8

Was wir immer tun sollten: Mindest-Schutz!

Sachinformation

Passwortepidemie

E-Mail-Konto, Onlineshop, Onlinebanking oder Chat, egal, um welchen Internetdienst es sich handelt: Passwörter (sind übrigens synonym zu Kennwörtern) sind zur Identifizierung des Nutzers unerlässlich. Sie erlauben dem Nutzer, sich vor unerlaubten Eingriffen von Fremden zu schützen. Und wer ein Passwort sucht, sollte es zuerst mit den Namen des Partners/der Partnerin, den Kindernamen und dem Haustier versuchen, denn allzu viele vergeben leichtsinnig Passwörter und erleichtern es den „Bösen Buben" damit. Die Top Ten der Passwörter in Europa: Haustiername, Hobby, Geburtsname Mutter, Geburtstag Familienmitglied, eigener Geburtstag, Name des Partners, eigener Name, Lieblings-Fußballmannschaft, Lieblingsfarbe und Name der Grundschule (erhoben von MacAfee, veröffentlicht in Focus 42/2007 vom 15.10.2007, S.18)

Das Problem

Folgende Punkte sollte man im Umgang mit Passwörtern vermeiden:

- keine im Wörterbuch (Duden) zu findenden Wörter
- keine (Kose-) Namen
- nicht dasselbe Passwort für mehrere Webdienste nutzen
- Passwörter nicht in E-Mails oder Ähnlichem weitergeben
- Passwörter nicht auf einem Zettel in der Nähe des PCs aufbewahren
- vor der Eingabe des Passwortes sollte immer darauf geachtet werden, dass die Webseite nicht über einen Link, sondern selbst angewählt wird (Achtung: Phishing-Mails!)

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-Knacker-Software arbeitet. Sie benutzen eine „brutale" Methode („Brute-Force" genannt) und probieren einfach alle im Duden vorkommenden Wörter aus, per Software geht das innerhalb von Minuten. Der Datenschutzbeauftragte des Kantons Zürich schreibt dazu: „Es existieren neben den reinen Brute-Force und den Hybrid-Attacken weitere Methoden, um Passwörter zu finden. Am Labor für Sicherheit und Kryptografie der ETH Lausanne wurde die Methode „Rainbow Table" entwickelt, bei welcher durch Vorausrechnen einer grossen Anzahl von Passworten ein erheblich schnelleres Finden des Kennworts möglich wird." (Quelle: **www.passwortcheck.datenschutz.ch**)

Vorbeugung

Der beste Schutz ist selbstverständlich die Wahl eines starken Passwortes. Aber wie sollte ein starkes Passwort aussehen? Ein starkes Passwort besteht bestenfalls aus Groß- und Kleinbuchstaben sowie aus verschiedenen Ziffern und Sonderzeichen wie z. B. */%#. Des Weiteren sollten Passwörter mindestens acht Zeichen haben. Damit ein Passwort schwer zu erraten ist, sollte es eine scheinbar sinnlose Zeichenfolge enthalten. Zusammenfassend kann Folgendes festgehalten werden:

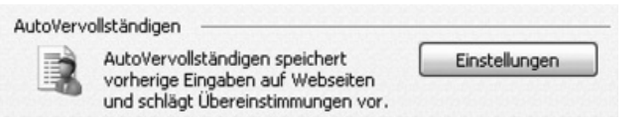
- Das Passwort sollte aus mindestens acht Zeichen bestehen.
- Dabei sollte es sich aus Zahlen, Buchstaben und Sonderzeichen zusammensetzen (Bsp.: 7uz6"Fb4); auf Groß- und Kleinschreibung achten!
- Das Passwort sollte dennoch gut zu merken sein und in angemessenen Zeitabständen gewechselt werden.
- Das Passwort geheim halten.

Ein guter Tipp für die Passworterstellung ist, ein System zu verwenden. So könnten sie bspw. alle „a" in Namen durch die Zahl „1" ersetzen, aus dem Passwort „Andrea" würde „1ndre1". Oder man fügt die Telefonnummer ein, nach jedem Buchstaben eine Ziffer, so würde aus „Willi" und „876530" das Passwort „W8i7l6l5i3". Oder sie merken sich kurze Sätze wie z. B. „Morgens stehe ich auf und putze meine Zähne." und verwenden nur jeweils die ersten Buchstaben: „MsiaupmZ". Welches System auch immer Verwendung findet, man sollte es sich selbst ausdenken, geheim halten und sich gut merken! Weitergehende und ausführlichere Informationen hat das Bundesamt für Sicherheit in der Informationstechnik unter **www.bsi-fuer-buerger.de** (unter „Schützen – aber wie?", „Passwörter") bereitgestellt.
Warum ausgerechnet acht Zeichen? Hier kommen die Mathematik-Kolleginnen und -Kollegen zum Zuge: Die

Menge aller Kleinbuchstaben, Großbuchstaben, Ziffern sowie einiger Sonderzeichen ergibt ca. 80 mögliche Zeichen und damit ca. 1 680 000 000 000 000 mögliche Kombinationen. Bei einem Computer, der eine Million Kombinationen pro Sekunde ausprobiert, dauert es rechnerisch 25 Jahre, die richtige Kombination zu knacken. Bei einer Länge von nur sechs Zeichen habe ich nur noch ca. 262 000 000 000 mögliche Kombinationen. Das ließe sich mit dem o. a. Computer in 36 Stunden schaffen.

Verwaltung der Passwörter

Eine der wohl gefährlichsten Funktionen ist die Möglichkeit, Passwörter vom Computer speichern zu lassen. So werden sie bspw. im Internet-Explorer gefragt, ob Sie das Passwort speichern möchten (Funktion „Auto-Vervollständigen").



Beim nächsten Aufruf der Seite brauchen sie es nicht mehr eingeben. Schön bequem und schön gefährlich. Selbstverständlich kann auch der nächste Benutzer des Computers diese Funktion nutzen und wie sicher ihre Daten auf dem heimischen PC sind, ist im Kapitel 7_2 „Viren, Würmer, Trojaner und Spyware" nachzulesen.

Screenshots: Im Internet-Explorer die Registerkarte „Extras – Internetoptionen – Inhalte – Autovervollständigen Einstellungen. Hier sollten keine Häkchen gesetzt sein.

Screenshots: Im Internet-Explorer 7 die Registerkarte „Extras – Internetoptionen – Allgemein – Browserverlauf löschen". Hier können sie mit einem Klick auf „Alle löschen" alle Passwörter (hier Kennwörter genannt) löschen. Beim Mozilla Firefox 2 ist diese Option unter „Extras – Private Daten löschen" sowie unter „Extras – Einstellungen – Datenschutz" zu finden.

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. man muss sich nur ein Einziges merken. Hier ist Vorsicht geboten: Nur wirklich seriösen Anbietern sollte man Vertrauen schenken.

Passwort-Check
Einige Webseiten bieten die Möglichkeit, sein Passwort zu testen. Man gibt es ein und erhält eine Beurteilung. Auch hier bitte Vorsicht! Nie das tatsächliche Passwort verwenden, sondern nur ein ähnlich aufgebautes, denn wer garantiert, dass die Seite das Passwort nicht speichert? Unter **https://passwortcheck.datenschutz.ch** kann man beim Datenschutzbeauftragten des Kantons Zürich in der Schweiz bspw. beliebige Passwörter auf ihre Sicherheit überprüfen lassen. Man erhält einen detaillierten Prüfbericht mit vielen Kriterien für eine sichere Wahl.

TIPP: Geben sie kein aktuell genutztes Passwort ein. Probieren sie zur Überprüfung ein Passwort aus, welches nach demselben Schema zusammengestellt ist, wie das Passwort, welches sie tatsächlich nutzen.

Captchas
Für Internetanbieter stellt sich das Problem, erkennen zu müssen, ob sich ein Mensch oder eine Software (automatisch) anmeldet. Der Vollständigkeit halber seien noch die bekannten Zerrbilder mit Zahlen- oder Buchstabenkombinationen erwähnt, die man inzwischen bei zahlreichen Anmeldeprozeduren eingeben muss. Diese Symbole heißen „Captchas" (übrigens das Akronym für Completely Automated Public Turing test to tell Computers and Humans Apart) und sollen sicherstellen, dass sich tatsächlich ein Mensch anmeldet und keine Software (sog. „Bots"). Auch diese sind nicht mehr 100%ig sicher und manche Firmen gehen dazu über, Bilder zu zeigen, die wirklich nur Menschen unterscheiden können, aber keine Maschinen.

Links

www.internet-abc.de (unter „Suchen und Finden von A-Z")	Glossar des Internet-ABC
www.sicherheit-macht-schule.de (unter „Schutz der Privatsphäre", „Starke Passwörter")	die Aktion „Sicherheit macht Schule" der Firma Microsoft zum Thema Passwörter
www.klicksafe.de	das Thema Passwörter bei klicksafe.de: „Wie sollte ein sicheres Passwort aussehen?"
www.lizzynet.de/dyn/106731.php	Hinweise zum sicheren Passwort bei Lizzynet von Schulen ans Netz (für Mädchen)
www.secure-it.nrw.de (Pfd-Datei zum Download unter „Angebote für die Schule")	Material der Initiative secure-it.nrw für die Grundschule, mit Thema Passwörter: „Internetfibel für die Grundschule", „Wie sicher ist mein PC?"

Methodisch-didaktische Hinweise

Arbeitsblatt	▶●●	▶▶●	▶▶▶
Zeitangabe (Unterrichtsstunden)	1–2	1	2
Ziele	Die Schülerinnen und Schüler nähern sich spielerisch dem Thema Passwortschutz, indem sie eigene Passwörter anhand verschiedener Systeme entwickeln.	Die Schülerinnen und Schüler wissen Regeln für den Passwortschutz und lernen ein System kennen, mit dem sie sich Passwörter merken können.	Die Schülerinnen und Schüler lernen die gängigsten Methoden zum Passwortknacken und die wichtigsten Bewertungskriterien für sichere Passwörter kennen.
Methode/n	Geheimsprache	Passwortsystem erfinden	Passwortcheck
Organisationsform/en	Einzel, Partner, U-Gespräch, Erwachsenenintegration	Einzel, U-Gespräch	Einzel, U-Gespräch
Zugang Internet **Zugang PC**	nein nein	ja ja	ja ja

Kommentare zu den Arbeitsblättern

▶●●

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. 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 (siehe Sachinformationen oben).
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 letzten Arbeitsauftrages. Hier sollen sie für sich ein System entwickeln, mit dem die Wörter gut zu merken sind. Ich verwende das Beispiel auf der nächsten Seite.
Danach können sie sehr schnell einsehen, dass man mit diesem System viele verschiedene, gute Passwörter erstellen kann, denn ich brauche nur den Ausgangsnamen verändern (eigener Name, Name der Mutter, des Vaters, der Haustiere etc.). In diesem Fall ist auch eine kleine Notiz wie „Mail=Hund“ nicht schlimm, denn niemand kennt das System. „Passwörter niemals verraten“ lautet der Lösungssatz.
Immer 2 Zahlen zusammen nehmen und den Buchstaben davor wählen (Bsp: 16=p;01=a)

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 eine 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://passwortcheck.datenschutz.ch/check** 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 des Schweizer Datenschutzbeauftragten sollte man im Internet nie auf einer unbekannten Webseite ein richtiges Passwort eingeben. Die Tabelle zum 1. Arbeitsauftrag ist oben erläutert.

Die Jugendlichen sollen die Bewertungskriterien für „starke" Passwörter einschätzen, wodurch sie hoffentlich einsichtiger werden. Bestenfalls geben sie sich anschließend sichere Passwörter, die viele der Kriterien erfüllen. Im 2. Arbeitsauftrag ist ein Problem angesprochen, das alle Passwörter haben, die z. B. „§1.C4QM0" lauten: Man kann sie sich schlecht merken. Wie oben erwähnt, Passwörter sollten möglichst in ein merkbares System eingebettet sein.

Möglichkeiten zur Weiterarbeit „Lust auf mehr"

„Sicherheit macht Schule" ist eine Initiative der Firma Microsoft. Sie bietet auf ihren Seiten zwei interessante Unterrichtsideen zum Thema. Die Erste basiert auf der ältesten bekannten Chiffrierung, der Cäsarverschlüsselung, einer Verschiebechiffre: **www.sicherheit-macht-schule.de**. Die zweite Unterrichtsidee behandelt sichere Passwörter: Auch ein historischer Ansatz ist sicherlich spannend, wie z. B. der im Zweiten Weltkrieg spielende Film „Enigma" zeigt.

Arbeitsblatt vom **Name:** .....

Kennst du 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!

