

7|1 Spam-Mails

7|2 Viren, Würmer, Trojaner, Spyware

7|3 Illegale Downloads und Tauschbörsen

Was wir nicht brauchen:
Unerwünschtes und Unnötiges!



7

7_1 Spam-Mails

- 7_2 Viren, Würmer, Trojaner, Spyware
- 7_3 Illegale Downloads und Tauschbörsen

Sachinformation

Spams

„Spam-Mails“ oder kurz „Spams“ sind unerwünschte E-Mails, die oft als Werbe-E-Mails die Internet-Briefkästen verstopfen. Die Herkunft des Wortes ist – wie so vieles – mit Mythen, Anekdoten und Geschichten behaftet. So soll das Dosenfleisch namens SPAM (das Akronym für SPiced hAM) der Firma Hormel Foods Pate gestanden haben. Die Komiker des Monty Python Flying Circus haben 1970 das Wort Spam in einem Restaurant-Sketch rund 100-mal genannt und so zum Synonym für „massenhaft und unerwünscht“ gemacht. Die Geschichte ist vielfach im Internet zu finden, u. a. hier: www.pcwelt.de; wer den Sketch („Spam“: Monty Python) sehen möchte:

www.video.google.de, Stichwort Monty Python Spam. Echte, wünschenswerte E-Mails werden auch scherzhaft „Ham“ genannt.

Wie viele und warum?

T-Online verzeichnete im April 2006 nach eigener Aussage täglich bis zu 1 Milliarde Spam-Mails (Quelle: www.heise.de, Artikel: „T-Online verzeichnet eine Milliarde Spam-Mails pro Tag“ vom 25.4.2006) und Schätzungen gehen dahin, dass heutzutage neun von zehn E-Mails unerwünscht sind. Und dies bei einer geschätzten Zahl von weltweit 100 Milliarden E-Mails pro Tag. Die Firma McAfee meldete im August 2007, dass 85 % aller E-Mails im Jahre 2006 Spam-Mails waren, übrigens lag der Anteil im Jahre 1997 bei 5 %! (Quelle: FOCUS 32/2007, S. 150)

Alle Spam-Nachrichten jetzt löschen (Nachrichten, die mehr als 30 Tage im Ordner "Spam" waren, werden automatisch gelöscht.)			
<input type="checkbox"/>	☆ Fabian Hicks	***Spam***: Stop being obese and unhappy - Take advantage of the chance! – Anatrium – The very up-to-date & most delighting	18:34
<input type="checkbox"/>	☆ Maxine Golden	***Spam***: Doping für Ihr bestes Stück from their -- Design Patterns, you'll avoid - Meinung von unserem Kunden: Ich nehr	18:32
<input type="checkbox"/>	☆ Roderick Lowery	***Spam***: Greatest artworks from top artists - GorgeousArt is the one-stop store for the greatest in artwork from famous Rus:	18:26
<input type="checkbox"/>	☆ Kamilah Lewis	» Gotta a sec - sane form increase Cliff stung began to laugh. How very Catholic of wooly them, Nancy said ...	18:13
<input type="checkbox"/>	☆ Silva@lfsvws01.mail.lfs.	» ***Spam***: Visit our pharmacy store and you won't regret! - Viagra Pro (SALE 50%) - Increase S*e*x Drive - Boost Sexual F	18:05
<input type="checkbox"/>	☆ Beverly	» Be her man - Pick up a hottie from our website They're waiting... http://br.geocities.com/caryfzwb298/ it ...	17:49
<input type="checkbox"/>	☆ Leila Brennan	» 50mg x 30 pills buy now - Unreadable from behind—they are well down then takes a step back, to be safe as she reaches. By	17:44
<input type="checkbox"/>	☆ Shane Duran	***Spam***: Don't ignore me, I have the solution to your problem. - Are you looking for we1ght-IDss med1cations such as M	17:31
<input type="checkbox"/>	☆ Latoya Gayla	Latest 2007 SwissReplica from \$179 - AudemarsROLEX, Bvlgari, Cartier, Chopard & other B...	17:21
<input type="checkbox"/>	☆ Daltonv Trudys	xexgoa Wie sind Sie info? - Hallo (, MAILTO_USERNAME) Sie wollen, der Ihres " Gurke " GROSS & STARK geworden ist, als	16:47
<input type="checkbox"/>	☆ Rudolph Dean	***Spam***: Blaues Wunder - dann klappts auch mit der Nachbarin our agency for your - ... - Meinung von unserem Kund	16:44
<input type="checkbox"/>	☆ Jazmin Jennette	***Spam***: not enough SPERM/CUM? increase 5x more with this cfeuu - Cum Pills : Increase Ejaculate: * LongerOrgasms	16:19
<input type="checkbox"/>	☆ Sales Department	Get now your pack of Genuine Viagra! - Now you can order Authentic Viagra directly from Pfizer Here: http://www.konarkcher	16:17
<input type="checkbox"/>	☆ Marshall Martinez	» Why be an average guy any longer - My sling. Your what? She cuddl I hit you with a stone from my She paused to yawn noisi	16:15
<input type="checkbox"/>	☆ Selena Lloyd	***Spam***: Re: Your Mer1dia Order #8125329 - Are you looking for we1ght-IDss med1cations such as Merid1a at a reduced pri	16:15
<input type="checkbox"/>	☆ Braden Robinson	» ***Spam***: What IS OEM Software And Why DO You Care? - OEM means Original Equipment Manufacturer. So OEM is sync	16:11
<input type="checkbox"/>	☆ Alexandria Latasha	***Spam***: We sell both BRAND(100% original) & GENERIC(35% cheaper) medications, Up to...	16:08
<input type="checkbox"/>	☆ Jody Grace	***Spam***: Reliable w4tches for everyone at Prest1ge Repl1cas - Repl1ca w4tches are not necessarily synonymous of low	16:08
<input type="checkbox"/>	☆ Morton Longoria13181	» ***Spam***: Morton, The prices out of competition, Vi.... Agra - 1.79 \$ - iii...!//AVGR A ONLY today! 10 pills of (viagra) for che	15:54
<input type="checkbox"/>	☆ Vito Norman35159	» ***Spam***: Vito, Vi.... Agra - 1.79 \$ order now and take pleasure - VIIAG...R//A ONLY today! 10 pills of (viagra) for cheap pr	15:46
<input type="checkbox"/>	☆ Ava Metz	» Hello Marco.fileccia - Si Lon a de bons outils et que Lon n.en emploie que de mauvais, repondit M. Tapley, on ne fait ...	15:32

Screenshot: die Spams der letzten drei Stunden! Vom 23.7.2007 von 15:32 bis 18:34 Uhr.

Der Versand von E-Mails ist kostenlos (es gibt Stimmen, die darin ein Grundübel des Problems sehen), kostet aber Computerkapazität und Zeit: Warum also gibt es eine solche Flut? Spams bringen Geld, und nicht nur der SPIEGEL vermutet dahinter mafiose und inzwischen gut organisierte Strukturen („Spiegel Special: Wir sind das Netz“ 03/2007, S. 109). Zum einen gibt es tatsächlich noch Kunden, die auf Angebote aus Spam-Mails reagieren, was bei den minimalen Kosten auch bei einem pro 100.000 noch ein gutes Geschäft ist.

Zum anderen werden Börsengeschäfte durch Aktien-tipps manipuliert. (Wer sich informieren möchte: z. B. www.heute.de, Artikel: „Spam made in Germany“ vom 18.4.2007). Und schließlich gibt es noch die verseuchten Spam-Mails, die den Computer des Empfängers mit einem Virus infizieren. Anschließend kann der Computer ausspioniert oder fremdgesteuert werden (mehr dazu im Baustein 7_2 „Viren, Würmer, Trojaner, Spyware“).

7_1 Spam-Mails

7_2 Viren, Würmer, Trojaner, Spyware

7_3 Illegale Downloads und Tauschbörsen

Trends

Die Spams des Jahres 2007 zeichnen sich durch immer raffiniertere Methoden aus, wobei zu beobachten ist, dass viele E-Mails personalisiert sind (man wird als Person direkt angesprochen), es werden Bilder statt Texte verschickt (was den Spam-Filtern die Arbeit erschwert) und es wird immer wieder variiert.

Letztlich ist noch zu vermelden, dass die Anzahl der verschickten Spam-Mails exponentiell angestiegen ist. Das „Spamhaus-Projekt“ widmet sich, wie viele andere, dem Kampf gegen Spam und listet regelmäßig die zehn größten Spammer-Nationen (Dezember 2007 U.S.A., China und Russland), die 10 betroffenen Netzwerke und die Namen der schlimmsten Spammer auf (Quelle: www.spamhaus.org).

Ein Beispiel? Der 27-jährige Robert Soloway soll 150 Millionen E-Mail-Adressen von Internetnutzern besessen haben. Für rund 495 US-Dollar (370 Euro) schickte er 15 Tage lang E-Mails an 20 Millionen Adressen oder er verkaufte 80.000 E-Mail-Adressen direkt an seine Kunden. Damit soll er im Laufe der Jahre rund 600.000 Dollar verdient haben. Er wurde im Mai 2007 gefasst und ihm drohen bis zu 20 Jahre Haft. (Quelle: www.computerwoche.de, Artikel „Spam-König“ in USA festgenommen – weltweiter Rückgang erwartet“ vom 1.6.2007).

Das Perfide an der Sache: Die Spams rekrutieren ihre eigenen Mutterkühe. Durch Viren in Spam-Mails werden Computer zum Teil eines „Botnets“, eines ferngesteuerten Computernetzes. Die Computerbesitzer ahnen nicht einmal, dass sie dazu beitragen, den E-Mail-Müll zu versenden.

Die gute Nachricht: „Die Spam-Flut schafft Informatikern neue Arbeitsplätze und Herstellern von Anti-Spam-Software glänzende Quartalsabschlüsse“ („Spiegel Special: Wir sind das Netz“ 03/2007, S. 108).

