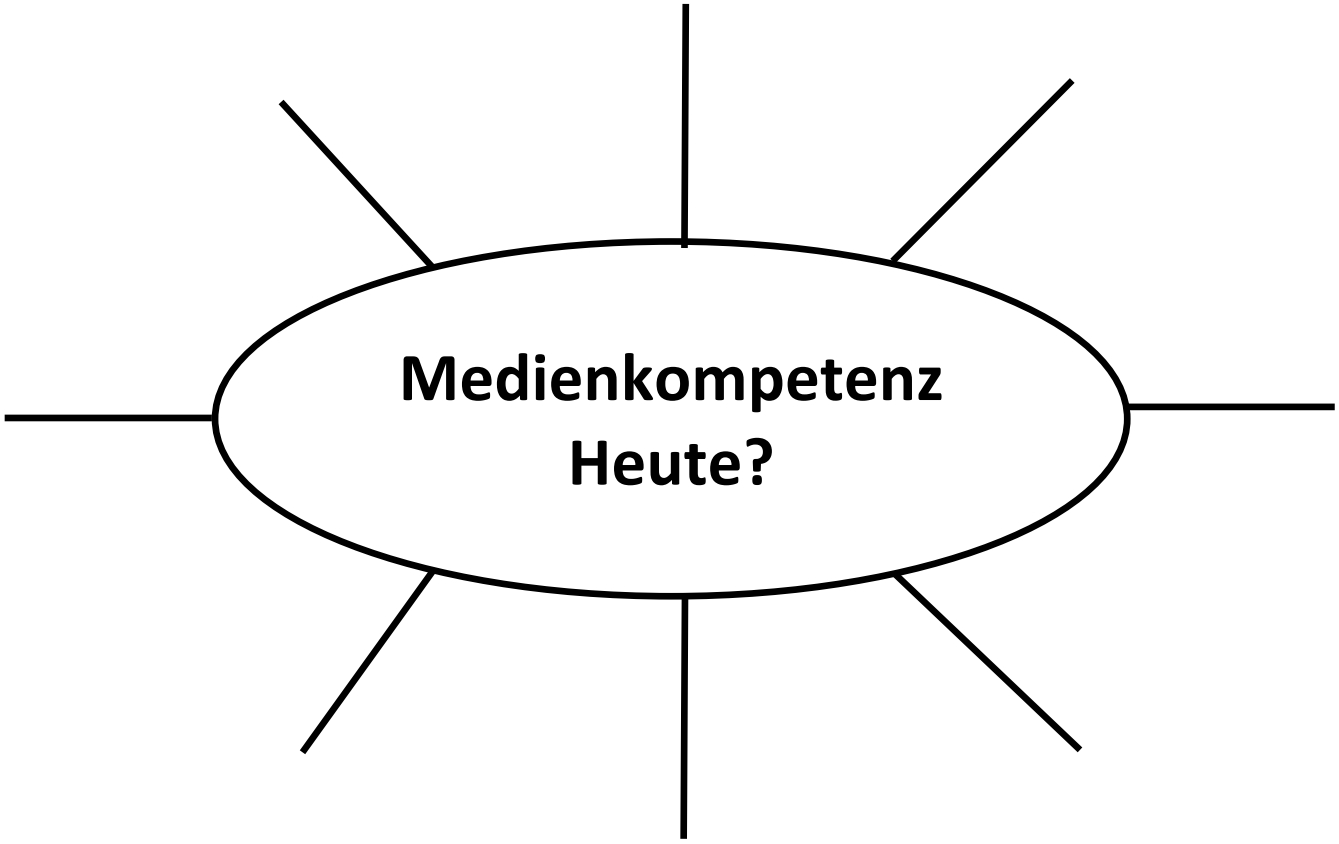
Liebe Ausbildungsteilnehmende,

wir möchten Euch gerne bis zu unserem nächsten Termin und dem Ausbildungsmodul 2 (Thema „Social Media“) folgende Arbeitsaufträge mitgeben:

1. Veranstaltet ein erstes Treffen mit euren Mitschülerinnen und Mitschülern, die an der Ausbildung teilnehmen.
2. Bringt die Liste der Themen in eine neue Reihenfolge (von oben nach unten der Prioritäten). Überlegt gemeinsam, welche der Themen bei euch an der Schule am wichtigsten/dringlichsten sind. (Methodischer Tipp: Erstellt diese Liste zunächst jeder für sich alleine, danach erst eine gemeinsame). Bringt eure Liste bitte zum nächsten Mal mit.
3. Notiert euch offene Fragen der Ausbildung, bringt diese ebenfalls bitte mit.

Thema	**unsere Reihenfolge der Prioritäten**
Technischer Schutz	
Passwörter	
E-Mail und Spam	
Suchen im Netz	
Wikipedia	
Datenschutz und Privatsphäre	
Instant Messenger und Chat	
Videoportale	
Vergisst das Internet?	
Werbung und Abzocke	
Pornografie	
Urheberrecht	

1.8

WORKSHOP
INTERNET & SICHERHEIT

Aufgabe:
Tauscht euch in der Gruppe darüber aus, was „Medienkompetenz“ für euch bedeutet.
Was sollten Jugendliche in Bezug auf Medien heute wissen, können, lernen? Bsp.: Der sichere Umgang mit Passwörtern