Hier ist ein Beispiel für eine Geheimsprache:
160119192315051820051814090513011219 2205181801200514

1. Arbeitsauftrag:
Entschlüssle die Geheimsprache oben! Vergleicht eure Ergebnisse in der Klasse.

Zu einer Geheimsprache gehört immer ein „Schlüssel", mit dem man sie wieder „entschlüsseln" kann.
Hier der Schlüssel der Geheimsprache oben:
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

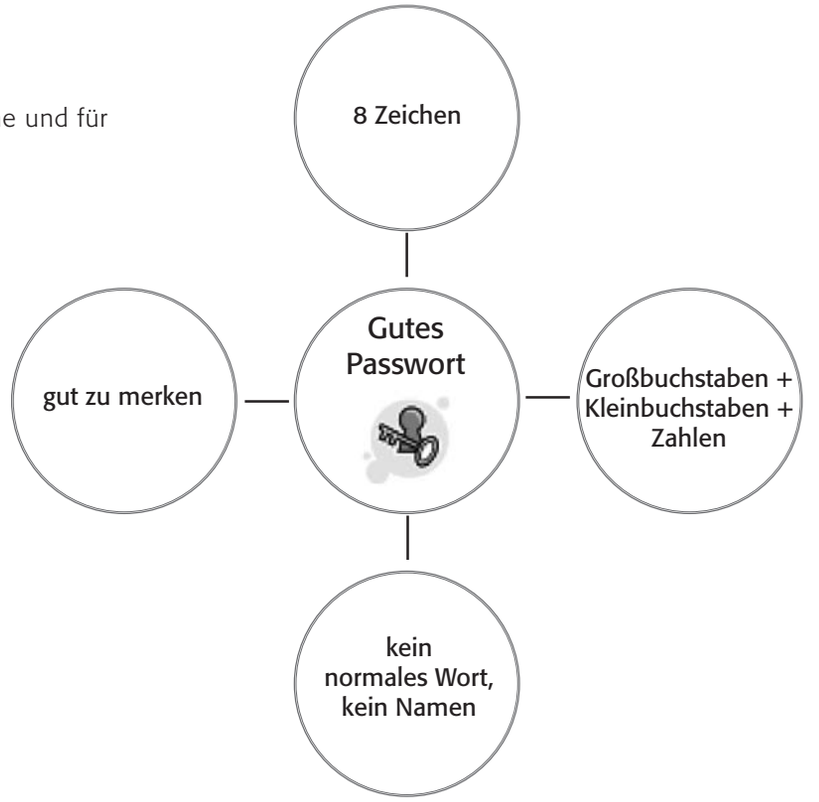
2. Arbeitsauftrag:
Erfinde eine eigene Geheimsprache, in der auch Zahlen vorkommen können.

3. Arbeitsauftrag:
Zeige sie deiner Nachbarin/deinem Nachbarn und lasse sie „entschlüsseln"!

Passwörter sind auch eine Art Geheimsprache und für gute Passwörter gibt es ein paar Tipps:

4. Arbeitsauftrag:
Erfinde gute Passwörter in einer Geheimsprache, die du dann auch für dein Postfach verwenden kannst. Diesmal darfst du sie aber niemandem verraten!

5. Arbeitsauftrag (Hausaufgabe):
Kontrolliere mit deinen Eltern ihre Passwörter! Denke daran: Sie müssen sich ein eigenes System überlegen!



Arbeitsblatt vom **Name:**

Sichere Passwörter – wie geht das?

„Statt vom Computerzeitalter sollte man lieber vom Passwortzeitalter sprechen", stöhnt Jasmin beim Abholen 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 8 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!

Aber wie soll das gehen? 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".**

Merken	Passwort	Beschreibung der Veränderung
Mein Hund heißt:	Naischa	
?	nAIschA	
Meine Telefonnummer lautet 765499	N7A6I5s4c9h9A	
?	(N7A6I5s4c9h9A)	

Wie funktioniert folgendes System? Findest du es heraus?

1. Arbeitsauftrag:
Beschreibe das System oben! Probiere es mit zwei anderen Wörtern aus (zum Beispiel mit deinem eigenen Namen oder deinem Haustier)!

2. Arbeitsauftrag:
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?)

3. Arbeitsauftrag:
Ausnahmsweise darfst du dein System NICHT mit den anderen austauschen! Denke an Jasmin und ihren jüngeren Bruder! Teste es jedoch im Internet:

https://passwortcheck.datenschutz.ch/check.php

Denke jedoch daran, dass du nicht dein echtes Passwort hier testest!

Arbeitsblatt vom Name:

Passwort – ist deines sicher?

Passwörter sind allgegenwärtig. Es gibt kaum eine Anmeldung (und das nicht nur im Internet: Denke mal an die Girokontokarte oder Pin-Nummer beim Handy etc.), bei der ich nicht ein Passwort (= Kennwort) vergeben muss. Und ich muss sie mir alle merken und schützen. Aber wie gelangen Unberechtigte an mein Passwort?

Erraten

Die wohl einfachste Methode ist das Erraten. Noch immer vergeben viele Computernutzer ein Passwort, das sie sich gut merken können. Beliebt sind die Namen der Familienangehörigen, der Haustiere oder des Fußballvereins. Diese Methode heißt unter Experten „Password Guessing" und wird häufiger angewandt als man vielleicht denkt.

Brute-Force

Einfache Passwörter sind auch zu knacken über eine „brutale" Methode, dem „Brute-Force-Attack". Dabei werden die Wörter einfach aus einer Wortliste ausprobiert (z. B. alle Wörter des Dudens werden durchprobiert). Diese Methode funktioniert bei kurzen und einfachen Wörtern gut, hat aber Grenzen, wenn das System nur drei Fehlversuche zulässt (so beim Online-Banking).

Mitlesen

Über spezielle Programme (so genannte „Keylogger"), die auch als „Spyware" bezeichnet werden, kann mitverfolgt werden, welche Tastatureingaben der Nutzer macht.

Auslesen

Spezielle Programme lesen die hinterlegten Passwörter aus, z. B. in Skript- oder Konfigurationsdateien.

Phishing

Auf eine falsche Website gelockt, geben Nutzer ihr Passwort ein und damit weiter (Phishing ist ein Kunstwort aus Password und Fishing).

Proxy-Falle

Bei der Verwendung eines Proxyservers ist es möglich, bestimmte Log-Dateien auszulesen.

Sniffer

Mit diesen „Netzwerkschnüfflern" können Passwörter, die über das Netzwerk übertragen wurden, ausgelesen werden. Besondere Gefahren bergen hier unverschlüsselte E-Mails.

Software

Spezielle Programme können verschlüsselte Passwörter wieder in eine lesbare Form umwandeln.

Es gibt also zahlreiche Gefahren, trotzdem geben starke Passwörter einen besseren Schutz. Hier findest du eine von vielen Adressen mit einem „Passwortgenerator": **www.anonym-surfen.com/service/330-passwort-generator**

1. Arbeitsauftrag:
Probiere diesen (oder einen anderen Passwortgenerator) aus! Formuliere einen Satz, der erklärt, wie starke Passwörter aussehen!

2. Arbeitsauftrag:
Wenn ihr starke Passwörter habt, sind diese sicher, aber welches Problem haben sie dennoch? Besprecht diese Frage in der Klasse!

Arbeitsblatt vom **Name:**

Auf folgender Seite des Datenschutzbeauftragten des Kantons Zürich in der Schweiz kannst du deine Passwörter testen lassen (Aber Vorsicht! Benutze kein echtes, sondern nur ein ähnliches!):
https://passwortcheck.datenschutz.ch/check.php

Der Check benutzt folgendes Bewertungssystem:

Bewertungskriterien	**Spezifikationen**
Optimale Passwortlänge ist 10 Zeichen	pro fehlendes Zeichen
Fehlende Kleinbuchstaben	a-z
Fehlende Großbuchstaben	A-Z
Fehlende Interpunktions- und Sonderzeichen	-+.,;:_#/*%&?${}[]() usw.
Fehlende Zahlen	0-9
Leerzeichen, Umlaute oder nicht druckbare Zeichen enthalten	öäüéàèÖÄÜÉÀÈç usw.
identische Zeichen in Folge	ab dem 3. Zeichen
Zeichenfolgen auf der Tastatur	ab dem 3. Zeichen
ABC- und Zahlenreihen	ab dem 3. Zeichen
Passwort durch Wortliste erleichtert eruierbar	deutsch & englisch
Qualität des Passworts in Punkten:	

3. Arbeitsauftrag:
Erläutere das Bewertungssystem! Warum sind die einzelnen Kriterien wichtig!
Tausche dich mit einer Partnerin/einem Partner aus!

4. Arbeitsauftrag:
Überprüfe deine eigenen Passwörter nach dem Bewertungssystem oben! Beachte aber, dass du dich hierbei nicht mit einer Partnerin/einem Partner austauschst. Immerhin geht es um deine echten Passwörter!

5. Arbeitsauftrag:
Erstelle sichere Passwörter nach einem eigenen System! (Schließlich müssen Passwörter auch noch gut zu merken sein!)

TIPP: 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"**.

Sachinformation

Ob es sich nun um die Bestellung eines Buches bei einem Onlineversandhandel, die Anmeldung einer Internetadresse oder die Teilnahme an einem Gewinnspiel handelt, schnell sind persönliche Daten zur eigenen Person in ein Onlineformular eingegeben. Doch kann man im Internet wirklich so sorglos mit diesen empfindlichen Informationen umgehen? Was passiert nach der Eingabe mit den Daten? Und welche Rechte schützen diese?

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
„Sensitive Daten", wie z. B. Angaben über die Herkunft, politische Meinungen, Gesundheit oder Sexualität.

Geregelt ist der Datenschutz vor allem im Bundesdatenschutzgesetz und in den Landesdatenschutzgesetzen. Speziell für den Bereich des Internets finden sich die Datenschutzregelungen in den §§ 11 ff. Telemediengesetz. 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 die Eingehung 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 Auskunft verlangen – ob bei einem Unternehmen oder einer Behörde – über:

- Daten, die zur Person verarbeitet wurden
- den Zweck der Datenverarbeitung
- die Herkunft der Daten oder weitere Empfänger, an die die Daten weitergeleitet werden
- die Technologien, die zur Verarbeitung der Daten benutzt wurden

Sind die verarbeiteten Daten nicht richtig, so hat man den Anspruch auf Berichtigung, ggfs. auf Sperrung, Löschung oder sogar Schadensersatz.

Im Internet
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 man auf das Recht auf Widerruf und Widerspruch hingewiesen?
- Wer bekommt die Daten noch? Kann man die Weiterleitung ablehnen?
- Wird man 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: https://… statt http://…)?
- Besteht ein Unterschied zwischen notwendigen und freiwilligen Angaben?

Beispiele und Beschwerden
Hier finden sich zwei Beispiele für datenschutzgerechte Angebote: **www.trustedshops.de** und **www.shopinfo.net**, die jeweils mit Gütesiegel und nachvollziehbaren Kriterien arbeiten. Bei Verstößen gegen das Datenschutzgesetz hat man die Möglichkeit, sich bei den jeweiligen Datenschutzbehörden zu beschweren. Eine Übersicht findet sich auf der Webseite des Datenschutzbeauftragten Rheinland-Pfalz unter **www.datenschutz.rlp.de.** Besonderheiten gelten für die Schulen in kirchlicher Trägerschaft.
Bundesbeauftragter für Datenschutz
Friedrich-Ebert-Str. 1, 53173 Bonn, Tel: 0 18 88/77 99-0, Fax: 0 18 88/77 99-550 **www.bfd.bund.de**

Links

www.shopinfo.net	Shop-Info als Beispiel
www.trustedshops.de/de/home	Trusted Shops
www.gesetze-im-internet.de/bdsg_1990	Bundesdatenschutzgesetz (BDSG)
www.gesetze-im-internet.de/tmg	das Telemediengesetz TMG im Wortlaut
www.mekonet.de (Pdf-Datei zum Download unter „Handreichungen“)	Handreichung „Datenschutz“ der Mekonet des Europäischen Zentrums für Medienkompetenz
www.datenschutz.de	Initiative „virtuelles Datenschutzbüro“
www.sicherheit-im-internet.de	Seite der Bundesregierung zum Thema Datenschutz
www.bdf.bund.de/buergerfragen/index.html	Bundesbeauftragter für den Datenschutz
www.secure-it.nrw.de (unter „Angebote für die Schule“)	Unterrichtsmaterialien zum Thema von Secure-IT NRW

Methodisch-didaktische Hinweise

Arbeitsblatt	▶●●	▶▶●	▶▶▶
Zeitangabe (Unterrichtsstunden)	2	1–2	2–3
Ziele	Die Schülerinnen und Schüler werden durch ein Fallbeispiel dafür sensibilisiert, im Internet keine persönlichen Daten preis zu geben.	Die Schülerinnen und Schüler lernen die Bedeutung der informellen Selbstbestimmung kennen und werden dafür sensibilisiert, keine persönlichen Daten im Internet preis zu geben.	Die Schülerinnen und Schüler lernen das Recht auf informelle Selbstbestimmung im Wortlaut kennen, lernen Webseiten auf deren Einhaltung zu überprüfen und sollen Tipps für andere Schüler entwickeln, wie diese sich vor der Weitergabe persönlicher Daten schützen können.
Methode/n	Liste, Lesezeichen	Stichwortliste/Plakat	Recherche, Präsentation, Fragenliste, Flyer
Organisationsform/en	Einzel, Partner, U-Gespräch	Einzel, U-Gespräch	Einzel, Kleingruppen, U-Gespräch
Zugang Internet **Zugang PC**	nein nein	nein nein	ja ja

Kommentare zu den Arbeitsblättern

Kritisches Surfverhalten bedeutet, den gesunden Menschenverstand im Internet nicht auszuschalten. Würden Kinder auf der Straße von Fremden nach ihrer Telefonnummer gefragt, würden sie sicherlich skeptisch, und hoffentlich geben sie keine Antwort. Auf dieses Verhalten, durch die Eltern und durch uns Lehrer trainiert, zielt dieses Arbeitsblatt. Denn selbstverständlich sollen die Kinder im Internet skeptisch bleiben und keine privaten Daten weitergeben, nur weil sie bei einer Anmeldung verlangt werden. Der zweite Arbeitsauftrag stellt die Frage nach dem „Bauchgefühl": „Bei welcher Frage fühlst du dich komisch? Was willst du einem Fremden eigentlich gar nicht sagen?" Hier gibt es kein richtig oder falsch, denn die Antworten sind immer unterschiedlich. Vielleicht schließen sie ein Gespräch darüber an, warum diese Fragen ein solch schlechtes Gefühl verursachen.
Im dritten Punkt schließlich ist ein Bastelauftrag enthalten, das Wichtigste in Form eines Lesezeichens festzuhalten. Dies können sie gerne abwandeln und eine andere Form der Sicherung wählen.