Rechtliches

In Deutschland ist das Zusenden unaufgeforderter Werbemails verboten, wie es die „Richtlinie über den elektronischen Geschäftsverkehr“ der EU im § 7 forderte (Pdf-Datei auf: www.eur-lex.europa.eu, Richtlinie vom 17.7.2000) und in verschiedenen Gesetzen fixiert ist (Bürgerliches Gesetzbuch, Gesetz gegen den unlauteren Wettbewerb und Telemediengesetz). Deswegen verschicken die Spammer ihre Bot-schaften entweder über Internetanbieter aus dem Ausland oder über die ferngesteuerten Rechner,

den sogenannten Botnets. Das Brief- und Postgeheimnis ist in Deutschland durch das Grundgesetz garantiert: Artikel 10 bestimmt die Unverletzlichkeit des Brief-, Post- und Fernmeldegeheimnisses (der Artikel im Wortlaut www.gesetze-im-internet.de, zuletzt geändert durch das Gesetz vom 28.8.2006 (BGBl. I. 2034)). E-Mails gehören dazu, und aus diesem Grunde darf auch niemand anderes ihre privaten E-Mails löschen als sie selbst und darum landen die verdächtigen E-Mails in einem Spam-Ordner und werden automatisch erst nach 30 oder 60 oder 90 Tagen gelöscht (dazu haben sie den Anbieter in den Nutzungsbedingungen ermächtigt).

Vorbeugendes Handeln

Spams sind mehr als ärgerlich: sie verursachen zusätzliche Verbindungskosten, sind zum Teil gefährlich und das Aussortieren und Löschen kostet Zeit.

Um die Flut an Spam-E-Mails zu beschränken, sind folgende Maßnahmen hilfreich:


- niemals auf eine Spam-Mail reagieren
- den Spam-Filter „trainieren“
- die E-Mail-Adresse nicht überall angeben und immer eine zweite E-Mail-Adresse anlegen

Eine falsche Antwort auf eine Spam-Mail ist eine Beschwerde beim Absender. Dadurch bekommt der Spammer die sehr wertvolle Information, dass die E-Mail-Adresse gültig ist und sie erhalten in Zukunft noch mehr Spam-Mails. Alle Web-Mail-Anbieter (in Deutschland bspw. GMX.de oder WEB.de oder Googlemail.com) haben einen Spam-Filter integriert. Dieser sorgt dafür, dass verdächtige E-Mails in einem separaten Ordner landen. Wenn sie dem Anbieter (meist durch einem oder zwei Klicks möglich) mitteilen, dass es sich um eine Spam-Mail handelt, kann dieser beim nächsten Mal besser reagieren. Dieses „Training“ ist ein wenig mühevoll, lohnt sich aber!

Wegwerf-E-Mail-Adressen

In Spam-Zeiten wie diesen haben sich einige Anbieter darauf spezialisiert, Wegwerf-E-Mail-Adressen bereitzustellen. Sie gelten nur kurzzeitig und alle dort ankommenden E-Mails werden nach einer bestimmten Zeit automatisch gelöscht. Ideal für unwichtige/unseriöse Anmeldungen, Werbung o. ä.. Hier seien nur zwei dieser Anbieter genannt: www.temporaryinbox.com und www.10minutemail.com. Aber Vorsicht! Überall, wo sie dauerhaft Nachrichten erhalten

wollen, können sie diese nicht nutzen. Einige große Anbieter kennen inzwischen diesen Trick und haben diese E-Mail-Adressen gesperrt.

Hier finden sie eine „Liste der Anbieter von Wegwerf-E-Mail-Adressen“:  www.jethwa.de, unter „Aktuell“.

Technische Maßnahmen

Wenn Sie keine Web-Mail-Adresse benutzen (was mit einer schnellen Internetverbindung wie DSL durchaus zu empfehlen ist), sondern die E-Mails auf Ihrem eigenen Rechner empfangen (durch das „POP3“, Post Office Protocol Version 3), wird eine deutliche Verminderung an Werbemails im eigenen Postfach erreicht, falls die elektronische Post erst durch den Online-Filter des eigenen E-Mail-Dienstes und dann durch ein Filterprogramm des E-Mail-Programms geprüft wird. Viele Firmen haben sich auf diese E-Mail-Filtersysteme spezialisiert und bieten die entsprechenden Produkte als „Spam-Filter“ an.

Verschlüsselung

Neben den Spam-Mails droht auch bei der Übertragung von E-Mails Gefahr, denn die Übertragungswege sind keineswegs sicher und E-Mails können abgehört werden. Ein – relativ – einfaches und auch kostenlos erhältliches Verfahren besteht in der Verschlüsselung der übertragenen Daten. Das Stichwort lautet PGP (Pretty Good Privacy), womit ein Verfahren beschrieben wird, das Anfang der 90er Jahre von Phil Zimmermann entwickelt wurde. Es arbeitet mit einem „Public-Key“, einem eindeutig zugeordneten Schlüsselpaar: So gibt es einen öffentlichen Schlüssel zur Verschlüsselung der Daten. Nur ein privater Schlüssel kann die Daten wieder lesbar machen. Dieser private Schlüssel ist geheim, besitzt nur der Empfänger und ist durch ein Passwort verschlüsselt. Solche Verfahren werden auch asymmetrische Verfahren genannt, da Sender und Empfänger zwei unterschiedliche Schlüssel benutzen. Lehrer-Online bietet dazu eine Unterrichtsreihe an:  www.lehrer-online.de/sichere-e-mail.php.

Probleme und Risiken

Es klang oben schon an: E-Mailing kann auch gefährlich sein. Gerade bei Anhängen (engl. „Attachments“) besteht die Gefahr, dass sich dort ein Virus, Wurm oder Dialer verbirgt. Deswegen sollte man nur Anhänge öffnen, die man von vertrauenswürdigen Menschen bekommen


hat und die vorher angekündigt wurden. Eltern und Pädagogen können aber schon mit ein paar Tricks sich und ihre Kinder weitgehend vor Reklamefluten, dubiosen Geschäftemachern und verseuchten E-Mails schützen.

Wie können Kinder sicherer mailen?

Kinder, die im Netz aktiv sein möchten, benötigen eine eigene, geschützte E-Mail-Adresse, hinter der niemand den echten Namen erkennen kann. Es gibt nur wenige kostenlose E-Mail-Anbieter, die für Kinder ein gutes Angebot zur Verfügung stellen: Zuerst muss man sich auf einer der folgenden Webseiten anmelden, um eine eigene E-Mail-Adresse anlegen zu können:

- Kidstation.de
- ZUM-Mail (der Zentrale für Unterrichtsmedien)
- Lizzynet (für Mädchen, Angebot von Schulen ans Netz e.V.)

Die geringe Zahl an Anbietern liegt daran, dass der Kontrollaufwand riesig und es praktisch unmöglich ist, die E-Mailbox von Kindern dauerhaft von Spam und anderen Problemen frei zu halten.

Eine Alternative ist, dass Eltern über ihren Provider mehrere E-Mail-Adressen einrichten. Den Kindern sollten zwei Adressen zur Verfügung gestellt werden: Eine Adresse ist nur für den Kontakt mit Freunden reserviert und darf auch nur an diese weitergegeben werden. Die zweite Adresse kann das Kind bei seinen Ausflügen ins Internet verwenden. Der Posteingang dieser Adresse sollte von Eltern überprüft werden. Diese kann bei Bedarf geändert werden, sofern über sie unerwünschte Werbung empfangen wird. (Quelle: Text aus der Broschüre „Ein Netz für Kinder“ (2004) des BMFSFJ, Download der Pdf-Datei unter  www.jugendschutz.net).

Empfehlungen fürs Mailen

- **Der Betreff:** In der Betreffzeile wird der Empfänger schon vorab über den Inhalt der E-Mail informiert und kann ihren Stellenwert einschätzen. Die Betreffzeile kann entscheidend dafür sein, ob eine E-Mail sofort gelesen, zur Seite gelegt oder gar direkt gelöscht wird. Der Betreff sollte also stets genannt und so formuliert werden, dass er kurz und prägnant den Inhalt oder das Anliegen des Schreibens verrät. Und vermeiden sie die Schlüsselbegriffe, auf die jeder Spam-Filter reagiert. Welche das sind? Schauen sie kurz in ihre E-Mails!



7_1 Spam-Mails

7_2 Viren, Würmer, Trojaner, Spyware

7_3 Illegale Downloads und Tauschbörsen

- **Der Inhalt:** Knapp aber herzlich! E-Mails sollten sich durch einen kurzen und knappen Stil auszeichnen. Das bedeutet aber nicht, ganz und gar auf Höflichkeitsformeln und einen netten Umgangston zu verzichten. Sich im ersten Satz für eine erhaltene Mail zu bedanken oder durch eine persönliche Ansprache („Ich hoffe, sie hatten einen schönen Urlaub“) eine positive Atmosphäre zu schaffen, kann auch in einer elektronischen Nachricht nicht schaden.
- **Klein oder groß?** Es gilt zwar als schick und modern, nur die Kleinschreibung zu nutzen, man erschwert aber damit dem Adressaten unnötigerweise das Lesen. Denn manche Wortkombinationen werden erst durch Groß- und Kleinschreibung eindeutig. Gern zitiertes Beispiel: der gefangene Floh / der Gefangene floh. Handelt es sich hier um den gefangenen Blutsauger oder um den entwischten Sträfling? Wörter oder ganze Sätze in Großbuchstaben sind im Internet gleichbedeutend mit Schreien (in der Chatsprache). Dieser Verdacht sollte weder in geschäftlichen noch in privaten E-Mails entstehen. AUSSERDEM LASSEN SICH TEXTE, DIE NUR IN GROSSBUCHSTABEN GESCHRIEBEN SIND, ÄUSSERST SCHLECHT LESEN.
- **Rechtschreibung:** Auch Tipp- und Rechtschreibfehler müssen nicht sein. Eine von Fehlern strotzende Mail ist nicht lässig – sondern nachlässig. Man kann seine Mail vorweg in einem Standard-Textverarbeitungsprogramm mit aktivierter Rechtschreibprüfung schreiben und anschließend den Text in den Mailer kopieren oder, falls vorhanden, das Rechtschreibprogramm im Mailer nutzen. Dies wird dann jeweils vor dem Versand der E-Mail aktiv.
- **Abkürzungen:** Die Kombination von Zahlen und Wortfetzen oder das gnadenlose Abkürzen von Begriffen ist zwar modern, aber nur für Eingeweihte zu verstehen. „FYI“ (for your information) ist vielleicht noch bekannt – aber andere Kürzel, die zum Beispiel in Chats gang und gäbe sind, gehören längst nicht zum Allgemeinwissen. Sie sollten daher in Mails möglichst nicht genutzt werden.
- **Vorsicht mit Ballast:** Im schnellen Medium werden auch schnelle Antworten erwartet. Und wenn es nur ein kurzer Dank oder die Bestätigung dafür ist, dass die Mail angekommen ist. Am einfachsten geht das, indem man auf den Schalter „Antworten“ in der Symbolleiste klickt. Der Text der ursprünglichen

Mail hängt dann der Antwort an. Das kann sinnvoll sein, denn wer viel mailt, vergisst möglicherweise, was er vor kurzem geschrieben hat – und so hat er Brief und Antwort in einer Mail vor Augen. Aber Vorsicht: Wird die Mail im Pingpong-Verfahren mehrmals hin- und hergeschickt, dann wird sie immer umfangreicher – bleiben doch die alten Texte erhalten. Empfehlenswert ist es, bei solchem E-Mailwechsel ältere Textteile hin und wieder zu löschen.