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).
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.

Mithilfe dieses Arbeitsblattes sollen die Schülerinnen und Schüler das Recht auf informationelle Selbstbestimmung überprüfen. Anhand einer selbst gewählten (angegeben sind auch drei Beispiele: MySpace oder YouTube oder schülerVZ) Internetseite, bei der eine Anmeldung gefordert ist, sollen die Jugendlichen Tipps der Initiative klicksafe abarbeiten und die Fragen dazu mit Ja oder Nein beantworten.
Als Vergleich dient ein Onlineshop mit zertifiziertem Datenschutz, wie sie das „Trusted Shop"-Siegel bietet. Auch hier sollen die Schülerinnen und Schüler auf die Suche gehen und vergleichen.
Nach der gegenseitigen Vorstellung der Ergebnisse sollen sie gemeinsam überlegen, wie man bei einem Verstoß reagieren sollte und die Tipps festhalten.
Als Vorschlag ist hier angegeben, eine Information für andere Jugendliche zu realisieren, vielleicht in Form eines Info-Flyers o. ä..

Möglichkeiten zur Weiterarbeit „Lust auf mehr"

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_4 „Digitaler Fußabdruck".

Arbeitsblatt vom **Name:**

Was verrätst du im Internet?

Anna hat eine tolle Seite im Internet gefunden: www.hiergibtestollespielefuerkinder.dex.
(Du brauchst sie nicht auszuprobieren, sie ist frei erfunden).

Tolle Spiele heißt es auf der Seite. Super! Mega! Hyper! Melde dich an!
Und weil Anna alleine zu Hause ist, klickt sie weiter zur Anmeldung. Sie wird gefragt:

Frage	Antworten oder lieber Eltern fragen? Schreibe A oder E!	Das will ich keinem Fremden sagen: Schreibe ein rotes X!
Wie heißt du?		
Wie alt bist du?		
Welchen Spitznamen hast du?		
Wo wohnst du?		
Wie lautet deine Telefonnummer?		
Wie lautet deine Handynummer?		
Wie groß bist du?		
Wie lautet deine E-Mail-Adresse?		
Wie heißt dein Kuscheltier?		
Wie heißen deine Eltern mit Vornamen?		
In welche Schule gehst du?		
In welche Klasse?		
Welche Schuhgröße hast du?		
Wie viel verdienen deine Eltern?		

Anna überlegt. Muss ich das wirklich alles angeben? Ist das gut?

1. Arbeitsauftrag:
Das Beispiel oben ist übertrieben, aber nicht allzusehr. Manchmal wirst du ganz viele private Dinge gefragt, die man besser nicht verraten sollte. Welche der Angaben kannst du machen? Bei welchen solltest du lieber deine Eltern fragen? Schreibe in die Liste hinein:

Hier darf ich antworten = **A.**
Hier sollte ich lieber meine Eltern fragen! = **E.**

2. Arbeitsauftrag:
Überlegt gemeinsam, warum die Menschen, die diese Internetseiten machen, all das wissen wollen.
Ergänzt eure Liste um einen dritten Punkt: Das will ich keinem Fremden sagen!

3. Arbeitsauftrag:
Überlegt auch, wie ihr euch das nächste Mal bei einer solchen Anmeldung verhalten könnt!
Ihr findet sicherlich gute Tipps! Bastelt ein Lesezeichen mit den besten Tipps darauf!

Arbeitsblatt vom **Name:**

Informationelle Selbstbestimmung – was ist das denn?

*Du hast das Recht auf „**informationelle Selbstbestimmung**", was zugegebenermaßen ein schwieriges Wort für eine einfache Sache ist. 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.

1. Arbeitsauftrag:
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. Arbeitsauftrag:
Sprecht gemeinsam im Klassenverband darüber, warum die Menschen, die diese Internetseiten machen, all das wissen wollen.

3. Arbeitsauftrag:
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!

Arbeitsblatt vom **Name:**

Webseite = Datensammler?

> *Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.*
>
> *(Quelle: Bundesverfassungsgericht,* **www.servat.unibe.ch/law/dfr/bv065001.html** *Stand 4.3.08)*

So sieht das „Recht auf informationelle Selbstbestimmung" aus, wie es vom Bundesverfassungsgericht definiert wurde. Mit anderen Worten: Du hast das Recht zu wissen, **wer was wann** über dich weiß.

Auf vielen Internetseiten wirst du bei einer Anmeldung nach persönlichen Daten gefragt. Ist diese Sammelwut immer gerechtfertigt? Die EU-Initiative klicksafe hat Fragen zusammengestellt, mit deren Hilfe du ein Internetangebot überprüfen kannst:

1. Arbeitsauftrag:
Suche dir eine beliebige Internetseite mit Anmeldung aus (du brauchst dich nicht tatsächlich anzumelden. Du kannst bei MySpace oder YouTube oder schülerVZ o. ä. schauen). Überprüfe sie anhand der Fragenliste!

Internetseite	Ja/Nein
Finden sich auf der Internetseite die Kontaktdaten des Anbieters? (Firmennamen, Vertretungsberechtigter des Dienstanbieters, dazugehörige Anschrift mit Telefonnummer, E-Mail-Adresse oder Faxnummer)	
Wird in einer „Datenschutzerklärung" darüber informiert, in welcher Form die personenbezogenen Daten erfasst und verarbeitet werden?	
Welche Daten sind wirklich erforderlich?	
Wird man auf das Recht auf Widerruf und Widerspruch hingewiesen?	
Wer bekommt die Daten noch? Kann man die Weiterleitung ablehnen?	
Wird man 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: https://www… statt http://www…)?	
Besteht ein Unterschied zwischen notwendigen und freiwilligen Angaben?	

Arbeitsblatt vom **Name:**

2. Arbeitsauftrag:
Stelle deine überprüfte Seite der Klasse vor!

3. Arbeitsauftrag:
In der Initiative „Trusted Shops" haben sich Firmen zusammengeschlossen, die besonderen Wert auf Datenschutz legen. Suche dir zum Vergleich eine dieser Firmen aus und recherchiere, wie sie mit persönlichen Daten umgehen:

www.trustedshops.de

4. Arbeitsauftrag:
Bildet Gruppen (3–4 Schüler) und überlegt gemeinsam, wie man reagieren kann/sollte, wenn man keine persönlichen Daten weitergeben möchte. Habt ihr Tipps? Erstellt eine Liste, vielleicht in Form eines Info-Flyers, die ihr z. B. an andere Schüler/Schülerinnen in eurem Alter verteilen könntet!

TIPP: Bei Verstößen gegen den Datenschutz kannst du hier die Beschwerdestellen erfahren: **www.datenschutz.de/beratung**

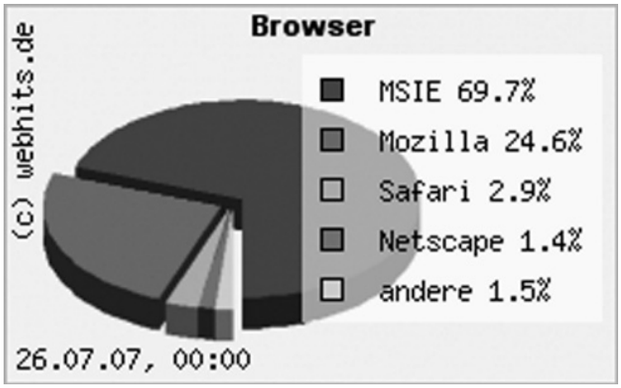
Sachinformation

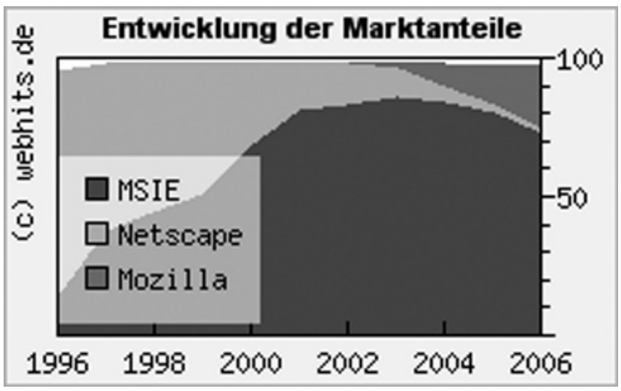
Der Bedeutung des Browsers

Die Software, welche den Zugang zum Internet ermöglicht, heißt „Browser" (vom engl. „Blättern"). Sie ist die Schnittstelle zwischen dem heimischen Computer und dem Internet und somit auch für Sicherheitsfragen sehr wichtig. Der Umgang im Browser mit Passwörtern, aktiven Inhalten, Phishing-Attacken, dem Datenschutz (welche Daten über einen digitalen Ausflug werden wo und wie lange gespeichert?), Werbung in Form von Pop-up-Fenstern, Virenattacken, sicheren Verbindungen mit Verschlüsselungstechniken etc. berühren direkt die Internet-Sicherheit.
Wie kontrolliert man, auf welchen Seiten zuletzt gesurft wurde? In einem ungesicherten Browser ist dies einfach. Der Verlauf der besuchten Seiten wird ebenso gespeichert wie z. B. kleine Dateien („Cookies" genannt), die oft Daten über Uhrzeit usw. beinhalten. Dann noch ein Blick in den Speicher („Cache" genannt) der die Seiten nebst Bildern auf dem Computer zwischenspeichert und es lässt sich gut nachvollziehen, welche Seiten aufgerufen wurden. Sind dazu die Passwörter automatisch gespeichert, liegt die geführte E-Mail-Korrespondenz oder der Bankzugang offen.

Der Browserkrieg

Das letzte Jahrzehnt war geprägt von einem spannenden Kampf um Marktanteile und einem Lehrstück über wirtschaftliche Macht und Monopolstellung. Im Jahre 1996, in den Anfangszeiten des uns bekannten World Wide Web, hatte ein bestimmter Browser einen Anteil von fast 90 Prozent und war unangefochten Spitzenreiter bei der – damals allerdings zahlenmäßig sehr viel kleineren – Gemeinde der Internetnutzer. Elf Jahre später ist dieser Browser namens Netscape Communicator auf einen Marktanteil von 1,4 Prozent degradiert (Quelle: siehe: Statistik). Die Firma Microsoft hat mit Ihrem kostenlosen Browser Internet-Explorer in den letzten Jahren systematisch aufgeholt und besitzt heute einen Marktanteil von fast 70 Prozent (Quelle: ebd.).





Bilder-Quelle:
www.webhits.de/deutsch/index.shtml?webstats.html

Nur ein einziger Konkurrent kann noch ernsthaft als solcher genannt werden: Der Mozilla-Firefox wurde in den letzten Jahren vor allem wg. seiner Sicherheitsstandards und Funktionalität immer beliebter und belegte im Jahre 2007 mit knapp 25 Prozent den zweiten Rang.

Welcher Browser?

Die Frage ist im Jahre 2008 eigentlich nicht mehr so sehr, welchen Browser sie benutzen (ob Internet Explorer 7, Mozilla Firefox 2 oder Opera 9 oder einen der vielen Kleinen wie z. B. Browzar), sondern wie gut sie ihn einrichten und wie aktuell sie ihn halten. Zwei Dinge sollten sie immer tun: Die Sicherheitseinstellungen optimieren und automatische oder regelmäßige Updates machen (lassen).

Internet-Explorer und Firefox

An dieser Stelle soll keine technische Anleitung gegeben werden. Ausführliche Informationen darüber, wie man die beiden Browser Internet-Explorer und Firefox einrichten kann, findet man hier:
Der Autor Ralph Segert hat eine Anleitung für die aktuelle Version Firefox 2 erstellt: **www.firefox-anleitung.net**
Die Computerzeitschrift PC-Welt hat eine Anleitung für die aktuelle Version des Internet Explorers 7 erstellt: **www.pcwelt.de** (unter „Software & OS“). Es seien nur zwei wichtige Stellen genannt: Im Internet-Explorer die Befehle „Extras – Internetoptionen“ sowie diejenigen in „Allgemein“ (Browserverlauf löschen), „Sicherheit“ (Sicherheitszone einstellen), „Datenschutz“ (z. B. Popupblocker) und „Inhalte“ (u. a. Autovervollständigen ausschalten). Im Mozilla Firefox ist das Äquivalent zu finden unter „Extras – Einstellungen“, dann unter „Sicherheit“ und „Datenschutz“.

Der Besuch im Internet-Café

Besondere Vorsicht ist geboten bei allen Rechnern, die von mehreren Personen genutzt werden, wie z. B. in der Schule oder im Internet-Café. Hier sollte man einige Tipps beherzigen:

- alle temporären Dateien im Browser löschen (s. o.)
- wenn möglich, den Papierkorb und die temporären Dateien von Windows löschen (was nicht ganz einfach ist, hier ein Hinweis dazu: **www.pc-magazin.de** (unter „XP Tipps medium“, „Temporäre Dateien löschen“)
- immer den Browser schließen
- wenn möglich – immer Windows herunterfahren
- keine persönlichen Daten eingeben, insbesondere keine Passwörter
- keine sensiblen Seiten – wie das Online-Banking o. ä. – aufsuchen
- Vorsicht beim E-Mailing walten lassen (ändern sie u. U. später das Passwort)

Screenshots: Internet Explorer 7 und Mozilla Firefox

Links

www.netzwelt.de	Anleitung für den Mozilla Firefox: „firefox installieren und einrichten“, Tobias Röhring (20.12.2004)
www.webhits.de	Statistiken zum Einsatz der Browser
www.pc-magazin.de unter „Downloads/Browser: weitere Artikel (Pdf-Datei zum Download)	Artikel: „Browser Test, Geheimsache IE 7“: Internet Explorer 7 wird vorgestellt. Abschließend werden die wichtigsten Browser vergleichend dargestellt; unter „Downloads“, „Browser“: weitere Artikel
www.validome.org/blog/news/Item-127	Statistik Browser-Nutzung im April 2007
www.heise.de (unter „Security“, „Dienste“, Browsercheck“)	Sicherheitslücken bei diversen Browsern und Gegenmaßnahmen

Methodisch-didaktische Hinweise

Arbeitsblatt	▶●●	▶▶●	▶▶▶
Zeitangabe (Unterrichtsstunden)	2–3	2	2–3
Ziele	Die Schülerinnen und Schüler erfahren etwas über die Verwendung eines Browsers, indem sie sich über den Browser auf ihrem eigenen PC/Schul-PC informieren.	Die Schülerinnen und Schüler kennen die Bedeutung von Verlauf, Cookies, Passwörtern und Cache im Zusammenhang mit einem Browser, können Einstellungen verändern und gespeicherte Daten löschen.	Die Schülerinnen und Schüler vergleichen die beiden großen Browser (Internet Explorer und Mozilla Firefox) in einem praktischen Test.
Methode/n	Experten, Elternintegration	Experte	Recherche, Präsentation, Plus-Minus-Tabelle „kooperative“
Organisationsform/en	Einzel/Partner, U-Gespräch	Einzel/Partner, U-Gespräch	Großgruppen, Kleingruppen
Zugang Internet **Zugang PC**	ja ja	ja ja	ja ja

Kommentare zu den Arbeitsblättern

Das Arbeitsblatt soll einen (kleinen) Blick in einen Browser ermöglichen. Die Schülerinnen und Schüler sollen nachschauen, welchen Browser sie in welcher Version besitzen und kontrollieren, ob er aktuell ist. Hier könnten sie helfen, indem sie die aktuellste Version kennen und angeben. Im letzten Schritt könnten die „Experten" unter den Kindern den anderen etwas über die Bedienung beibringen und die wichtigsten Grundlagen vorführen und nachvollziehen lassen.

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 sehen kann, welche Seiten ich aufgerufen habe. Die „Cookies" sind kleine Dateien, die die Anbieter von Internetseiten auf den Computern hinterlassen können (mehr darüber im Baustein 8_4 „Digitaler Fußabdruck"), 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 beim Aufruf einer passwortgeschützten Seite es nicht einzugeben braucht, bei der Unsicherheit der Browser ist dies eine große Sicherheitslücke. 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 Downloads) kann darüber sogar strafrechtlich Relevantes erkannt werden.

Die neueste Generation von Browsern (2008 Internet Explorer 7 und Mozilla Firefox 2) ermöglichen ein Löschen all dieser Daten auf einen Mausklick (beim Internet Explorer 6 waren dazu Klicks an unterschiedlichen Stellen notwendig). Beim Firefox unter „Extras – Private Daten löschen" und im Internet Explorer „Extras – Browserverlauf löschen" und dann jeweils die Einstellung „Alles löschen" o. ä..

Hier sollen die Schülerinnen und Schüler einen kleinen Vergleich der beiden großen Browser (Internet Explorer und Mozilla Firefox) durchführen. Bitte sorgen sie doch im Vorfeld dafür, dass die aktuellsten Versionen zur Verfügung stehen.
Zum 2. Arbeitsauftrag:
Hier können sie auch „kooperativ" arbeiten lassen (siehe Methodenkapitel).
Wahrscheinlich fällt das Fazit nicht eindeutig aus, denn beide Browser haben Vor- und Nachteile.

Möglichkeiten zur Weiterarbeit „Lust auf mehr"

Die modernen Browser bieten viele weitere technische Möglichkeiten, auch des Jugendschutzes. Aus eher technischer Sicht ist vielleicht ein Blick in diese Einstellungsmöglichkeiten und ein kritisches Hinterfragen interessant. Beim Mozilla Firefox findet sich dies unter: „Extras – Einstellungen – Sicherheit bzw. Datenschutz" und beim Internet Explorer „Extras – Internetoptionen – Sicherheit bzw. Datenschutz".

Arbeitsblatt vom Name: .....

Weißt du was ein Browser ist?

Ein **Browser** ist das Programm, mit dem du im Internet surfen kannst. Jemand hat mal gesagt: Im Internet surfen ohne Browser ist wie Autofahren ohne Auto. Es geht einfach nicht. Der Name „Browser" [gesprochen Brauser], stammt vom englischen Wort „to browse", was „durchblättern, schmökern, sich umsehen" bedeutet. Es gibt zwar viele verschiedene Browser, aber davon werden zwei am häufigsten benutzt, nämlich **Mozilla Firefox** und der **Internet Explorer** von Microsoft.

1. Arbeitsauftrag:
Finde heraus, welcher Browser auf deinem Computer ist:

Internet Explorer **Mozilla Firefox** **Opera** **Netscape** **anderer:**

Zu jedem Browser gibt es immer mal wieder neue Versionen. Sie werden in der Computerwelt üblicherweise nummeriert. Im Jahre 2008 waren Internet Explorer 7 und Mozilla Firefox 2 die Neuesten. Manchmal werden auch Zahlen vergeben wie z. B. 2.1.

2. Arbeitsauftrag:
Finde heraus, welche Version des Browsers auf deinem Computer ist. Dies findet man meist unter „Hilfe" oder „Info" oder „?" und dann bei „Über ..." oder „Info". Du kannst auch in der Hilfe in die Suchleiste „Browser" eingeben.

Mein Browser ..... hat die Version .....

3. Arbeitsauftrag:
Manchmal kann es wichtig sein, die neueste Browserversion zu benutzen. Fehler im Programm oder Sicherheitslücken werden mit neuen Versionen meistens beseitigt. Frage einen Erwachsenen, ob ihr die neueste Version des Browsers benutzt. Wenn nicht, lasse ihn installieren (die Browser sind kostenlos!).

4. Arbeitsauftrag:
Vielleicht gehörst du ja schon zu den Computerexperten und weißt, wie man einen Browser bedient? Wenn ja, dann zeig den anderen die wichtigsten Funktionen:

- Wie rufe ich eine Internetseite auf?
- Wie gehe ich eine Seite zurück?
- Wie speichere ich eine interessante Seite?
- Wie drucke ich etwas aus?
- Wie schließe ich den Browser?

TIPP: Wenn du mehr über die Technik rund um das Surfen wissen möchtest, dann schaue hier: **www.internet-abc.de/kinder/112099.php**.

Arbeitsblatt vom Name: .....

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** oder der **Mozilla Firefox**, sind ganz schön speicherwütig. Daten über dein Internet-Surfen werden von ihm 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.

1. Arbeitsauftrag:
Überlege und schreibe auf, warum diese Daten nicht in fremde Hände fallen sollten:

a. Verlauf

.....

b. Cookies

.....

c. Passwörter

.....

d. Cache

.....

2. Arbeitsauftrag:
Schaue nach, wie und wo du sie löschen kannst!

3. Arbeitsauftrag:
Kannst du einstellen, dass diese Daten automatisch beim Schließen gelöscht werden? Erkläre deiner Nachbarin/deinem Nachbarn, wie dies geht!

TIPP: Im Internet Explorer 7 ist die Funktion „Extras – Browserverlauf löschen", im Mozilla Firefox 2 „Extras" – „Private Daten löschen" wichtig. Wichtig ist auch, den Browser danach sofort zu schließen!

Arbeitsblatt vom **Name:**

Internet Explorer oder Firefox?

Der Browser ist als Schnittstelle zwischen Internet und Nutzer enorm wichtig, besonders in Sicherheitsfragen. In den letzten Jahren haben sich zwei Browser durchgesetzt: Internet Explorer mit einem Marktanteil von fast 70 % und Mozilla Firefox mit 25 %. Alle anderen Browser haben nur einstellige Verbreitungsprozentzahlen.

Doch welcher Browser ist der bessere? Ihr dürft vergleichen!

1. Arbeitsauftrag:

a) Teilt euch in zwei Gruppen auf, je eine für Internet Explorer, eine für Mozilla Firefox.
b) Teilt euch innerhalb der Gruppen in folgende Teams auf:
- *Bedienung und Benutzerfreundlichkeit*
- *Sicherheitseinstellungen, Löschen privater Daten*
- *Marktanteile / Verkauf / Wirtschaftsaspekte*
- *Die Firmen / das Konzept dahinter / Hintergrundinformationen*

c) Bereitet jeweils eine kleine Präsentation von max. 2 Minuten Länge vor – pro Team – und informiert darin eure Klassenkameradinnen/Klassenkameraden über euer Spezialthema.

2. Arbeitsauftrag:

Versucht nun, jeder für sich, die Frage zu beantworten: Welcher ist der Bessere?
Stellt dazu eine doppelte Plus-Minus-Tabelle mit einem Fazit auf, in dem ihr eure Entscheidung begründet!:

Internet Explorer		**Mozilla Firefox**	
Version:		**Version:**	
Plus	**Minus**	**Plus**	**Minus**
Fazit:			

Sachinformation

Fußabdruck? Trampelpfade!

Sie glauben, sie haben alle Vorsichtsmaßnahmen getroffen um sicher, unbeschwert und vor allem unverfolgt die weite Welt des WWW erkunden zu können? Sie glauben, dass ihr Surfverhalten bei der Masse an Usern und täglich aufgerufenen Webseiten niemanden weiter interessiert? Sie glauben, dass sie unbeschwert Anonymität genießen? Weit gefehlt: Unsere digitalen Datenspuren im Internet „Fußabdruck" zu nennen, ist eine fahrlässige Verharmlosung. Wir hinterlassen ganze Trampelpfade voller Daten. Bevor sie weiterlesen, rufen sie doch bitte folgende Seite auf und schauen, was sich durch einen harmlosen Aufruf einer Internetadresse in Erfahrung bringen lässt: **www.anonym-surfen.com/anonym-surfen/test**.
Dabei ist – nebenbei gesagt – der Ausflug ins WWW nur ein kleiner Teil des digitalen Trampelpfades, denn jedes Mal, wenn sie ihr Handy dabei haben, weiß man, wo sie sich aufhalten. Wenn sie die EC-Karte benutzen, weiß man, wie viel sie wo bezahlt haben, wenn sie mit Kreditkarten zahlen oder Payback-Karte benutzen, auch was sie gekauft haben. An den Straßen, Bahnhöfen und Flughäfen stehen Videoüberwachungskameras, die auch eine Identifikation ermöglichen (oder das Nummernschild erkennen lassen).
Auch panopti.com die „schöne neue Welt der Überwachung" veranschaulicht, inwieweit der gläserne User schon Realität geworden ist:
www.panopti.com.onreact.com/swf/index.htm.

Anonymität im Netz ist eine Illusion

Der Eindruck der Anonymität im Internet ist eine Illusion. Sie sind durch eine eindeutige Adresse (die sog. IP-Nummer) identifizierbar. Diese Nummer erhält jeder Rechner, der sich in das Internet einwählt. Ihr Provider kann diese Daten seit dem 1.1.2008 (durch das Gesetz zur Speicherung von Telekommunikationsdaten, hier ein Artikel zur Übersicht beim Magazin FOCUS Online **www.focus.de**: „Was der Provider künftig speichern soll", Claudia Frickel, 8.6.2007) sechs Monate speichern, sodass jederzeit festgestellt werden kann, wo sie wann und wie lange gesurft haben. Jeder Eintrag z. B. in einem Gästebuch lässt sich so eindeutig zuordnen (dies nutzt z. B. auch Wikipedia bei anonymen Einträgen).

Die Betreiber von Webseiten speichern die Daten (oder lassen sie speichern über z. B. Bannerwerbung, genannt sei hier „Doubleklick") der Besucher, um damit Kundenprofile zu erstellen: Und sie merken fast nichts davon. Über kleine Dateien (sog. „Cookies") weiß der Anbieter sogar, wann sie das letzte Mal bei ihm waren und welche Angebote sie besonders verlockend fanden. Der gläserne Nutzer ist längst Realität.