- **„Dicke“ Mails:** E-Mail-Anhänge von mehr als einem Megabyte sollte man nicht ungefragt verschicken, sondern in einer separaten Mail ankündigen. Das spart allen, die nur per Modem am Netz hängen, viel Wartezeit. Zudem erlauben bestimmte Provider die Versendung von E-Mails nur bis zu einer bestimmten Datenmenge.

CC und BCC

Es mutet schon anachronistisch an und ist es eigentlich auch: Wenn ich eine E-Mail an einen zweiten Empfänger schicken möchte, kann ich die Taste „Carbon Copy“ (CC) nutzen, die aus den Zeiten des Kohlepapiers und der Schreibmaschine stammt. Daneben gibt es die Taste „Blind Carbon Copy“.

Die elektronische Post sieht drei verschiedene Adresszeilen vor. Und die gilt es, richtig einzusetzen: An, CC und BCC stehen zur Auswahl

- In der An-Zeile wird der Adressat eingetragen, für den die Mail gedacht ist.
- Unter CC (steht für Carbon Copy und bedeutet Kopie) erscheinen all die, die eine Kopie dieses Schreibens bekommen sollen. So erfährt auch der ursprüngliche Empfänger, wer außer ihm mit dieser Nachricht versorgt wurde.
- Wer das vermeiden will, setzt diese Kopie-Adressen in die BCC-Zeile (das steht für Blind Carbon Copy und bedeutet Blindkopie). Blind deshalb, weil alle Adressen, die an dieser Stelle eingetragen werden, bei keinem Empfänger angezeigt werden. Sehr nützlich, wenn der Empfänger nicht sehen soll, an wen diese E-Mail außerdem ging. Außerdem ist auch dies eine Form des Datenschutzes, denn man sollte keine E-Mail-Adresse leichtfertig weitergeben.

Übrigens: Bei FOCUS-Online kann man seine E-Mail-Kenntnisse testen ☺ <http://www.focus.de/DD/DD176/dd176.htm> unter „Test: E-mail Knigge, Mailen mit Stil“.

🔗 Links

www.stiftung-warentest.de	Tests zu E-Mail Diensten Suchbegriff: E-Mail
www.netzwelt.de/sicherheit/spam.html	kostenlose Filtersoftware zum Download
www.internauten.de/22.0.html	Mission E-Mails und Spam
www.10minutemail.com	der kostenlose Wegwerf-E-Mail-Dienst
www.temporaryinbox.com	Kostenloser Wegwerf-E-Mail-Dienst
www.kidsville.de (unter „Internautenschule“)	Kidsville – Kinderseite mit Internautenschule
www.mediageneration.net/eMail	Online-E-Mail-Dienste im Überblick: Media@generation – Internetseite der GMK
www.secure-it.nrw.de (unter „Angebote für Schulen“)	Arbeitsmaterial: „Elektronische Signatur. Arbeitsmaterialien für den Unterricht“
www.kinderbrauser.de	Kinderbrauser mit Polly und Fred: (auch als CD-ROM des FWU zur Einführung ins Internet)
www.lehrer-online.de/it-sicherheit.php	Lehrer-Online – Unterrichtseinheiten und Infor- mationen zu verschiedenen Themen der IT-Sicherheit

Methodisch-didaktische Hinweise

Arbeitsblatt			
Zeitangabe (Unterrichtsstunden)	2	1	2
Ziele	Die Schülerinnen und Schüler lernen Tipps und Regeln für das Erstellen sicherer E-Mail-adressen kennen und können dieses Wissen praktisch anwenden, indem sie sich eine E-Mail-Adresse einrichten.	Die Schülerinnen und Schüler lernen die drei goldenen Regeln des E-Mailing kennen und können diese begründen.	Die Schülerinnen und Schüler reflektieren, welche wirtschaftlichen Interessen hinter Spam-Mails stecken.
Methode/n	Erwachsenenintegration	Ergänzungstext	Stufenleiter/Plakat
Organisationsform/en	Einzel/Partner, U-Gespräch	Einzel	Einzel/Partner, Großgruppe, U-Gespräch
Zugang Internet	ja	nicht zwingend	ja
Zugang PC	ja	nicht zwingend	ja



7_1 Spam-Mails

7_2 Viren, Würmer, Trojaner, Spyware

7_3 Illegale Downloads und Tauschbörsen

Kommentare zu den Arbeitsblättern

Hier sollen die Kinder zwei Anbieter von Kinder-E-Mail-Adressen kennen lernen. Dabei gibt es selbstverständlich das Problem, dass das Einverständnis der Eltern eingeholt werden muss, in diesem Fall sogar schriftlich.

Wichtiger sind vielleicht die Tipps zum E-Mailing, sodass bereits die Kinder die wichtigsten Regeln für ein sicheres Mailen kennen lernen. Hier könnte sich vielleicht sogar ein kleines Projekt mit E-Mailing anschließen, ein Austausch untereinander zu einem Thema zum Beispiel, das in der Schule besprochen wurde.



Anhand dieses Arbeitsblattes sollen die Schülerinnen und Schüler die drei „goldenen“ Regeln des E-Mailing kennen lernen und begründen können. Die Form des E-Mailing kann dabei gewählt werden, wenn die Möglichkeiten dazu bestehen, ansonsten lassen sie die Begründung vielleicht einfach als zusammenhängenden Text schreiben.

Die Ergänzungen zu den Sätzen soll eine kleine Wissensabfrage zum E-Mailing sein, denn oft beherrschen Schülerinnen und Schüler das E-Mailing, wissen aber nichts mit CC oder BCC o. ä. anzufangen:

Mögliche Antworten:

- Der Betreff einer E-Mail ist wichtig, weil ... der Empfänger daran sofort sehen kann, ob es eine Spam-Mail ist oder nicht, auch ohne sie zu öffnen.
- Wenn ich mehrere Empfänger habe, mache ich Folgendes ... Ich schreibe sie in die Empfängerzeile, getrennt durch ein Komma (Dies kann von Programm zu Programm variieren).
- Das BCC beim E-Mailing steht für ... Blind Carbon Copy, also eine „blinde“ Kopie. Die anderen Empfänger der E-Mail können diesen BCC-Empfänger nicht sehen.
- Anhänge öffne ich nur von ... Bekannten oder Freunden oder wenn ich weiß, von wem er stammt.
- Große Dateien über 1 MB verschicke ich nur, wenn ... es unbedingt notwendig ist und ich beim Empfänger nachgefragt habe.


- Ich habe zwei E-Mail-Adressen, weil ... ich eine private benutze für meine Freunde und Bekannten. Eine andere gebe ich öffentlich weiter.
- Die privaten E-Mail-Adressen bekommen nur ... meine Freunde und Bekannten.
- Das mache ich mit blöden E-Mails ... Ich lösche sie sofort oder ich markiere sie als SPAM.
- E-Mails von Unbekannten behandle ich so: Ich öffne nie Anhänge und bin vorsichtig mit dem Inhalt. Wenn mir etwas komisch vorkommt, lösche ich sie. Vor allem antworte ich nicht ohne weiteres.
- Auch in E-Mails bin ich höflich, weil ... auf der anderen Seite keine Maschinen, sondern Menschen sitzen.



Als Einstieg dient ein kurzer Text zur Problematik der Spam-Mails. Wie auch bei den anderen Arbeitsblättern geht es auch hier um einen kompetenten Umgang mit Spam-Mails. Hier sollen die Schülerinnen und Schüler die Tipps im Internet selbstständig recherchieren und bewerten.

Der dritte Arbeitsauftrag schließlich dient der Vertiefung. Vielleicht spornen sie hier ein wenig die Kreativität der Jugendlichen an?

**Möglichkeiten zur Weiterarbeit
„Lust auf mehr“**

E-Mailing bietet viele Anknüpfungspunkte für die Schule. Interessant ist vielleicht im Fach Deutsch eine Fortführung des Themas zur E-Mail-Sprache. Interessante Beispiele für verhunzte E-Mails hat die Süddeutsche Zeitung gesammelt:  www.sueddeutsche.de/jobkarriere/erfolggeld/artikel/540/82458/.

Sie könnten als Einstieg in eine Überprüfung der Sprache in E-Mails dienen. Eine tolle Unterrichtsreihe zum Thema Verschlüsselung von E-Mails bietet Lehrer-Online unter

 www.lehrer-online.de/sichere-e-mail.php.

Ganz spannend ist vielleicht neben der kommerziellen Frage von Spam-Mails auch die Frage nach dem Zeitverlust durch das E-Mailing in den Firmen oder auch – etwas abstrakter – die Frage nach der Veränderung unserer Kommunikation.



Arbeitsblatt vom

Name:

Was ist Spam?



E-Mails sind toll. Du kannst allen Freundinnen und Freunden schreiben und Post bekommen. Aber leider gibt es große Probleme durch unerwünschte E-Mails, die auch als „Spam-Mails“ oder kurz „Spams“ bezeichnet werden. Diese Spams können Werbung sein und auch gefährliche oder nicht für Kinder geeignete Inhalte haben.

1. Arbeitsauftrag:

Lies die Tipps zum sicheren E-Mailing.

Schreibe in die Spalte „warum?“, aus welchem Grund dieser Tipp wichtig sein kann.