E-Mail und Browser

E-Mails können auf dem langen Weg durch das Internet abgefangen und gelesen werden. (Auch wenn es nicht mehr aktuell ist, so ist doch der Fall des FBI und des E-Mail-Schnüffelprogramms „Carnivore" aus dem Jahre 2000 immer noch sehr anschaulich: **www.tecchannel.de**, Artikel: „FBI verteidigt sein Schnüffelprogramm" vom 25.7.2007). „Carnivore" wurde bis 2005 verwendet und macht eines deutlich: Auch der E-Mail-Verkehr ist nicht sicher. (Und das FBI hat bessere Methoden als den „Bundes-Trojaner": **www.spiegel.de**, Artikel „FBI schnüffelt schon mit Bundestrojaner" vom 20.7.2007).
Windows und der Internet-Explorer haben ein riesiges Gedächtnis. Sie speichern, wann sie welche Internetseite aufgerufen, welches Programm sie geöffnet haben und sogar die Inhalte der Internet-Seite mit Bildern, Texten und Videos. Und Daten im Papierkorb von Windows sind nichts anderes als verschoben, noch lange nicht gelöscht.

Der Schul-PC und das Internet-Café

Während wir uns zu Hause noch sicher wähnen und auch entsprechende Vorkehrungen (z. B. über Firewall und Anti-Viren-Programm) getroffen haben, so ist das Arbeiten an einem fremden Rechner wie in der Schule oder in einem Internet-Café doch besonders sensibel. Folgende Tipps können helfen:

- keine persönlichen Daten auf den Computern speichern
- keine wichtigen Geschäfte wie Online-Banking etc. tätigen
- Vorsicht bei der Benutzung von E-Mailing
- nach dem Surfen immer den Browser schließen, erneut öffnen und alle gespeicherten Daten (Verlauf, Cookies, temporäre Dateien etc.) löschen, wieder schließen. (Genaueres dazu im Kapitel „Browser")
- nach der Arbeit am Computer den Papierkorb von Windows löschen (bedenken, dass auch dies kein 100%iger Schutz ist)

Kleine Helfer

Wer ein noch größeres Maß an Sicherheit haben möchte, kann Software benutzen, sog. „Tools“, die jeweils eine spezielle Aufgabe erledigen (hier sind nur kostenlose Programme/Angebote aufgeführt). Genannt sei hier die Möglichkeit zur Verschlüsselung von E-Mails (über PGP (Pretty Good Privacy), z. B. unter **www.helmbold.de/pgp** oder **www.pgpi.org**) oder die Benutzung von Kurz-Zeit-E-Mail-Anbietern (z. B. „10-Minute-Mail“: **www.10minutemail.com**). Weiterhin gibt es Angebote, die das anonyme Surfen im Internet ermöglichen (hier ein Vergleich der Anbieter: **www.meineipadresse.de**) oder man benutzt gleich einen Browser, der keine Daten speichert, wie z. B. Browzar **www.browzar.com**. Wem das Löschen aller Datenspuren des Browsers zu mühselig ist, kann Software dazu benutzen, wie z. B. CCleaner **www.filehippo.com/download_ccleaner** oder MilShield (**www.computerbild.de**, unter „Programme“). Wer sicher sein will, dass die Datenspuren aus Windows verschwinden, muss zum einen die temporären Ordner und den Papierkorb löschen. Leider sind die Daten auch nach dem Löschen im Papierkorb leicht wieder herstellbar. Profis empfehlen ein physikalisches Überschreiben auf der Festplatte (für das es bestimmte Verfahren gibt), wie es die Software Eraser leisten kann: **www.heidi.ie/eraser**.
Schließlich und endlich kann man sich zunutze machen, dass Daten auch in anderen Dateien, wie Bildern, versteckt werden können. Allerdings muss man dazu professionelle Software wie die „Steganos Security Suite 2007“ verwenden.

Probleme und Risiken

Das anonyme Surfen im Internet hat selbstverständlich zwei Seiten, denn was einmal dem Datenschutz dient, kann beim nächsten Mal missbraucht werden. Die Benutzung der o. a. kleinen Helfer setzt fast immer die Installation von Software voraus (echte Spezialisten können einen USB-Stick mit den installierten Programmen einrichten), was normalerweise an Rechnern in der Schule oder im Internet-Café nicht möglich ist (bzw. nicht möglich sein sollte). Also bleibt nur das Verwischen der Datenspuren per Hand.

Links

www.sicherheitskultur.at/privacy_glosse.htm	ein Artikel der Computerwoche Österreich, in dem die Autoren Philipp Schaumann und Christian Reiser über einen Tag ohne Datenspuren berichten
www.bsi.de/literat/anonym/vorwort.htm	eine Studie des Bundesamtes für Sicherheit in der Informationstechnik BSI über „Anonymität im Internet“
www.netplanet.org/sicherheit/anonym.shtml	interessanter und aktueller Artikel über Anonymität im Internet
www.n-tv.de/832128.html	„Anonym durchs Internet? Speicherung von Nutzerdaten“ (27.2.2007) ein Artikel von Christof Kerkmann
www.echo-online.de (unter „Service“, „Multimedia“)	„Unerkannt durchs Netz bummeln – Der gläserne Nutzer ist längst Realität“ Artikel zum Thema

Methodisch-didaktische Hinweise

Arbeitsblatt	▶●●	▶▶●	▶▶▶
Zeitangabe (Unterrichtsstunden)	2–3	2–3	2–3
Ziele	Die Schülerinnen und Schüler machen sich einige grundsätzliche Gedanken darüber, warum der Datenschutz beim Browser wichtig ist oder wichtig sein könnte und lernen, selbst wichtige Einstellungen vorzunehmen.	Die Schülerinnen und Schüler lernen die Problematik von Cookies kennen und erfahren wie man die Browsereinstellungen ändern kann.	Die Schülerinnen und Schüler lernen die Waybackmachine kennen und probieren diese aus.
Methode/n	Tabelle (Tafel)	Talkshow	Pro/Contra-Tabelle
Organisationsform/en	Einzel/Partner, U-Gespräch	Einzel, U-Gespräch	Einzel, U-Gespräch
Zugang Internet **Zugang PC**	ja ja	ja ja	

Kommentare zu den Arbeitsblättern

▶●●

Im ersten Teil sollen die Schülerinnen und Schüler sich einige grundsätzliche Gedanken darüber machen, warum der Datenschutz beim Browser wichtig ist oder wichtig sein könnte. Bei dieser Frage kommen meistens ganz unterschiedliche Ergebnisse heraus. Aber Kinder können auch einschätzen, dass es manchmal nicht gut ist, wenn ihre Eltern alles erfahren (was im Prinzip kontraproduktiv zum Ansatz dieses Buches ist, aber im Sinne des kritischen Surfverhaltens trotzdem wichtig!) oder wenn man plötzlich komische Werbung bekommt.

Zugegebenermaßen erfordert dieses Arbeitsblatt im zweiten Teil auch sie als Kollegin/Kollegen. Denn ohne ihre Hilfe werden die Kinder nicht die Feinheiten in den Einstellungen des Browsers einschätzen können. Diskutieren sie die Tabelle bitte und erklären sie die nötigen technischen Hintergründe. So könnte sie aussehen:

Im Browser steht:	Das bedeutet:	Das stelle ich ein:
„Besuchte Seiten“ oder „Verlauf“ und „Temporäre Internetdateien“	Wo ich im Internet war und was ich mir angeschaut habe.	Besuchte Seiten: 0 Tage, Verlauf löschen
„Daten speichern, die in Formularen …“ oder „Formulardaten“	Es wird auf meinem Computer gespeichert.	Keine Daten speichern.
„Cookies“	Informationen von der Internetseite, auf der ich war.	Cookies beim Schließen löschen.
„Kennwörter“	Meine Passwörter sind im Browser gespeichert.	Keine Passwörter speichern.

Im letzten Arbeitsauftrag sollen die Schülerinnen und Schüler, vielleicht methodisch in Form einer Talkshow, sich mit dem Pro und Contra auseinandersetzen und auch die Meinung von Onlineshop-Betreibern nachvollziehen können.

Die „Wayback-Machine“ 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. Methodisch sollen sie in Form eines kleinen Beitrags z. B. für eine Schülerzeitung dieses Internetgedächtnis darstellen und das Für und Wider diskutieren.

Möglichkeiten zur Weiterarbeit „Lust auf mehr“

Auch viele Erwachsene sind unwissend, wie groß der „Digitale Fußabdruck“ ist, den sie hinterlassen. Vielleicht könnten sie eine Informationsveranstaltung, durchgeführt von den Schülerinnen und Schülern, zu dem Thema anbieten? Gerade die Wayback-Machine liefert sehr anschauliche Beispiele für den nötigen Datenschutz.

Arbeitsblatt vom **Name:**

Fußabdrücke im Internet?

Ein Spaziergang am Meer, der Sand ist warm und weich und die Wellen rauschen. Mit jedem Schritt hinterlässt du Fußabdrücke am Strand, aber wenn eine Welle darüber schwappt, sind sie schon wieder weg. Am Computer kann dies anders sein:

Einige Menschen sprechen von „Digitalen Fußabdrücken", die wir bei einem Spaziergang im Internet hinterlassen. Dabei kann man sehen,
- *welche Internetseiten du aufgerufen hast,*
- *wie lange du auf diesen Internetseiten warst,*
- *von welchem Computer aus du im Internet warst*
- *und einige weitere Dinge.*

Besonders wichtig sind dabei so genannte „Cookies" [gesprochen kukies], das heißt übrigens „Kekse" auf Englisch. In einem „Cookie" werden Informationen auf deinem Computer gespeichert und die Internetseite kann diese Cookies beim nächsten Aufruf wieder auslesen.

1. Arbeitsauftrag:
Eigentlich sind diese Informationen doch ganz harmlos, oder?
Jeder kann doch wissen, auf welchen Internetseiten du warst und von welchem Computer aus.
Überlegt gemeinsam, warum es vielleicht doch nicht so toll ist,
wenn diese Informationen in fremde Hände gelangen!

Jetzt darfst du deinen Computer noch ein wenig sicherer machen:

2. Arbeitsauftrag:
Überlege vorher gut, wie du den Browser sicherer machen kannst! Dazu fülle bitte die folgende Tabelle aus!

Im Browser steht:	Das bedeutet:	Das stelle ich ein:
„Besuchte Seiten" oder „Verlauf" und „Temporäre Internetdateien"		
„Daten speichern, die in Formularen …" oder „Formulardaten"		
„Cookies"		
„Kennwörter"		

Arbeitsblatt vom **Name:**

3. Arbeitsauftrag:
Lest eure Tabelle vor und notiert das Wichtigste an der Tafel!

4. Arbeitsauftrag:
Finde folgende Einstellungsmöglichkeiten deines Browsers und mache ihn sicherer, indem du sie veränderst.

Wenn du den Firefox benutzt	Wenn du den Internet Explorer benutzt
	
Tipp: Suche unter „Extras“ und „Einstellungen“.	Tipp: Suche unter „Extras“ und „Browserverlauf löschen“.

Arbeitsblatt vom **Name:**

Cookies = gefährliche Kekse?

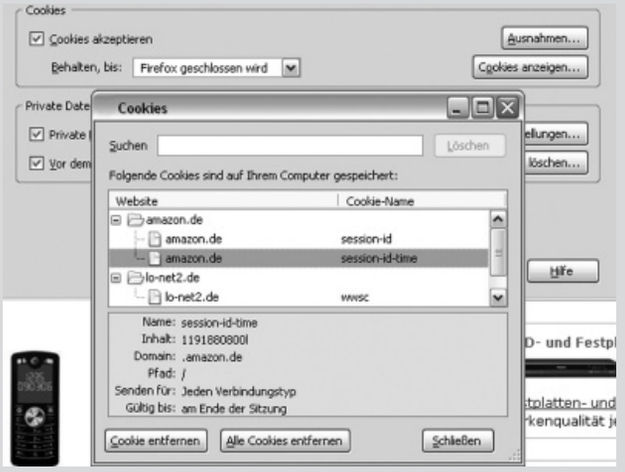
Cookies. Eigentlich ein süßer und harmloser Name für regelrechte Plagegeister. (Der Name übrigens soll von Rauschgifterfahrungen, ursprünglich „Magic Cookies“, mit denen man in das „Magic Cookie Land“ gelangt, stammen).

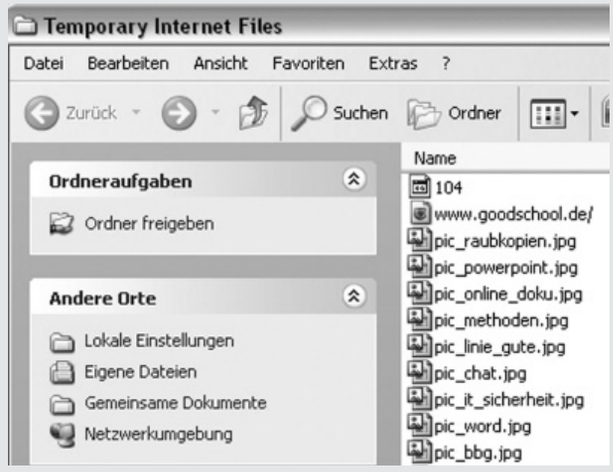
Klicksafe.de definiert es so: „Cookies – wörtlich übersetzt Kekse – sind kleine Dateien, die beim Lesen bestimmter Internet-Seiten vom Server auf die eigene Festplatte gespeichert werden. Damit sammeln zum Beispiel Online-shops alle möglichen Informationen über ihre Kunden. Sie merken sich so nicht nur Identifizierungsdaten der Besucher – soweit sie erkennbar sind – wie Namen oder Anschrift, sondern oft auch persönliche Vorlieben, etwa was zuletzt bestellt wurde. Im Cookie sind außerdem Informationen darüber gespeichert, wie lange man auf einer Seite war oder welche Seiten man sich angesehen hat. Besucht man später wieder diese Internet-Seite, „weiß“ der Server dank des Cookies, dass man schon einmal dort war.“

Zwar machen Cookies das Surfen äußerst bequem. Denn dank der virtuellen Kekse muss man zum Beispiel beim Besuch eines Onlineshops oder eines anderen Webangebots nicht jedes Mal die eigenen Daten – inklusive Passwort – erneut eintippen. Doch Cookies können auch unangenehme Folgen haben. Viele Webseiten enthalten unsichtbare Grafiken, so genannte Web Bugs, die in einer Webseite, einer E-Mail oder einem Werbebanner versteckt sind und die an die Cookies geknüpft sind. So kann etwa der Betreiber eines Anzeigen-Servers nachverfolgen, welche Seiten sich jemand angesehen hat und ihn mit passender Werbung „zuschütten.“

Cookies sind so etwas wie ein Gedächtnis einer Internetseite und auf den ersten Blick nicht gefährlich, können aber ganz schön lästig und auch problematisch werden. Findest du die Cookies auf deinem Computer? (Zwei Tipps: Im Internet-Explorer unter „Extras – Internetoptionen – Browserverlauf – Einstellungen – Dateien anzeigen“ im Firefox unter „Extras – Einstellungen – Datenschutz – Cookies anzeigen“.