Regeln/Tipps

warum?

Ich suche mir einen Spitznamen, der nichts über mich verrät! (auch nicht, ob ich ein Junge oder ein Mädchen bin).

Ich gebe mein Kennwort niemals weiter.

Ich gebe niemals meine Adresse, Telefonnummer oder andere Daten weiter.

E-Mails, die irgendwie komisch sind, beantworte ich nie.

Ich treffe mich nie mit E-Mail-Freundschaften, außer meine Eltern haben es erlaubt.

Wenn ich etwas doof finde oder mir etwas Angst macht, gebe ich sofort meinen Eltern Bescheid.

Ich öffne keine Anhänge (wie Bilder oder Dateien) von Unbekannten.

Ich gebe meine E-Mail-Adresse nur Freunden.

2. Arbeitsauftrag:

Besprecht die Tipps in der Klasse!



Arbeitsblatt vom

Name:

Damit Kinder sicher E-Mails benutzen können, gibt es Anbieter, die spezielle Kinder-E-Mail-Adressen anbieten. Hier lernst du zwei von ihnen kennen: Bei beiden musst du dich anmelden, sogar schriftlich und mit Unterschrift der Eltern!

Name	Mail4Kidz	ZUM-Mail
Internet-Adresse	 www.mail4kidz.de	 www.zum-mail.de
Anleitung / Wichtiges	 www.mail4kidz.de/eltern	 www.zum-mail.de/pdf/webmail.pdf
Anmeldeformular	 www.mail4kidz.de/registrieren.phtml	 www.zum-mail.de/grundschule/antrag.pdf

3. Arbeitsauftrag:

Schaue dir beide Seiten an und zeige sie deinen Eltern. Frage nach, ob sie mit einer Anmeldung dort einverstanden sind! Falls sie einverstanden sind – und falls du möchtest – melde dich bei einer der beiden Adressen an!

Tauscht doch mal untereinander eure E-Mail-Adressen aus und schreibt euch was Nettes.



Arbeitsblatt vom

Name:

Spam-Mails – wie schützt du dich?



Spam-Mails sind eine wahre Plage, oder? Bestimmt hast du auch schon solche unerwünschten E-Mails bekommen. Der Name stammt übrigens von „Spiced HAM“ (englisch für „gewürzter Schinken“) was früher der Name eines Dosenfleisches war. Als Begriff für „massenhaft“ und „unerwünscht“ soll das Wort aus einem alten Fernsehsketch der Komikergruppe „Monty Python“ stammen.

Spam-Mails sind nicht nur lästig, sondern können auch gefährlich werden. Deshalb gibt es drei goldene Regeln des E-Mailing:

- niemals auf eine Spam-Mail reagieren
- den Spam-Filter „trainieren“
- die E-Mail-Adresse nicht überall angeben und immer eine zweite E-Mail-Adresse anlegen

1. Arbeitsauftrag:

Überlege, warum diese Regeln sinnvoll sind! Schreibe eine E-Mail an eine Freundin/einen Freund, indem du ihr/ihm diese Regeln erklärst. Wenn du keine Möglichkeit hast eine E-Mail zu schreiben, schreibe die Erklärung auf die Rückseite des Arbeitsblattes!

2. Arbeitsauftrag:

Aber es gibt noch weitere wichtige Dinge, die man beachten sollte. Hier findest du Hinweise, ergänze sie zu ganzen Sätzen:

Der Betreff einer E-Mail ist wichtig, weil ...

Wenn ich mehrere Empfänger habe, mache ich folgendes ...

Das BCC beim E-Mailing steht für ...

Anhänge öffne ich nur von ...

Große Dateien über 1 MB verschicke ich nur, wenn ...

Ich habe zwei E-Mail-Adressen, weil ...

Die privaten E-Mail-Adressen bekommen nur ...

Das mache ich mit blöden E-Mails ...

E-Mails von Unbekannten behandle ich so:


Auch in E-Mails bin ich höflich, weil ...



Arbeitsblatt vom

Name:

Vollgemüllt?!

 T-Online verzeichnete im April 2006 nach eigener Aussage täglich bis zu 1 Milliarde Spam-Mails und Schätzungen gehen dahin, dass heutzutage neun von zehn E-Mails unerwünscht sind. Und dies bei einer geschätzten Zahl von weltweit 100 Milliarden E-Mails pro Tag. Die Firma „McAfee“ meldete im August 2007, dass 85% aller E-Mails im Jahre 2006 Spam-Mails waren, übrigens lag der Anteil im Jahre 1997 noch bei 5%! (Quelle: FOCUS 32/2007, S. 150)

Der Versand von E-Mails ist kostenlos (es gibt Stimmen, die darin ein Grundübel des Problems sehen), kostet aber Computerkapazität und Zeit ... Warum also gibt es eine solche Flut? Spams bringen Geld und man vermutet dahinter mafiöse und inzwischen gut organisierte Strukturen.


Zum einen gibt es tatsächlich noch Kunden, die auf Angebote aus Spam-Mails reagieren, was bei den minimalen Kosten auch bei einem Kunden pro 100.000 noch ein gutes Geschäft ist. Zum anderen werden Börsengeschäfte durch Aktientipps manipuliert. Und schließlich gibt es noch die verseuchten Spam-Mails, die den Computer des Empfängers mit einem Virus infizieren. Anschließend kann der Computer ausgespioniert oder fremdgesteuert werden.

1. Arbeitsauftrag:

Recherchiere im Netz, warum es so viele Spam-Mails gibt. Welche Geschäfte lassen sich damit machen? Suche aktuelle Beispiele und stelle sie den anderen vor!

2. Arbeitsauftrag:

Im Internet gibt es viele gute Tipps, wie man sich vor Spam-Mails schützen kann. Suche gute Tipps heraus und schreibe diese mittels einer Stufenleiter auf. Ganz oben steht hierbei der wichtigste Tipp!

 TIPP: Es gibt so genannte „Wegwerf-E-Mail-Adressen“, die man nur für kurze Zeit nutzen kann und die sich danach wieder selbst zerstören. Hier findest du eine Liste mit Anbietern: www.jethwa.de/aktuell,liste-anbieter-von-wegwerfemailadressen,72.html

3. Arbeitsauftrag:

Vergleiche deine Ergebnisse mit den Ergebnissen der Anderen und erstellst ein gemeinsames Plakat der besten Tipps, gestaltet es auffällig, arbeitet auch mit Farben!

7_1 Spam-Mails

7_2 Viren, Würmer, Trojaner, Spyware

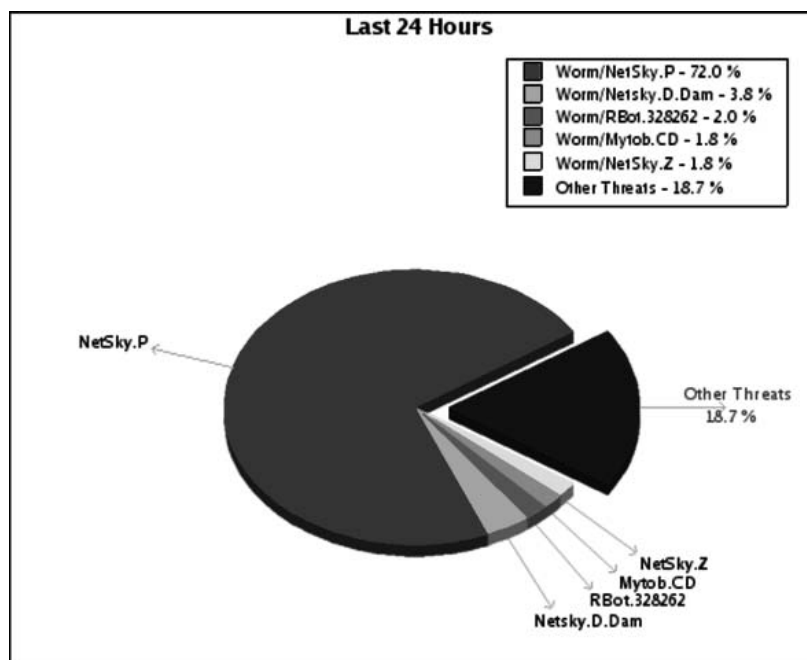
7_3 Illegale Downloads und Tauschbörsen

Sachinformation

Geschichte und Entwicklung

Der Klein-Zoo aus Viren und Würmern hat weltweit so erschreckend viele Tiere „in der Wildnis“ („in the wild“ ist der Ausdruck der Antiviren-Kämpfer für akute Bedrohungen), dass Experten wie Toralv Dirro von der Sicherheits-Software-Firma McAfee vermuten, die „Cyber-Mafia“ ist wie eine Industrie organisiert (Quelle: „Spiegel Special: Wir sind das Netz“ 03/2007, S. 90) und es geht um so klassische Verbrechen wie Betrug, Erpressung und illegale Geldbeschaffung. Die Schäden gehen jährlich in die Milliarden. Dabei hatte alles so harmlos mit einem kleinen Wurm angefangen, der für die Programmierer John Hepps und John Shock im Jahre 1982 Routineaufgaben erledigen sollte. Das Ergebnis waren leider 100 tote Computer im Xerox Research-Center in Palo Alto. Virus Nummer 1 stammte hingegen aus Pakistan und hörte auf den Namen BRAIN. Auch dieser war eigentlich harmlos, denn zwei Brüder wollten den Weg ihrer raubkopierten Disketten (damals gab es das noch!) mit Computerspielen nachverfolgen. Und wer noch ein wenig in Erinnerungen an die gute alte Viren-Zeit schwelgen will, dem seien noch

Namen genannt, die auch durch die Presse geisterten: „BugbearB“, „Blaster“, „I love you“, „Melissa“, „Sasser“ und viele andere. In den letzten Jahren aber scheint die Dimension und die Professionalität neue Ausmaße angenommen zu haben, denn es sind nicht mehr talentierte, aber verantwortungslose Programmierer, die – warum auch immer – die Unsicherheit der Computernetze und der Betriebssysteme ausnutzen wollen, sondern offenbar gut organisierte Banden. Der neueste Trick: Schutzgelderpressung online. Mit einer harmlosen Variante wird die Verletzlichkeit des Datenbestandes dargestellt: Wer nicht zahlt, wird digital angegriffen. (Quelle: ebd.). Aus diesem Grunde sind die spektakulären Viren-Fälle in den Jahren 2006 und 2007 auch ausgeblieben. Die neue Generation arbeitet lieber im Verborgenen. Der hohe Grad der Vernetzung durch das Internet, durch Funknetze aber auch per Handy steigert indes das Sicherheitsrisiko. Einen Monitor der Virenbedrohung bietet die Firma Avira auf ihrer Website. Dort kann man sich die Angriffe der letzten 24 Stunden und weitere Statistiken anzeigen lassen: ☺ www.avira.com, unter „Virus-Info“.



Screenshot: Die letzten 24 Stunden (24.7.2007, 15 Uhr bis 25.7.2007, 15 Uhr), dargestellt als Viren-Bedrohung auf


☺ www.avira.com/en/threats/index.html


7_1 Spam-Mails

7_2 Viren, Würmer, Trojaner, Spyware

7_3 Illegale Downloads und Tauschbörsen

Viren und Würmer

Eigentlich kennen wir am Computer „Viren“ und meinen damit alle Programme, die böswillig sind und Schaden an fremden Computern anrichten wollen. Streng genommen muss man unterscheiden zwischen Viren, Würmern, Trojanern, Spyware (und Hoaxes, die praktisch elektronische Kettenbriefe sind und meistens keinen Schaden anrichten; deshalb lassen wir sie hier weg). Eine Übersicht mit Beschreibungen aktueller Viren bietet das Bundesamt für Sicherheit in der Informationstechnik unter  www.bsi.de.

Viren. Computerviren sind kleine, von Menschen geschriebene Computerprogramme, die das Ziel haben, sich möglichst rasch zu verbreiten. An den befallenen Computern können sie Schäden von unterschiedlichem Ausmaß anrichten. Viren brauchen ein Transportmittel um sich verbreiten zu können. Welchen Schaden sie anrichten, das hängt von dem betreffenden Virus und Wurm ab, die Schlimmsten löschen die Festplatte und zerstören das ganze Windows-System. „Lovebug“ bspw. richtete weltweit im Jahre 2000 einen Schaden von sieben Milliarden! Dollar an! (Quelle: „Viren, Hacker, Firewalls“ von Andreas Janssen, 3. Auflage 2007;  www.knowware.de)

Würmer. Würmer funktionieren ähnlich wie Viren, benötigen zur Verbreitung jedoch keine anderen Programme. Sie können sich selbst kopieren und als Anhang einer E-Mail versenden. Öffnet man diese angehängte Datei, wird der Wurm aktiviert.

Trojaner und Spyware

Bei Trojanern und Spyware handelt es sich im Großen und Ganzen um Dateien, die Daten eines PCs ohne Zustimmung über das Internet an andere Leute verschicken können. Weiterhin sind damit auch sämtliche Prozesse gemeint, die sich auf einem PC abspielen, die Daten verfolgen und weitergeben. Was das bedeutet, kann man sich leicht vorstellen, denn alle privaten Daten, Passwörter und so weiter fallen in fremde Hände.

Trojaner. Die Legende vom Trojanischen Pferd ist bekannt: Versteckt im Inneren eines Holzpferdes sollen griechische Soldaten in die Stadt Troja gelangt sein, um diese zu erobern. In der PC-Welt versteht man unter Trojanern oder Trojanischen Pferden scheinbar nützliche Programme, in denen Viren, Würmer oder Spionagesoftware enthalten sein können. Die Programmierer, die diese Schädlinge in Umlauf bringen, sind sehr geschickt und tarnen die Trojaner, in denen die Spyware enthalten sein kann, gut.

Spyware. Versteckt in Trojanern – oder ungewollt über „aktive Inhalte“ von Internetseiten – kann Spyware auf dem Rechner installiert werden. In der Regel bemerkt der Nutzer weder etwas von der Installation, noch vom Ausführen der Programme. Häufig ist auch in so genannter „Adware“ ein Spionageprogramm eingebunden und man installiert in gutem Glauben die eigentliche Software + den Trojaner. So manche Spyware („Keylogger“ genannt) kann genaue Tastenbetätigungen aufzeichnen und den Empfängern der Daten sämtliche eingetippte Passwörter und Namen überliefern. So können das Surfverhalten von Nutzern sowie sensible Daten (Passwörter, Zugangs- und Kreditkartennummern, Kontonummern) ausgespäht und weitergeleitet werden. Beim Diebstahl von Passwörtern spricht man auch von Password-Fishing oder „Phishing“. Häufig werden unbemerkt und ungewollt weitere Programme installiert, wie z.B. Dialer oder Software zur Errichtung sog. „Botnets“. Botnets sind dezentrale Netzwerke – meist von Privatcomputern – die als Verteiler für den massenhaften Versand von Werbe-E-Mails oder für Hackerangriffe auf Bankkonten u.Ä. genutzt werden. Man kann sie auch als „Zombie-Rechner“ veranschaulichen, die ohne das Wissen des Besitzers illegale Dinge tun.



Die Problematik

Von der oben erwähnten Cyber-Mafia bleibt der Normal-User üblicherweise verschont. Dennoch können Viren und Würmer auf dem Computer schlimme Folgen haben. Die Auswirkungen reichen von merkwürdigen Botschaften auf dem Bildschirm über Rechnerabsturz bis zum Löschen von Dateien oder schlimmstenfalls der kompletten Festplatte. Darüber hinaus können ganze Netzwerke lahm gelegt werden bzw. zu einer Verlangsamung des Internetverkehrs führen. Während man sich Viren durch das Öffnen von Dateien oder E-Mail Anhängen i.d. Regel aktiv „einfängt“, verbreiten sich Würmer häufig vom Benutzer unbemerkt über die Adressbücher der E-Mail-Inhaber.

Das Problem ist auch größer geworden durch viele „aktive“ Inhalte, also Programme, die selbstständig Aktionen ausführen können. Aus diesem Grunde können Viren, Würmer, Trojaner und Spyware nicht nur in (ausführbaren) Programmen stecken, sondern auch in E-Mails, Bildern, Word-Dokumenten und sogar ganz einfach über das Aufrufen einer Internetseite. Ein Schutz davor ist fast unmöglich, aber trotzdem können sie etwas tun.

Vorbeugung

Um sich vor Schadprogrammen zu schützen, sind neben technischen Maßnahmen auch einige Vorsichtsmaßnahmen einzuhalten, um das Risiko einer Infizierung zu reduzieren:

- externe Daten, die auf den PC geladen werden, auf ihre Seriosität prüfen
- einen Download nur von vertrauenswürdigen Adressen starten
- E-Mail-Anhänge nur öffnen, wenn sie von bekannten Personen stammen und erwartet werden
- aktuelle Version des Betriebssystems und der Anwendersoftware, d. h. regelmäßige Updates machen
- die Ausführung von „aktiven Inhalten“ durch entsprechende Einstellungen in ihrem Browser (dadurch wird allerdings der Komfort beim Surfen eingeschränkt, hiermit ist vor allem das Abschalten von Javascript, Java, ActiveX usw. genannt) verhindern
- nur solche Software aus dem Internet auf ihrem PC installieren, die sie wirklich brauchen

Anti-Viren-Programm

Auf ein Antivirenprogramm sollte man nicht verzichten. Egal für welches Antiviren-Programm man sich entschieden hat, wichtig sind regelmäßige Updates, damit der Rechner auch gegen neue Viren geschützt ist. Es gibt gute kostenlose Antiviren-Software und selbstverständlich kommerzielle Produkte. Wichtig ist, dass man einen seriösen Anbieter wählt.

Benutzerprofile

Benutzen sie Windows, so sollten sie als normaler Benutzer arbeiten und nicht als „Administrator“, auch wenn es im Alltag manchmal mühselig ist umschalten zu müssen. Wird der Computer gar von mehreren Personen benutzt, so sollte jede Person ein eigenes Benutzerprofil (unter Windows XP bei Start – Systemsteuerung – Benutzerkonten) haben, selbstverständlich ohne Administratorenrechte. Hierfür sollte ein eigener „Admin“, „Chefin“ oder „Boss“ eingerichtet werden. Dadurch vermindert man den Schaden, den ein Virus verursachen kann, beträchtlich.

Firewall

Der Rechner kann außerdem durch eine persönliche Firewall (der Ausdruck stammt von der „Brandwand“ als Element des vorbeugenden Brandschutzes beim Hausbau) oder ein Netzwerk durch eine zentrale Firewall

7_1 Spam-Mails

7_2 Viren, Würmer, Trojaner, Spyware

7_3 Illegale Downloads und Tauschbörsen

geschützt werden. Diese schützt vor Angriffen und unberechtigten Zugriffen aus dem Internet. Die Windows-Firewall sollte deshalb niemals ausgeschaltet sein und auch die Ausnahmen (also die Programme, die sie umgehen dürfen) gering gehalten werden.

Befallene Rechner

Woran erkennen sie einen befallenen Rechner? Zum Beispiel durch langsames Surfen im Internet, häufige Werbefenster, einen geänderten Browser (z. B. die Startseite, geänderte Favoriten); weiterhin verbindet der PC sich selbstständig mit dem Internet. Außerdem sollten sie die Antiviren-Software warnen, vielleicht lassen sie auch mal gezielt suchen. Wichtig ist: Die Viren mutieren wie ihre biologischen Pendanten ständig, nur eine aktuelle Antiviren-Software hilft wirklich! Bei einem speziellen Befall – sie wissen, um welchen Virus oder Wurm oder Trojaner es sich handelt –, helfen die entsprechenden Experten meist schnell und bieten ein Tool zum Entfernen an. Aber! Auch hier gilt: Seriöse Quellen wählen! (s. Links).

Der Kompass

Neugierig, ob Ihr persönlicher Schutz ausreicht? Dann sei Ihnen der Kompass der Polizei empfohlen:

📍 www.polizeiberatung.de, unter „Vorbeugung“, „Gefahren im Internet“, „Sicherheitskompass“.