Im Firefox	**Im Internet Explorer**
Extras – Einstellungen – Datenschutz – Cookies anzeigen	Extras – Internetoptionen – Allgemein – Browserverlauf – Einstellungen – Dateien anzeigen





Arbeitsblatt vom **Name:**

1. Arbeitsauftrag:
Ändere die Einstellungen, wie dein Browser Cookies behandeln soll, sinnvoll. Vielleicht musst du dazu noch ein wenig nachschauen, was die einzelnen Ausdrücke (zum Beispiel „Cookies von Drittanbietern") bedeuten!

2. Arbeitsauftrag:
Findet Beispiele, warum diese neuen Einstellungen von Cookies sinnvoll sind und notiere sie schriftlich!

3. Arbeitsauftrag:
Diskutiert das Pro und Contra von Cookies auch aus Sicht von Online-Shops in einer gespielten Talkshow mit dem Thema: Cookies – nützliche Helfer oder Plagegeister?!?

Arbeitsblatt vom **Name:**

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? Bis heute (2007) hat sein „Internet Archiv"
(**www.archive.org**) seit 1996 ca. 3 Petabyte (das ist eine Drei mit 15 Nullen) archiviert, rund 20 Terabyte kommen monatlich hinzu. Sein Internet-Archive steht 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 jetzt 85 Milliarden Seiten (für immer?) zugänglich.

Mit einer „Wayback-Machine" kann man sich die Seiten von Klicksafe.de anschauen. Danach erhält man eine Datumsliste und kann auf die gespeicherten Seiten zugreifen.

1. Arbeitsauftrag:
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?

Der bekannte Medienrechtler Viktor Mayer-Schönberger, Professor an der Harvard-Universität in den U.S.A. fordert ein Verfallsdatum für digitale Informationen. In der Stuttgarter Zeitung vom 6.9.2007 findest du einen Zeitungsartikel darüber: **www.stuttgarter-zeitung.de/stz/page/detail.php/1509699**

2. Arbeitsauftrag:
Stelle in Form eines Pro-Contra-Blattes die Vor- und Nachteile eines Internet-Archivs nebeneinander.
Diskutiert die Vor- und Nachteile in der Klasse!
Wie stehst du persönlich dazu?

3. Arbeitsauftrag:
Stelle dir vor, in zehn oder zwanzig Jahren stoßen folgende Menschen auf die Sachen (z. B. Fotos, Foren-Einträge, Texte, Bilder, Videos, eigene Webseiten, My Space-Accounts, Blogs), die du heute im Internet hinterlassen hast:
a. deine Mutter/dein Vater
b. deine Ehefrau/Partnerin
c. deine Kinder
d. dein Arbeitgeber
e. deine (wichtigen) Kunden
f. deine Arbeitskollegen
Welche Folgen könnte das für dich haben! Schreibe sie in einer Tabelle auf!

4. Arbeitsauftrag:
Schreibe (mit MS Word/OpenOffice.writer) einen Zeitungsartikel für eine Jugendzeitschrift. Schildere darin das Internet-Archiv, seine guten Seiten und die Risiken, die darin lauern können. Vielleicht kannst du auch Tipps für Jugendliche einbauen, wie sie schon heute mit ihren „digitalen Fußabdrücken" umgehen sollten!

Sachinformation

W-LAN

W-LAN oder „Wireless Local Area Network" (oder noch einfacher: Funknetz) ist der große technische Boom der letzten Jahre. Inzwischen setzen viele Unternehmen, Privatleute und auch Schulen auf diese Technik, alle modernen Laptops besitzen eine eingebaute Funknetzkarte, mit der man Zugang zu einem W-LAN (was den Zugang zu anderen Computern und zum Internet ermöglicht) erhält.
Nach Schätzungen des Bundesverbands Informationswirtschaft, Telekommunikation und Neue Medien (BITKOM) wurden Ende 2006 deutschlandweit bereits knapp sieben Millionen Breitband-Anschlüsse per WLAN betrieben. Fast 40 Prozent aller deutschen Haushalte verfügen zurzeit über einen Breitbandzugang, zur Jahresmitte 2008 wird es jeder Zweite sein. (Quelle: **www.bitkom.org**). Immer mehr so genannte „Hotspots" ermöglichen einen Internetzugang in Cafés, Bahnhöfen, Einkaufszentren usw. Größere Hotspots, bei denen ganze Stadtteile ein Funknetz besitzen, heißen „Hotzones".

Probleme

Die grenzenlose Mobilität bringt aber auch Probleme mit sich. Das Bundesamt für Sicherheit in der Informationstechnik warnt: „Werden Daten durch Funk oder Infrarot-Licht, also ohne direkte Verbindung zwischen Geräten wie PCs, PDAs oder Telefonen übertragen, so treten neben Störungen oder Netzausfällen vor allem Sicherheitsprobleme auf. Wenn sie zuvor nicht ausreichend verschlüsselt und geschützt wurden, können auf diese Weise übertragene Informationen von Dritten empfangen, aufgezeichnet und manipuliert werden." (Quelle: **www.bsi-fuer-buerger.de**).
Vor allem zwei Problembereiche berühren den Datenschutz:

- 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

Übertragungsweg über Funk

Alle Daten, die den Weg von einem Computer zum Nächsten finden sollen, werden in ein Funksignal umgesetzt. Logischerweise kann jeder, der dieses Funksignal auffängt (und dieselbe „Sprache" spricht, der Standard heißt heute IEEE 802.11), es nutzen.
Die Reichweiten der handelsüblichen Funknetze sind nicht größer als 100 bis 300 Meter bei optimalen Bedingungen (ohne Hindernisse wie Beton o. ä.).
Sie können aber leicht erhöht werden: Im Internet kursiert eine Anleitung für eine Richtfunkantenne für wenige Euro (das Kernstück ist eine Pappdose), die leicht die 500 m-Grenze überwinden kann. Damit kann ein Funknetz leicht abgehört werden, auch wenn man denjenigen nicht sieht!
Deshalb wurden zur Absicherung des Datenverkehrs Verschlüsselungsverfahren entwickelt, die die Datenübertragung sicherer machen sollen. Ein älteres System heißt „WEP" (Wired Equivalent Privacy, schön übersetzt mit „eine dem Kabelanschluss vergleichbare Privatsphäre"), ein verbessertes „WPA" „Wi-Fi Protected Access", inzwischen in der Version WPA2. (Für die Spezialisten: 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 z. Zt. die Sicherheit in der Datenübertragung gewährleistet.

Zugang zum Funknetz

Das weitere Problem, der Zugang zum Netzwerk, kann über verschiedene technische Verfahren gewährleistet werden: Das Einfachste ist eine Zugangsbeschränkung für unbekannte Computer (über die so genannte MAC-Adresse). Wie sie ihre WLAN-Verbindung sicher gestalten können, ist u. a. hier beschrieben: **www.zdnet.de** (unter „Security", „Sicherheit", „Praxis", Artikel: „WLAN ohne Risiko: Drahtlose Netzwerke sicher konfigurieren").
Außerdem sendet ein Funknetz seinen Namen aus, sodass Windows mit der automatischen Erkennung melden kann: „Drahtlosnetzwerke erkannt". Diese Sendung des Namens (SSID oder Service Set Identifier, auch SSID-Broadcast) kann unterdrückt werden, was eine weitere Hürde für die bösen Buben darstellt.

Folgen eines ungesicherten Funknetzes

Wenn sie ihr – privates oder möglicherweise schulisches – Netzwerk nicht absichern, so laden sie auf

der einen Seite Einbrecher ein, auf der anderen Seite haften sie u. U. für den Schaden, der durch Dritte verursacht wird (Quelle: **www.pressetext.ch** oder **www.vnunet.de**). Im Klartext bedeutet dies: Es trifft sie zumindest eine Teil-Schuld, wenn ein Fremder sich illegal Filme, Musik etc. über ihre W-LAN-Verbindung aus dem Internet herunterlädt.

„Schwarz-Surfen"

Vielleicht haben sie schon einmal gesehen, dass im Auto jemand mit einem Laptop auf den Knien saß. Es ist 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, aber in einem offenen Funknetz, das nicht abgesichert ist? Das Gesetz spricht von Daten, die besonders gesichert sein müssen:
Der § 202a StGB sagt:

Ausspähen von Daten: (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. (Quelle: **www.gesetze-im-internet.de** unter „StGB", zuletzt geändert durch Artikel 1 des Gesetzes vom 16.7.2007 (BGBl. I S. 1327)). Eindeutiger wird die Frage im „Telekommunikationsgesetz" beantwortet.

„§ 89 Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen":

1: 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.

2: 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.

3: § 88 Abs. 4 gilt entsprechend.

4: Das Abhören und die Weitergabe von Nachrichten aufgrund besonderer gesetzlicher Ermächtigung bleiben unberührt.

(Quelle: **www.gesetze-im-internet.de** unter „TKG", zuletzt geändert durch Artikel 3 des Gesetzes vom 18.2.2007 (BGBl. I S. 106))

Man sollte Schülerinnen und Schülern also dringend davon abraten, es als ein Kavaliersdelikt zu betrachten, in fremde Funknetze einzubrechen.

Mobile Spielkonsolen und Handys

Die Welt der mobilen Spielekonsolen ist in großer Bewegung und hat schon seit dem legendären Gameboy einen festen Platz in der Kinderwelt. Vor allem zwei Geräte haben herausragende Funkeigenschaften: die Sony Playstation Portable (PSP) und der Nintendo DS bzw. der Nachfolger Nintendo DS lite.
Klicksafe warnt: „Im Nintendo DS ist eine Chat-Funktion integriert. Es gibt vier Chat-Räume für bis zu 16 Personen. Die Chat-Räume sind nicht moderiert. Kontakt nehmen die einzelnen NDS Spielkonsolen über eine direkte drahtlose Funkverbindung auf. Die Reichweite des Pictochat beträgt ca. 30 Meter, auch durch Wände hindurch. Chatten macht Spaß, kann aber gefährlich werden, denn jeder der sich mit einem eigenen NDS in Reichweite befindet kann anonym Kontakt aufnehmen." Die Gefahr ist eher gering und im Nahraum zu sehen, trotzdem können Fremde Kontakt zu Kindern aufnehmen.
Beim Nintendo DS Spiel Nintendogs gibt es die Möglichkeit, Kontakt mit anderen Nintendogspielern aufzunehmen. Man kann den „WauWau-Modus" starten, den NDS zuklappen und durch die Gegend laufen. Sobald jemand vorbeikommt, der ebenfalls seinen NDS im WauWau-Modus Modus bei sich trägt, erkennen sich die Konsolen und reagieren mit Hundegebell. Das ist eine lustige Idee. Unangenehm würde es, wenn jemand über die niedlichen Hunde Kontakt zu Kindern erschleichen möchte.
Die Sony Playstation Portable als mobile Spielekonsole zu bezeichnen, ist eine leichte Untertreibung. Technisch ist dieses Gerät ein kleines Laptop, Fernseher, DVD-Player und anderes in einem. Selbstverständlich kann man damit ins Internet. Beim Nintendo ist dazu ein kleines Zusatzmodul und ein spezieller Browser nötig.

Auch einige, meist höherwertige Handys haben mittlerweile eine W-LAN-Funktion und damit einen Internetzugang in Funknetzen.
Mit diesen Geräten haben Kinder einen Internetzugang, der – anders vielleicht als beim heimischen PC – nicht unter der Kontrolle von Erwachsenen steht.

Die Zukunft
Selbstverständlich arbeitet die Industrie auf diesem Wachstumsmarkt intensiv und sucht verbesserte technische Lösungen, vor allem in der Übertragung großer Datenmengen. Der neueste Standard heißt WIMAX (Worldwide Interoperability for Microwave Access) und wird bereits in der Praxis eingesetzt.

Links

www.3sat.de/neues/dial/43898/index.html	der Sender 3sat bietet eine ausführliche und leicht verständliche Beschreibung der Technik von Funknetzen: „Local Area Network – Wireless LAN“
http://3s.hh.schule.de (Pdf-Datei zum Download unter „Wissen“, „Handouts“, „Funk-Netze-2007“, „WLAN“)	der Schul-Support-Service Hamburg zum Thema Funknetzen
www.bsi-fuer-buerger.de (unter „WLAN“, „Sicherheitstipps“)	Tipps des Bundesamts für Sicherheit in der Informationstechnik
www.itseccity.de	Artikel: „iPass-Statistik belegt: WLAN-Nutzung in Europa wächst rapide“ (2006) über die Funknetz-Steigerung in Europa
www.unit21.de/download/brosch_unit_050916.pdf	Broschüre „Ziel: Zukunft Notebook-Klassen NRW“

Methodisch-didaktische Hinweise

Arbeitsblatt	▶●●	▶▶●	▶▶▶
Zeitangabe (Unterrichtsstunden)	2–3	2	2–3
Ziele	Die Schülerinnen und Schüler setzen sich in praktischer Anwendung mit den Chancen und Risiken von Funknetzen auseinander.	Die Schülerinnen und Schüler sollen für die Sicherheitsrisiken von Funknetzen sensibilisiert werden.	Die Schülerinnen und Schüler sollen die wesentlichen Techniken eines Funknetzes kennen lernen.
Methode/n	Elternintegration, Demonstration, Plakate	Elternintegration, Fragenkatalog, Interview, Checkliste	Recherche, Merkzettel, Präsentation
Organisationsform/en	Einzel, Partner, U-Gespräch	Einzel, Partner, U-Gespräch	Großgruppen, Partner, U-Gespräch
Zugang Internet **Zugang PC**	ja ja	nein nein	ja ja

Kommentare zu den Arbeitsblättern

Dieses Arbeitsblatt benötigt ein wenig technische Vorbereitung. Die Kinder sollen sich mit den Funkmöglichkeiten der Sony Playstation Portable (unter den Kids nur „PSP" genannt, nicht zu verwechseln mit der „Playstation" zu Hause!) und dem Nintendo DS auseinandersetzen. Klar, dass dazu die Geräte benötigt werden. Bitte holen sie hier das Einverständnis der Eltern ein, denn die teuren Geräte können beim Transport oder in der Schule beschädigt oder sogar gestohlen werden. Vielleicht besteht die Möglichkeit, dass die Eltern die Geräte bringen und abholen?
Damit das Thema nicht nur dem Spielen, sondern auch dem Lernen dient, ist der Besuch der Eltern fest eingeplant. Oft kennen Eltern die Möglichkeiten der kleinen Geräte nicht oder unterschätzen diese, obwohl sie oftmals die erste Erziehungsinstanz bei heimischen Spielgeräten sind.
Im zweiten Arbeitsauftrag sollen die Schülerinnen und Schüler über die Chancen aber auch die Risiken der Funkmöglichkeiten reden (siehe Sachinformationen oben). Sie sollen sich Tipps für einen sicheren Umgang notieren und diese auch weitergeben.
Der dritte Arbeitsauftrag setzt voraus, dass die Eltern in die Schule kommen können, vielleicht beim Abholen in einer letzten Stunde? (Es werden sicherlich nicht alle Eltern kommen, aber vielleicht einige Interessierte). Die Kinder sollen den Eltern die Möglichkeiten mit ihren Chancen und Risiken vorführen. Wie im Kapitel zu Computerspielen weisen sie vielleicht die Eltern darauf hin, dass ein bloßes Verteufeln ebenso kontraproduktiv sein kann wie ein unkritisches „Das ist aber toll!".

Auch 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?"

Hier soll nach verschiedenen Funknetzen recherchiert werden. Die Großgruppen werden A und B benannt, nach der ersten Phase sollen sich jeweils ein Partner aus Gruppe A und Partner aus Gruppe B zu einem Team zusammenfinden und sich gegenseitig die Erkenntnisse vermitteln. Dieses Team soll auch Arbeitsauftrag Nr. 3 bearbeiten (Schutz beim Zugang, Schutz in der Übertragung) und einen Merkzettel erstellen. Damit ein Austausch dieser Merkzettel stattfinden kann, sollen die Gruppen A und B sich erneut zusammenfinden (d. h. aus jedem Team ist eine Schülerin/ein Schüler in jeder Gruppe) und sich austauschen.

Arbeitsblatt vom **Name:**

Nintendo – hat es gefunkt?

Verbindungen über Funk sind fast schon selbstverständlich. Klar, dass man mit einem Laptop ins Internet kann oder mit einem Handy telefonieren. Aber weißt du auch, dass schon die kleinsten Geräte – etwa die mobilen Spielekonsolen – Verbindungen über Funk herstellen können? Diese tolle Sache wollen wir mal Erwachsenen vorführen!

1. Arbeitsauftrag:
Für diese Vorführung brauchen wir ein paar Geräte und deshalb gibt es hier verschiedene Möglichkeiten:

Playstation Portable	Internet	Zeige, wie du eine Internetverbindung damit aufbauen kannst.
	Ein Spiel zu zweit	Zeige, wie ihr gegeneinander spielen könnt.
Nintendo DS oder Nintendo DS lite	Das Spiel Nintendogs	Gehe in den „WauWau-Modus“ und führ vor, wie der Nintendo zugeklappt bellt, sobald ein weiterer in der Nähe ist.
	Pictochat	Zeige, wie du mit anderen chatten kannst.
	Mario Kart oder ein anderes Spiel zu zweit	Zeige, wie ihr gegeneinander spielen könnt.

Schön wäre es, wenn ihr in der Klasse alle Möglichkeiten vorführen könntet!

2. Arbeitsauftrag:
Nun sind Funkverbindungen ganz tolle Möglichkeiten, miteinander zu spielen, aber es gibt auch Gefahren! Beim Surfen im Internet sowieso, aber auch bei einer Funkverbindung untereinander. Kannst du dir denken, welche? Schreibe Tipps auf Plakate, wie du mit den Gefahren umgehen kannst und vergesse sie nicht bei der Vorführung!

3. Arbeitsauftrag:
Jetzt kommt noch eine Riesenaufgabe: Zeigt euren Eltern diese Vorführung und redet mit ihnen darüber, was toll daran ist und was nicht so toll sein kann. Und – ganz wichtig – lasst sie es selbst ausprobieren! Vielleicht können die Eltern euch ja von der Schule abholen und ihr macht die Vorführung in der letzten Stunde?

Arbeitsblatt vom Name:

Euer Funknetz – ist es sicher?

Funknetz oder auf englisch „W-LAN" – sind der absolute Renner in der Computerwelt. Man findet sie mittlerweile überall: In Restaurants, auf Flughäfen – 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 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 (eine Mitschülerin/-schüler, Lehrerin/Lehrer, Nachbarin/Nachbar in deiner Straße …), der ein Funknetz zu Hause hat, ein paar unangenehme Fragen stellen.

1. Arbeitsauftrag:
Führe das Interview durch und notiere die Antworten in der dritten Spalte! Die richtigen Antworten findest du in der zweiten Spalte!

Ist das Funknetz einbruchssicher? Wenn ja, wie?	Hier müssen die Begriffe WEP (ein altes, schlechtes System) oder WPA (gut!) fallen. Außerdem kann man einen MAC-Filter benutzen, sodass nur angemeldete Computer in das Netz hineinkommen.	
Sendet es automatisch seinen Namen aus? (SSID genannt)	Jedes Funknetz hat einen Namen, der normalerweise ausgesendet wird. Dadurch kann 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 ich kann ein Funknetz so einrichten, dass nur die bekannten Kennungen (die ich vorher eingeben muss) hineindürfen.	

2. Arbeitsauftrag:
Klärt danach offene Fragen und erstellt schriftlich eine Checkliste auf der Rückseite des Arbeitsblattes, was ihr beachten müsst, wenn ihr in ein Funknetz geht.

Arbeitsblatt vom **Name:**

WPA, WEP, SSID, PSK?

W-LAN oder Funknetze haben vom Prinzip her zwei Möglichkeiten Geräte miteinander zu verbinden:
- direkt miteinander (so genannter „Ad-hoc-Modus") oder
- über eine zentrale Funkbrücke (so genannter „Access Point").

Letzteres ist die weitaus häufigere Variante und auch Standard bei Funk-DSL-Routern, die ihrerseits wiederum per Kabel an das Breitbandnetz angeschlossen sind. Heutzutage (Stand 2008) sind Übertragungsgeschwindigkeiten von über 54 Megabit pro Sekunde möglich, wobei dies in der Realität nur selten erreicht wird. Die Standards, auf denen die drahtlose Übertragung basiert, werden vom Institut der Elektrik- und Elektronikingenieure (IEEE) genormt und werden daher auch so: IEEE802.11x bezeichnet, wobei die letzte Zahl die Version (hier 11) angibt. Die Zukunft heißt – vielleicht – WIMAX (Worldwide Interoperability for Microwave Access), das mit dem Standard IEEE 802.16 arbeitet und schnellere Übertragungen als WLAN bietet.

Bei Funknetzen gibt es im Wesentlichen zwei Sicherheitsprobleme: Einbruch und Diebstahl.

1. Arbeitsauftrag:

a) Teilt euch in zwei Gruppen (A und B) auf. Recherchiert nach folgenden Begriffen und erstellt ein kleines Glossar (Erklärung) zum Thema.

b) Findet euch nun immer A+B zusammen und erläutert euch abwechselnd die Begriffe!

A	B
Was ist WEP?	Was ist WPA?
Was ist ein Hotspot?	Was ist ein PSK?
Was heißt SSID?	Was ist ein SSID?
Was ist die MAC-Adresse?	Was ist ein Shared Key?

Arbeitsblatt vom **Name:**

Die Absicherung eines Funknetzes kann im Prinzip über zwei Wege geschehen:
Ich verwehre den Zugang (Schutz vor Einbruch), oder ich verschlüssele die Übertragung (Schutz vor Diebstahl).

2. Arbeitsauftrag:

a) Recherchiert, diesmal im Team A+B, woran man dies bei einem Funknetz erkennt (ob es gesichert ist und wie).
b) Könnt ihr erklären, wie man sicher in einem Funknetz unterwegs sein kann? Schreibt es (immer noch A+B) als Merkzettel auf und stellt eure Tipps den anderen vor! Geht dazu in eure Ursprungsgruppe A oder B zurück.

TIPP: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat folgende Tipps **www.bsi-fuer-buerger.de/wlan/wlantipps.htm**

Sicherheitstipps für die Nutzung von Hotspots

- Rufen sie vertrauliche Daten nur über eine mittels SSL gesicherte Verbindung auf! (…)
- Viele Hotspots haben eine fundamentale Schwachstelle: Um dem Nutzer einen möglichst unproblematischen Netzzugang zu ermöglichen, erfolgt keine Verschlüsselung auf der Luftschnittstelle. Deswegen sind die Nutzer für die Vertraulichkeit der Datenübertragung immer selbst verantwortlich.
- Informieren sie sich über das Sicherheitsniveau des Hotspots!
- In den meisten Hotspots wird nicht verschlüsselt. Lesen sie die Beschreibungen des Hotspot-Leistungsangebots oder fragen sie – etwa in einem Café – einfach den Besitzer. (…)
- Schalten sie ihr WLAN nur bei Gebrauch ein!
- Auch beim Gebrauch im öffentlichen Raum gilt: Ein abgeschaltetes WLAN bietet keine Angriffsfläche.
- Verwenden sie ein aktuelles Virenschutzprogramm und eine Firewall, halten sie ihr Betriebssystem aktuell!
- Nutzen sie ein Betriebssystems-Benutzerkonto mit eingeschränkten Zugriffsrechten! Keinesfalls sollten sie bei der Nutzung von Hotspots Konten mit Administrationsrechten verwenden. Deaktivieren sie die Datei- und Verzeichnisfreigaben für Netzwerke!
- Schützen sie ihre Daten auch für den Fall des Verlusts Ihres mobilen Endgeräts!
- Sorgen sie für Zugangsschutz und bei hohem Schutzbedarf für eine Verschlüsselung der lokalen Daten!

Sachinformation

Die Zukunftsfrage

Stellen sie sich vor, sie finden heute wichtige digitale Daten zufällig wieder (nehmen wir mal an, die Examensarbeit, die sie schon damals am PC geschrieben haben oder die Urlaubsfotos von vor 15 Jahren – zur Erinnerung, die erste kommerzielle Digitalkamera kam 1976 mit 0,01 Megapixel auf den Markt). Was können sie heute damit anfangen? Könnten sie den Datenträger noch lesen? Könnten sie das Dateiformat noch verarbeiten? Genau vor diesem Problem werden wir in 20 Jahren auch stehen.
Große Institutionen wie Museen oder das Bundesarchiv **www.bundesarchiv.de** lösen das Problem heute mit großen Computern („Servern") und dem Hin- und Herkopieren der Daten sowie der regelmäßigen Aktualisierung (wer mitreden will: über NAS-Systeme; Network Attached Storage). Für den Normalanwender bleibt auch keine andere Möglichkeit, als seine wichtigen Daten mit neuer Soft- und Hardware zu aktualisieren.