Industrie und Schule

In der Schule brauchen wir uns vielleicht nicht so viele Sorgen machen wie ein Unternehmen, wenn es um die Datensicherheit geht. Einer der Tricks, wie Unbefugte auch ein gut gesichertes System infizieren können: Ein scheinbar herrenloser USB-Stick wird in der Firma platziert. Ein Mitarbeiter findet ihn, die Neugierde lässt den Stick einstecken, und schon ist das Beste von außen gesicherte System infiziert. Eine Kontrolle darüber, wer mit welchem USB-Stick am Computer war bietet z. B. die kostenlose Mini-Software „Dubium“. Sie listet auf, welche Sticks in letzter Zeit an der USB-Buchse eingesteckt waren.

www.secure-it-guard.de

📍 Links

www.bsi-fuer-buerger.de

Startseite des Bundesamtes für Sicherheit in der Informationstechnik, Informationen über „Viren und andere Tiere“ des BSI, Informationen zu Spyware und Adware des BSI

www.klicksafe.de

Informationen zu „Viren und Schädlingen“ sowie „Das Sicherheitsquiz für Kinder“ von Klicksafe

www.secure-it.nrw.de

„Arbeitsmaterialien für den Unterricht. Viren, Würmer, Trojaner“ (unter „Angebote für Schulen“). Broschüre „Computerkriminalität: So hilft die Polizei“ des nordrhein-westfälischen Landeskriminalamts (LKA) & der Initiative „secure-it.nrw“

www.sicher-im-netz.de

die Initiative „Deutschland sicher im Netz“ mit vielen namhaften Unternehmen als Mitglieder

www.lehrer-online.de/it-sicherheit.php

Unterrichtseinheiten und Hintergrundinformationen rund um das Thema IT-Sicherheit von Lehrer-Online

www.lehrer-online.de/viren-wuermer-trojaner.php




Unterrichtseinheit zum Thema Viren, Würmer und Trojaner

www.internauten.de/21.0.html

Quiz zur „Mission Download“ der Internauten

www.blinde-kuh.de/viren	die Kinder-Suchmaschine Blinde Kuh mit kindgerechten Informationen zu Viren und Co
www.lavasoft.com	Download der kostenlosen Software „Ad-Aware“ zum Erkennen von Spyware. Achtung: Nach der Installation werden sie erneut nach den kostenpflichtigen Varianten gefragt, einfach „Abbrechen“ anklicken
www.free-av.de	AntiVir PersonalEdition Classic, eines der weit verbreitetsten Antiviren-Programme der Fa. Avira Achtung: Es gibt auch kostenpflichtige Varianten
www.gmk-net.de (Pdf-Datei zum Download)	„Was tun bei Dialern, Spam und Viren?“ Eine Broschüre der Gesellschaft für Medienpädagogik und Kommunikationskultur (GMK)

Methodisch-didaktische Hinweise

Arbeitsblatt			
Zeitangabe (Unterrichtsstunden)	2–3	1–2	2–3
Ziele	Die Schülerinnen und Schüler werden mit dem Problem „Computervirus“ konfrontiert und überprüfen die Einstellungen am eigenen Computer/Schulcomputer.	Die Schülerinnen und Schüler erhalten Basisinformationen über das Problem „Computervirus“ und erarbeiten selbständig vertiefende Informationen und ein Merkblatt zu den verschiedenen Schutzmechanismen.	Die Schülerinnen und Schüler erarbeiten selbständig die wichtigsten Informationen zu Geschichte, Form, Schutz und Schäden durch Computerviren.
Methode/n	Schrittfolge, Plakat, Experte	Partnerinterview, Plakat, Experte (optional)	Gruppenarbeit, Präsentation, Stationenlernen oder „one stray – the others stay“ (optional)
Organisationsform/en	Einzel, U-Gespräch, Erwachsenenintegration	Einzel/Partner	U-Gespräch, Kleingruppe
Zugang Internet	ja	ja	ja
Zugang PC	ja	ja	ja



7_1 Spam-Mails

7_2 Viren, Würmer, Trojaner, Spyware

7_3 Illegale Downloads und Tauschbörsen

Kommentare zu den Arbeitsblättern



Zugegebenermaßen ist das Virenproblem am Computer für die jüngeren Schülerinnen und Schüler abstrakt und wenig fassbar. Das Arbeitsblatt gibt einige Informationen, die sie vielleicht mit einem deutlichen Beispiel (z. B. aus der eigenen Erfahrung) garnieren oder einführen können. Viele der Schülerinnen und Schüler kennen aber den Begriff des Computervirus und wissen auch, dass es sich um Schädlinge handelt.

Die Handlungsanleitungen zum E-Mailing können als Ergänzung des Kapitels „Spam-Mails“ verstanden und eingesetzt werden. Hier ist logischerweise die Hilfe von Erwachsenen gefordert, vielleicht können sie auch einen Experten aus dem Kollegium oder der Elternschaft hinzuziehen, der einige Beispiele veranschaulichen kann. Wichtig ist sicherlich auch, den Kindern keine Angst zu machen, sondern nur Vorsicht zu vermitteln im Umgang mit E-Mails und Downloads. Die angegebene Internetadresse von Internet-ABC ist sehr zu empfehlen und zeigt sehr anschaulich das Problem rund um den Computerzoo.



Nach einem kurzen einführenden Text sollen die Schülerinnen und Schüler hier in Gruppen arbeiten. Zu jeder der vier Gruppen (Geschichte, Formen, Schutz und Schäden durch Computerviren) sind einige Internetadressen angegeben, wo die Informationen zu dem Thema zu finden sind. Jede Gruppe soll eine kurze (gedacht sind fünf Minuten, was sie selbstverständlich ändern können) Präsentation erstellen und diese dann den anderen vorstellen. Wenn die Möglichkeit besteht, bietet sich eine Präsentationssoftware wie Microsoft PowerPoint oder Open Office Impress an. Die Präsentationen können im klassischen Referatsstil vor dem Plenum gehalten werden oder in einem Galeriegang. Vielleicht ist aber auch die Methode „one stay – the others stray“ möglich: Von Vorteil ist ein „Laufzettel“, mit dem alle Gruppen „abgehakt“ werden können. Er könnte so aussehen:

Gruppe	Besucht?	Wichtige Informationen	Noch offene Fragen
Geschichte der Computerviren			
Formen von Computerviren			
Schutz vor Computerviren			
Schäden durch Computerviren			



Im zweiten Arbeitsauftrag sollen die Schülerinnen und Schüler nach der Informationsbeschaffung ihren Partner/ihre Partnerin informieren. Dies kann in Form eines „Partnerinterviews“ geschehen: Als Synthese soll dann eine Seite mit den wichtigsten Informationen entstehen. Vielleicht besteht die Möglichkeit, auch andere Klassen über das Problem zu informieren. Vielleicht in Form eines „Stationenlernens“?

Möglichkeiten zur Weiterarbeit „Lust auf mehr“

Wie oben bei den Sachinformationen erläutert, scheint die Zeit der jugendlichen Computergenies, die die technischen Möglichkeiten testen wollen, vorbei zu sein. Die Viren und Würmer haben einen kriminellen Hintergrund bekommen. Diese Dimensionen und die Schäden, vielleicht auch die Hintergründe, sind eventuell spannende Themen bei älteren Schülerinnen und Schüler zum Thema Wirtschaft.



Arbeitsblatt vom

Name:

Wie schützt du dich vor Computerviren?

Hattest du schon einmal ein Problem mit deinem Computer? Dann war vielleicht ein Computervirus schuld!



Computerviren nennt man kleine Programme, die an deinem Computer Schaden anrichten. Dann kann es passieren, dass plötzlich wichtige Dateien gelöscht sind oder dein Computer nicht mehr richtig funktioniert oder wichtige Dinge wie deine eigenen Passwörter gestohlen werden. Diese Computerviren verbreiten sich ganz schnell, und es gibt ziemlich viele von ihnen, Experten schätzen über 100.000. Und weil das alles noch nicht schlimm genug ist: Ständig kommen neue hinzu, manchmal sogar täglich. **Und wie werden Computerviren verbreitet?** Die größte Gefahr geht heutzutage von E-Mails und Internetseiten aus. Oft werden viele Tausend E-Mails gleichzeitig verschickt. In den E-Mails gibt es einen „Anhang“ (englisch „Attachment“), wenn du diesen öffnest, kann sich das Computervirus auf deinem Computer ausbreiten.


Wie schütze ich mich vor Viren?

Das sollte ich tun:	So kontrolliere ich es:	Was muss ich tun?
Ich benutze ein Antiviren-Programm.	1. Antiviren-Programme finden sich bei Windows meist rechts unten als kleines Symbol. 2. Ich frage meine Eltern, ob sie ein solches Programm benutzen.	Sofort eines auf den Computer laden – ich frage einen Erwachsenen danach. Es gibt kostenlose Programme!
Ich öffne nie einen seltsamen/merkwürdigen/komischen Anhang in E-Mails.	Ich schaue in meine E-Mails nach den Anhängen, ohne sie zu öffnen.	Diese E-Mails lösche ich sofort!
Ich lade nichts von Internetseiten herunter.	Windows fragt bei mir immer nach, wenn etwas aus dem Internet auf meinen Computer geladen werden soll. Dann frage ich immer einen Erwachsenen.	Ich klicke auf „Abbrechen“ und schließe die Internetseite sofort.

1. Arbeitsauftrag:

Sei der Virendoktor und überprüfe, ob dein Computer gut vor Computerviren geschützt ist. Kontrolliere vor allem das Antiviren-Programm! Erstelle einen Merkzettel, auf dem du alle Schritte beim Verarzten deines Computers festhältst.



Leider ist auch die Sache mit den Viren in Wirklichkeit viel komplizierter. Wenn du mehr lernen möchtest, dann schaue hier:
 www.internet-abc.de/kinder/109922.php

2. Arbeitsauftrag:

Male oder zeichne dir ein Plakat mit dem Schutz vor Viren! Hänge es dir an den Computer, damit du immer daran denkst!



Arbeitsblatt vom

Name:

Ein ganzer Zoo im Computer?

Ein wenig Computer-Biologie? Wenn wir über Computerviren sprechen, dann meinen wir einen ganzen Zoo:

Computerviren

Darunter sind solche Dinge gefasst wie Bootviren (dann startet der Computer erst gar nicht mehr), Makroviren (weit verbreitet in Office-Programmen), Datei-Viren (sie starten mit einem Programm), Polymorphe Viren (sie heißen so, weil sie sich gut verkleiden können und ständig verwandeln) und die Tarnkappen-Viren (die sich besonders gut verstecken können).

„Trojaner“ – Trojanische Pferde

(Kennst du die Sage vom Trojanischen Pferd?) Ein Trojaner benutzt einen gemeinen Trick. Das Virus gibt vor, etwas anderes zu sein (z. B. ein Spiel oder nützliches Programm): Kaum hast du es aufgerufen, befällt es deinen Computer. In diesen Trojaner kann auch ein Spionageprogramm versteckt sein, das deinen Computer auskundschaftet (und deine Passwörter munter weiterleitet).

„Würmer“

Ein Wurm kann sich selbst vervielfältigen und automatisch Kopien verschicken. Er braucht auch kein anderes Programm (wie ein Virus), sondern arbeitet ganz selbstständig.



Hoaxes

Ein Hoax (zu Deutsch: Jux, Schabernack oder Schwindel) ist nichts anderes als eine Falschmeldung, die per E-Mail verbreitet wird. Ein Hoax besteht meist aus drei Elementen; einem Aufhänger, der Echtheit vermitteln soll, gefolgt von einer Aufklärung über die aus dem Internet drohende Gefahr und der abschließenden Bitte, diese Information an so viele Internetnutzer wie möglich weiterzuleiten. Echte Virus-Warnungen werden nie auf diese Weise verschickt.

Und wie kommen diese Viren, Würmer, Trojaner und Hoaxes auf deinen Computer?
Und wie kannst du dich davor schützen?

1. Arbeitsauftrag:

Informiere dich über das Problem auf den folgenden Seiten bei klicksafe.de und beim Internet-ABC:

-  www.internet-abc.de und
-  www.klicksafe.de

2. Arbeitsauftrag:

Wie sieht ein wirksamer Schutz aus? Erkläre es deiner Nachbarin/deinem Nachbarn und umgekehrt!

3. Arbeitsauftrag:

Erstelle eine Übersicht mit den wichtigsten Informationen über Viren und den Schutzmaßnahmen! Versuche doch bitte, Symbole und Bilder in deine Übersicht einzubringen. Falls du noch genügend Zeit hast, erstelle in MS Word/OpenOffice.writer ein Merkblatt mit Symbolen!



Arbeitsblatt vom

Name:

Computerviren – weißt du alles?



Es hatte alles so harmlos mit einem kleinen Wurm angefangen, der für die Programmierer John Hepps und John Shock im Jahre 1982 Routineaufgaben erledigen sollte. Das Ergebnis waren 100 tote Computer im Xerox Research-Center in Palo Alto. Virus Nummer 1 stammte hingegen aus Pakistan und hörte auf den Namen BRAIN. Auch dieser war eigentlich harmlos, denn zwei Brüder wollten den Weg ihrer raubkopierten Disketten – damals gab es das noch! – mit Computerspielen nachverfolgen. Und wer noch ein wenig in Erinnerungen an die gute alte Viren-Zeit schwelgen will, dem seien noch Namen genannt, die auch durch die Presse geisterten: „Bugbear“, „Blaster“, „I love you“, „Melissa“, „Sasser“ und viele andere. In den letzten Jahren aber scheint die Dimension und die Professionalität neue Ausmaße angenommen zu haben, denn es sind nicht mehr nur talentierte, verantwortungslose Programmierer, die – warum auch immer – die Unsicherheit der Computernetze und des Betriebssystems ausnutzen wollen, sondern offenbar gut organisierte Banden.

Der neueste Trick: Schutzgelderpressung online ... mit einer harmlosen Variante wird die Verletzlichkeit des Datenbestandes dargestellt: Wer nicht zahlt, wird digital angegriffen. (Quelle: „Spiegel Special: Wir sind das Netz“ 03/2007, S. 90.). Aus diesem Grunde

sind die spektakulären Viren-Fälle in den Jahren 2006 und 2007 auch ausgeblieben. Die neue Generation arbeitet lieber im Verborgenen. Der hohe Grad der Vernetzung durch das Internet, durch Funknetze auch per Handy steigert indes das Sicherheitsrisiko.

1. Arbeitsauftrag: Bildet folgende 4 Gruppen:

Gruppe	Thema	Internet-Adressen
A	Geschichte der Computerviren	www.securitymanager.de/magazin/artikel_742_die_geschichte_der_computerviren.html www.zdnet.de/security/analysen www.bsi.de/av/virbro/kap1/kap1_1.htm www.spiegel.de/netzwelt/tech
B	Formen von Computerviren	www.klicksafe.de/schmutz/viren.php www.internet-abc.de www.bsi-fuer-buerger.de/viren
C	Schutz vor Computerviren	www.klicksafe.de/schmutz/viren.php www.internet-abc.de www.bsi-fuer-buerger.de/viren www.bsi-fuer-buerger.de/infiziert www.bsi-fuer-buerger.de/schuetzen
D	Schäden (auch wirtschaftliche) durch Computerviren	www.bsi-fuer-buerger.de/infiziert www.zdnet.de/security/news/

2. Arbeitsauftrag: Erarbeitet innerhalb eurer Gruppe das Wichtigste zum Thema! Welche sind die zentralen Probleme und die zentralen Thesen, die dargestellt werden?

3. Arbeitsauftrag: Bereitet eine maximal 5-minütige Präsentation vor! Benutzt ein Plakat oder MS PowerPoint/ OpenOffice.impress oder ähnliches dazu! Informiert die anderen Gruppen über euer Thema in der Präsentation!

7_1 Spam-Mails

7_2 Viren, Würmer, Trojaner, Spyware

7_3 Illegale Downloads und Tauschbörsen

Sachinformation

Der schnelle Klick

Noch nie war es so einfach, Bilder, Texte, Lieder, Videos oder Software auf dem heimischen Computer abzuspeichern. Mit einem einzigen Klick und nach wenigen Sekunden nennt man das Gewünschte sein eigen. Und man ist nicht automatisch ein Verbrecher, obwohl es in der öffentlichen Meinung zu „Internet-downloads“ manchmal so scheint. Denn selbstverständlich sind viele der Angebote genau zu diesem Zweck im Internet: Fotos der Sportveranstaltung für die Teilnehmer, Bücher ohne Urheberschutz, Musik von unbekanntem Künstlern oder kostenlose Programme oder Updates, Erweiterungen etc. sollen heruntergeladen werden.

Mit Blick auf die Sicherheit im Internet müssen wir unterscheiden zwischen den Gefahren bei legalen Angeboten (z. B. durch Viren, Kosten etc.) und bei illegalen Angeboten (z. B. Jugendschutz und Urheberrecht).

Legales Angebot – illegales Handeln?

Sie wissen es sicherlich, trotzdem eine kleine Demonstration:

Rufen sie im Internet eine beliebige Seite mit einem Foto auf. Fahren sie mit der Maus drüber und klicken sie die rechte Maustaste. Wählen sie den Befehl „Grafik, speichern unter“ aus. Bestätigen Sie dies mit „Speichern“. Haben sie sich strafbar gemacht? (Habe ich sie zu einer strafbaren Handlung verführt?). Nein, aber ...

Das ist erlaubt

Nun kann ein Bild bspw. durchaus legalerweise im Internet veröffentlicht sein und man ist trotzdem nicht berechtigt, es zu veröffentlichen (z. B. auf meiner privaten Homepage) oder weiterzugeben (auf CD oder USB-Stick oder per Handy bspw.). Grundsätzlich gilt: Für ihren privaten Zweck ist eine solche – legale – Speicherung und Nutzung erlaubt, d. h., ein Bild dürfen sie sich als Hintergrundbild einrichten, es aber nicht weiter verbreiten. Deshalb ist es wichtig, vor einer weitergehenden Nutzung immer die schriftliche Einverständniserklärung des Rechteinhabers zu besitzen. Das geht, wenn sie keine kommerziellen Ziele verfolgen, per E-Mail oft erstaunlich gut.

Urheberrecht

Festgelegt ist dies an mehreren Stellen im Urheberrechtsgesetz (Gesetz über Urheberrecht und verwandte Schutzrechte), so in § 12 und 16 und vor allem im § 53, der die Privatkopie regelt © www.gesetze-im-internet.de (unter „Urhg“, vom 26.10.2007, in Kraft seit 1.1.2008).

Illegale Angebote

Neben den legalen Bildern, Texten, Videos, Liedern usw., die urheberrechtlich geschützt sein können, gibt es – bekanntermaßen – illegale Dinge im Internet, die eigentlich nicht zur Verfügung stehen dürften. Die illegalen Angebote im Internet sind unzählbar und manchmal unfassbar ... Die Spezialisten unter den Surfern berichten, dass es möglich sei, fast jeden Kinofilm, jedes Lied und jede Software (oder zumindest einen Freischaltcode o. ä.) zum Download zu finden. Es liegt in der Natur der Sache, dass sich vor allem die illegalen Angebote der Kontrolle entziehen, wodurch insbesondere der Jugendschutz leicht verletzbar ist; das Urheberrecht ist es meistens schon. Die Problembereiche des Internets lassen sich mit folgenden Überschriften beschreiben:

- Kinderpornografie und Grooming (erst Vertrauen aufbauen und dann ausnutzen)/pädophile Ringe
- Kommerzielle Seiten mit unseriösen Abzockerangeboten (z. B. per Kreditkarte)
- Rassismus/Gewaltverherrlichung/Propaganda
- Pornografie

Gewalt, Pornografie, Snuff-Videos und Propaganda

Ein großes Problem sind Gewalt- und Pornovideos aus dem Netz: Sie werden aus dem Internet heruntergeladen und z. B. per Handy untereinander ausgetauscht. So z. B. Snuff-Videos (v. engl. to snuff out = jemanden auslöschen). Es bezeichnet die filmische Aufzeichnung eines Mordes, wobei angemerkt sein muss, dass noch kein echter Mord nachgewiesen werden konnte, der auch tatsächlich gefilmt wurde. Dies macht die Darstellung aber nicht besser. Pornovideos der härtesten Art bspw. sind im Internet leicht zu finden, die Kriminalstatistik weist vor allem auf Kinderpornografie hin, deren Bilder und Videos über das Internet ausgetauscht werden (berührt ist hier § 184 Abs. 3 und Abs. 5 StGB37).