Die Haltbarkeit

Und selbst wenn sie sich einen alten Computer auf den Speicher stellen und die CDs und DVDs mit den wertvollen Datenschätzen daneben, so bleibt das Problem der eingeschränkten Haltbarkeit. Nach heutigen Erkenntnissen halten auch CDs und DVDs, je nach Lagerung, vielleicht nur 25 Jahre. Auch wenn die Angaben dazu zwischen 25 und 100 Jahre schwanken, so hatte der Autor Thilo Resenhoefft 2001 doch recht, als er seinen Artikel in der WELT betitelte: „Keine CD ist unsterblich" (**www.welt.de**, Artikel vom 10.7.2001). Und, wie gesagt, wer hat in 20 Jahren noch ein CD-Laufwerk? (Noch ein wenig Computergeschichte? 1976 gab es die erste 5,25-Zoll-Diskette und seit 1981 von Sony die kleinere Variante 3,5-Zoll, die sich erstaunlich lange hielt.)

Datensicherung

Daten können auf einem Rechner auf vielfältige Weise verloren gehen. Beispielsweise können durch den Befall eines Rechners mit Viren oder Würmern Daten zerstört und somit unbrauchbar gemacht werden. Festplatten können einen Defekt bekommen (wem das passiert, seien folgende 10 Gebote empfohlen: **www.festplattencrash.eu**), das Betriebssystem kann abstürzen, ich kann eine Datei versehentlich löschen oder überschreiben, der Strom fällt aus oder der Rechner wird nicht ordnungsgemäß heruntergefahren und, und, und … Es ist daher ratsam, regelmäßig wichtige Dateien zu sichern. Dabei sollte der Schwerpunkt der Datensicherung auf selbst erstellte Dateien, wie Texte, Grafiken oder Bilder gelegt werden. Weiterhin ist es ratsam, die Daten auf einem externen Datenträger zu sichern. Wer seine Software im Original mit Installations-CD oder -DVD besitzt, kann sich wirklich auf die Sicherung der eigenen Dateien konzentrieren. Im Notfall bestünde ja die Möglichkeit, das Betriebssystem und die Software neu zu installieren. Persönliche Daten aber können nicht wieder hergestellt werden (zumindest von uns Laien nicht, Profis können hingegen Erstaunliches leisten und vielleicht lohnt sich eine Nachfrage im Notfall; es gibt zahlreiche Anbieter, die eine Datenrettung offerieren).

Vorbeugung

Die einfachste und billigste Methode ist ein regelmäßiges Sichern der Daten auf externen Speichermedien. Für den privaten und schulischen Zweck reichen sicherlich CDs, DVDs, USB-Sticks oder externe Festplatten aus. Die Experten unterscheiden zwischen verschiedenen Speichermethoden:

- Voll-Datensicherung (alle Daten werden gespeichert)
- Inkrementelle Datensicherung (Nach einer Voll-Datensicherung werden nur geänderte Daten erneut gespeichert, danach jeweils nur die Dateien, die seit der letzten inkrementellen Sicherung geändert wurden)
- Differenzielle Datensicherung (wie bei der inkrementellen, es werden jedoch alle – seit der letzten Voll-Datensicherung – geänderten Dateien erneut gespeichert)

Der Vorteil der differenziellen Datensicherung ist, dass sie nur zwei Versionen der Speicherung brauchen: Die Voll-Datensicherung und die letzte differenzielle Datensicherung. Bei einer inkrementellen Sicherung bedarf es aller Speicher-Versionen. Eine Wiederherstellung ist per differenzieller Sicherung unkomplizierter, allerdings benötigt diese Variante auch mehr Speicherplatz.

Die Routine

Nun ist es sehr schwierig, den richtigen Rhythmus für eine Speicherung zu finden (stündlich? täglich? wöchentlich? monatlich?) und auch jedes Mal daran zu denken. Sinnvoll ist eine automatisierte Sicherung, für die es wiederum eine Vielzahl kommerzieller Softwareprodukte gibt. Aber auch Windows XP hat die Möglichkeit zur automatisierten Datensicherung integriert. Hier finden sie eine Anleitung dazu: **www.bsi-fuer-buerger.de**, unter „Datensicherung" und **www.support.microsoft.com** unter „Datensicherung mit Windows XP Home".
Das BSI stellt folgende Regeln zur Datenlagerung auf: **www.bsi-fuer-buerger.de**:

- Daten von Zeit zu Zeit überprüfen, ob sie 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)

Das Gegenteil

Das Gegenteil der Datensicherung ist ähnlich schwierig: Die Daten sicher zu löschen! Sie wissen sicherlich, dass wir als Lehrerinnen und Lehrer nicht ohne Weiteres Schülerdaten wie Namen, Noten, Fotos usw. auf unseren heimischen Rechnern verarbeiten dürfen.

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 Windows-Löschen bietet hier nicht die ausreichende Sicherheit, da die Daten nicht physikalisch von der Festplatte gelöscht werden und ein Spezialist kann sie jederzeit wiederherstellen. Sicherheit bietet die so genannte „Guttmann-Methode" (benannt nach ihrem Entwickler), bei der die Daten auf der Festplatte 35mal nach einem Zufallsprinzip überschrieben werden. Es gibt einige kostenlose Programme, die diese Aufgabe übernehmen. Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt auf seiner Internetseite einige dieser Programme: **www.bsi-fuer-buerger.de**. Eine kleine Anleitung zum Download, Installation und zur Benutzung eines solchen Löschprogramms finden sie hier: **www.goodschool.de** (internet+sicherheit).

TIPP: Festplatten sollten nicht an andere weitergegeben werden. Ausgemusterte Exemplare sollten – mit Hammer und Schraubendreher – zerstört und anschließend im Elektroschrott entsorgt werden. CDs, die keine Verwendung mehr finden, können anhand eines Lochers zerstört werden. Somit verhindern sie, dass empfindliche Daten an andere weitergegeben werden.

Links

www.secure-it.nrw.de (unter „Angebote für die Schule“)	„Arbeitsmaterialien für den Unterricht. Wie sicher ist mein PC?“
www.bsi-fuer-buerger.de (unter „Datensicherung“)	das Bundesamt für Sicherheit in der Informations-technik mit Tipps zur Datensicherung
www.bsi.bund.de (unter „Maßnahmenkataloge“, „M 2.167 Sicheres Löschen von Datenträgern“)	sicheres Löschen von Datenträgern
www.heise.de/ct/06/01/118	Erläuterung zu NAS bei Heise-Online
www.sicher-im-netz.de (unter „Im Fokus“, „Fokus im Archiv“, „Datensicherung – dem Totalverlust wichtiger Daten vorbeugen“)	Datensicherung – dem Totalverlust wichtiger Daten vorbeugen
www.pcfreunde.de (unter „Utilities“, „Datensicherung“)	Linkliste zu Programmen für Datensicherung
www.langzeitarchivierung.de	Nestor – Kompetenznetzwerk zur Langzeitarchivierung

Methodisch-didaktische Hinweise

Arbeitsblatt	▶●●	▶▶●	▶▶▶
Zeitangabe (Unterrichtsstunden)	1	2	2
Ziele	Die Schülerinnen und Schüler setzen sich kreativ mit dem Problem der Daten-sicherung ausein-ander, indem sie eine Geschichte weitererzählen.	Die Schülerinnen und Schüler lernen die Problematik der Datensicherung und deren globale Bedeutung kennen.	Die Schülerinnen und Schüler lernen Möglich-keiten des versehent-lichen Datenverlustes und des gewünschten Datenlöschens kennen.
Methode/n	Weitererzählung	Recherche, Diskussion	Recherche, Merkzettel
Organisationsform/en	Einzel	Einzel, U-Gespräch	Einzel, Partner
Zugang Internet **Zugang PC**	nein nein	ja ja	ja ja

Kommentare zu den Arbeitsblättern

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.

Auf der „Sound of Earth“ ist 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**)

Im letzten Arbeitauftrag sollen die Schülerinnen und Schüler darüber reflektieren, wie mit einer Festplatte vor einem Verkauf zu verfahren ist: Festplatten sollte man physisch zerstören und nicht weiterverkaufen!

Möglichkeiten zur Weiterarbeit „Lust auf mehr“

Das Thema Datensicherung ist hier auf einer oberflächlichen technischen Ebene und eher grundsätzlich behandelt. Für „Techniker“ bietet sich die Weiterarbeit an, bei der die Backup-Methoden behandelt werden, hier bietet Windows XP beispielsweise ein eigenes Programm an, das nicht zusätzlich gekauft werden muss.
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?

Arbeitsblatt vom **Name:**

Und in 1000 Jahren?

(Quelle: © **http://upload.wikimedia.org/wikipedia/commons/8/89/Rosetta_stone.jpg)**

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.

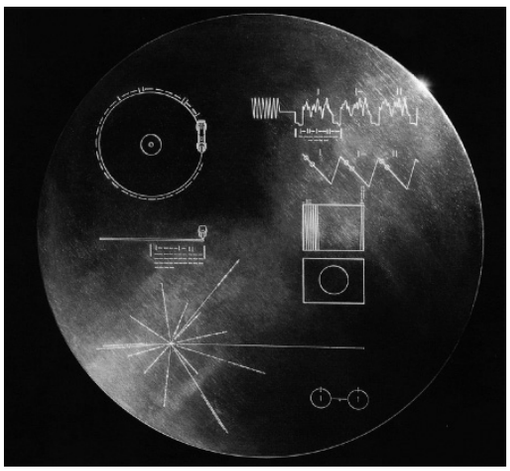
Stelle dir das mal mit einer CD von heute vor! Stelle dir vor, sie wird in 2000 Jahren gefunden!

1. 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. …

Arbeitsblatt vom **Name:**

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.

(Quelle: http://upload.wikimedia.org/wikipedia/commons/5/57/GPN-2000-001978.jpg)

1. Arbeitsauftrag:
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
■ 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, **www.bibliothek.uni-r.de/ubr/ink/pdf/digitalearchive.pdf**)

2. Arbeitsauftrag:
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. Arbeitsauftrag:
Jetzt wird es noch 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!

Arbeitsblatt vom Name:

Datenlöschen – geht das?

Anna ist verzweifelt. Stundenlang hat sie an ihrem Bio-Referat über die Proteinbiosynthese gefeilt, Grafiken und Animationen erstellt und jetzt das! Ihr Computer macht keinen Mucks mehr. Sie kommt auch nicht mehr an die Hausaufgaben, die Arbeitsblätter, von den Fotos der letzten Party oder ihrer Lieblingsmusik ganz zu schweigen. Katastrophe! Krise! Koma!

Drei große (neben vielen kleinen) Möglichkeiten, seine Daten irrtümlich zu löschen gibt es:

1. Auf deinem Computer werden alle Daten auf einer „Festplatte" gespeichert, dies sind magnetisierbare Scheiben, die übereinander liegen und sich bis zu 15.000 mal pro Minute drehen. Die Daten werden elektromagnetisch mit einem „Schreib-Lese-Kopf" gespeichert, der über die Scheiben rast, ohne sie zu berühren. (Übrigens: Die enorme Datenmenge ist möglich durch eine Technik, für die der deutsche Forscher Peter Grünberg 2007 den Nobelpreis für Physik erhielt). Dabei kann es zu Defekten kommen bis hin zu einem „Headcrash", dem Totalausfall. Schwer zu schaffen können diesen Magnetscheiben auch andere Magnete (Elektromotoren oder Lautsprecher) machen.
2. Dann gibt es selbstverständlich noch die Möglichkeit, dass man Daten versehentlich löscht. Doch Windows vergisst nicht so schnell und aus dem Papierkorb kannst du Daten meistens wieder rekonstruieren. Manchmal speichert man die Datei unter gleichem Namen ab und überschreibt somit eine ältere Version oder eine andere Datei. Dabei kann dann allerdings auch kein Papierkorb mehr helfen.
3. Die letzte große Möglichkeit seiner Daten verlustig zu werden sind Computerschädlinge wie Viren und Würmer, die absichtlich diese Katastrophe auslösten.

1. Arbeitsauftrag:
Überlege, wie Anna hätte vorbeugen können! Tipps dazu findest du unter: **www.bsi-fuer-buerger.de/daten**.
Erstelle ihr einen DIN-A5-Zettel zum Merken.

2. Arbeitsauftrag:
Tauscht eure Merkzettel aus und probiert die Tipps aus! Welche sind die Besten?
(Einfach und praktikabel und trotzdem sicher!) Erstellt eine Stufenleiter mit den besten Tipps!

Anna war beim letzten Mal ganz unvorsichtig – wie dieses Mal auch. Sie wollte eigentlich die Fotos löschen, die ihre Freundin auf der letzten Party aufgenommen hatte. Schließlich kann ihr Freund auch an den Computer. Aber der hat zufällig in den Papierkorb geschaut …

Bestimmte Daten unter Windows sicher zu löschen ist gar nicht so einfach, denn man muss dafür sorgen, dass genau dieser Bereich auf der Festplatte erneut überschrieben wird (am besten mehrfach, bis zu 35mal empfehlen Experten). Bis dahin sind die Daten rekonstruierbar, selbst beim Formatieren einer Festplatte! Also Löschen oder Papierkorb leeren oder auch Formatieren nutzt wenig. Hier helfen nur spezielle Löschprogramme. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt folgende:

- „Eraser" **www.eraser.dgeko.de/**
- „Space-Eraser" **www.winload.de/download/30452/Space.Eraser-1.3.1.html**
- „Secure-Erase" **www.secure-erase.de/**

3. Arbeitsauftrag:
Schaue dir an, wie du Daten sicher löschen kannst! Bei welchen Daten solltest du so vorgehen?
Tausche dich mit einem Partner aus!

4. Arbeitsauftrag:
Überlege: Stelle dir vor, du möchtest deinen Computer verkaufen. Was solltest du mit der Festplatte machen?