Auch die rechtsradikale Szene nutzt das Internet zur Verbreitung von Propaganda sowie in letzter Zeit vermehrt auch Terroristen. Extrem gewalthaltige Tasteless-Angebote, wie reale und inszenierte Bilder und Filme von Folter und Misshandlungen sind ein großes Problem und sind bereits gesetzlich verboten. Eine Gefahr stellen aber auch Angebote dar, die versteckt gewalttätige oder ideologische Inhalte, wie rechtsextremes Gedankengut präsentieren. (Genauer im Baustein 5_2, „Jugendgefährdende Inhalte“.)

Jugendliche

Was jedoch unbedingt unterschieden werden muss, ist, ob Jugendliche die Gewalt- und Pornoangebote konsumieren oder ob sie andere verprügeln, um die Gewalt mit dem Handy aufzuzeichnen (Happy Slapping). Beim Konsum sind es vor allem die Faszination und Neugier der problematischen und verbotenen Inhalte, die bereits für Jugendliche im Internet leicht zugänglich sind. Das Anschauen von Gewalt und Pornografie wird als Mutprobe und zum Austesten von Grenzen eingesetzt. Gerade mit dem Handy haben Jugendliche verbotene Inhalte immer dabei, sie können diese Anderen zeigen und verschicken. Das steigert den Status und das Prestige im Freundeskreis: Je härter die Szene, umso härter ist man selber. Noch problematischer wird es, wenn Jugendliche bewusst anderen Gewalt antun und dies mit dem Handy dokumentieren oder sogar weitergeben. Die Motive sind bereits aus der Gewaltforschung bekannt: Besonders Jugendliche, die selbst Gewalt erfahren haben, sind begeistert von Gewaltdarstellungen in den Medien. Durch beispielsweise das Happy Slapping kann über andere Macht und Kontrolle ausgeübt werden. Mittels des Internets oder Handys können diese Aufnahmen sogar öffentlich gemacht und verbreitet werden.

Kinderpornografie

Den wohl schlimmsten Auswuchs erlebt das Internet im Bereich der Kinderpornografie (s. auch Baustein 5_2 „Jugendgefährdende Inhalte“). Dabei ist es international gar nicht einfach, dafür eine Definition zu finden: „Kinderpornografie [ist] als Abbildung definiert, die eine Person zeigt, die ein Kind ist und an einer ausdrücklichen sexuellen Aktivität teilnimmt oder das zumindest so dargestellt wird.“ ist der Versuch für eine Definition (Quelle: © www.inhope.org).

org/de). Die Betroffenen sind dabei sowohl die Kinder, die missbraucht werden als auch die Kinder und Jugendlichen, die damit konfrontiert werden. Und es macht keinen Unterschied, ob die Bilder am Computer erstellt wurden (also kein Kind tatsächlich sexuell missbraucht wurde) oder real sind. Hier ein Artikel zum aktuellen Kampf gegen Kinderpornografie bei Spiegel-Online © www.spiegel.de, (Artikel: „Kinderpornographie – „Wir haben den Kampf verloren“ vom 20.5.2007).

Was tun?

Die Verbreitung von Kinderpornografie steht weltweit unter Strafe. Bei Kinderpornografie macht sich nicht nur der Anbieter strafbar, sondern auch derjenige, der entsprechende Daten besitzt. Sogar derjenige wird bestraft, der versucht, sich derartige Dateien zu verschaffen – egal, ob es sich um deutsche oder ausländische Angebote handelt (Achtung! Nicht auf eigene Faust Detektiv spielen und kinderpornografisches Material sammeln).

Die Organisation „Inhope“ ist die internationale Vereinigung der Internethotlines und wurde 1999 unter dem EU Safer Internet Action Plan gegründet © www.inhope.org/de. Inhope listet für die Teilnehmerländer die Beschwerdestellen auf, bei denen illegale Inhalte gemeldet werden können, für Deutschland sind es folgende:

- eco.de
- jugendschutz.net
- Freiwillige Selbstkontrolle Multimedia (FSM) in Englisch
- Freiwillige Selbstkontrolle Multimedia (FSM) in Deutsch

Schutzmaßnahmen

Die beste Schutzmaßnahme heißt sicherlich „Medienkompetenz“ der Kinder. Darüber hinaus gibt es technische Verfahren, die zwar keinen 100%igen Schutz bieten, aber helfen können.

Tauschbörsen

Nirgendwo anders als im Zusammenhang mit Internet-Tauschbörsen wird das Thema Urheberrecht aktuell so heiß diskutiert. Dabei variieren die Meinungen zwischen zwei Extremen. Zum einen werden die neuesten Entwicklungen als der



7_1 Spam-Mails

7_2 Viren, Würmer, Trojaner, Spyware

7_3 Illegale Downloads und Tauschbörsen

Untergang der Unterhaltungsindustrie gedeutet und zum anderen der Förderung von Kreativität, da die Künstler nicht mehr von der Musik- und Filmindustrie oder Verlagen abhängig sind.

Internet-Tauschbörsen bieten „Filesharing“-Dienste: Die Kontaktaufnahme von Tauschwilligen wird ermöglicht, es können Suchanfragen gestellt und Downloads vorgenommen werden.

Urheberrecht und Tauschbörsen

Grundsätzlich ist die Nutzung von Tauschbörsen im Internet nicht strafbar, wenn es sich bei den angebotenen Dateien um solche handelt, an denen man selbst die Rechte besitzt. Das können z. B. Fotos sein, die man selbst fotografiert hat, selbst komponierte und selbst aufgenommene Musik oder selbst verfasste Texte.

Des Weiteren gibt es Musik-, Film- und Softwaredateien, die eine freie Lizenz besitzen (z. B. die GNU General Public License für Software oder Creative-Commons-Lizenzen für Musik, Texte und Filme, Linux, Open Office etc.).

Der mutmaßlich größte Teil der auf Tauschbörsen (bspw. Kazaa, Emule, etc.) angebotenen Dateien darf jedoch legal nicht zum Download angeboten werden. Da man z. B. mit dem Kauf einer Musik-CD oder DVD keine „Internet-Rechte“ erwirbt, bedeutet dies, dass nur das Abspielen und Kopieren im bzw. für den privaten Bereich erlaubt ist.

(Quelle: © www.kriminalpolizei.de, Artikel: „Möglichkeiten und Grenzen des file sharing“ (2005), Daniel Mannweiler).

Mit dem so genannten „Zweiten Korb“ wurde das Urheberrecht 2008 erneut verschärft. Nun fallen auch alle „unrechtmäßig online zum Download angebotenen Vorlagen“ darunter. Dies bedeutet, dass sich auch jemand strafbar macht, der z. B. Musik herunterlädt und nicht nur derjenige, der sie dort veröffentlicht. Bleibt das ungelöste Problem, woran eine „offensichtlich rechtswidrig hergestellte Vorlage“ zu erkennen ist.

Usenet

Der Vollständigkeit halber sei noch das Usenet erwähnt. Es existiert seit 1979 und ist somit älter als das World Wide Web. In so genannten „Newsgroups“, die thematisch geordnet sind, können die Nutzer digital Texte, aber auch Dateien austauschen. Das Usenet ist immer wieder in Zusammenhang mit Kinderpornografie und Verstößen gegen das Urheberrecht in Verruf geraten, weil es sich dezentral weltweit über Tausende von Servern selbst organisiert und zum Teil nicht öffentlich ist. Es gibt bis heute in Deutschland noch keine einheitliche Rechtssprechung, wie mit bekannt gewordenen illegalen Inhalten im Usenet zu verfahren ist.

Genauerer bei ZDF-Heute:

© www.heute.de, (Artikel: „Wer haftet für illegale Inhalte“, Alfred Krüger vom 31.5.2007). Eine umfangreiche Einführung in das Usenet findet sich von Volker Gringmuth unter © www.einklich.net/usenet/usenet1.htm. Eine Liste deutschsprachiger öffentlicher Newsserver finden sie hier:

© www.cord.de/proj/newsserverliste.

© Links




www.stiftung-warentest.de
(unter „Computer und Telefon“, „Meldungen“)

Artikel „Offensive der Medienkonzerne“ (30.1.2006) bei Stiftung Warentest über den Kampf gegen Tauschbörsen

www.spiegel.de
(unter „Netzwelt“, „Web“, „Musik im Netz“)

Artikel: „Wie die Filmindustrie Tauschbörsen überwacht“, Christian Stöcker vom 28.7.2006

Methodisch-didaktische Hinweise

Arbeitsblatt			
Zeitangabe (Unterrichtsstunden)	2–3	1	2
Ziele	Die Schülerinnen und Schüler werden anhand lebensnaher Beispiele für das Problem der illegalen Downloads und Tauschbörsen sensibilisiert.	Die Schülerinnen und Schüler sollen selbstständig den Urheberrechtsparagrafen 53 recherchieren.	Die Schülerinnen und Schüler sollen sich über die aktuelle Entwicklung und die aktuelle Rechtslage von Tauschbörsen informieren und die verschiedenen Argumente gegenüberstellen.
Methode/n	E-Mail, Checkliste (Tafel)	Merkblatt	Pro/Contra-Tabelle, Rollenspiel
Organisationsform/en	Einzel, Partner, U-Gespräch	Einzel, U-Gespräch	Einzel, U-Gespräch
Zugang Internet	nicht zwingend	ja	ja
Zugang PC	nicht zwingend	ja	ja

7_1 Spam-Mails

7_2 Viren, Würmer, Trojaner, Spyware

7_3 Illegale Downloads und Tauschbörsen

Kommentare zu den Arbeitsblättern



Der zentrale Satz lautet „Sei misstrauisch im Internet!“ Auch wenn die Rechtslage nicht immer eindeutig und für Kinder erst recht nicht zu durchschauen ist, so kann man doch diesen allgemeinen Warnhinweis vermitteln. Es gibt im Internet zahllose gute, kostenlose Angebote, aber wenn etwas angeboten wird, was man sonst teuer bezahlen müsste, dann darf man zu Recht misstrauisch sein. Vielleicht dient der Vergleich mit dem Eis zu Beginn dazu, dieses Bewusstsein zu wecken. Denn auch Kinder werden schon misstrauisch, wenn sie plötzlich etwas geschenkt bekommen (außerdem gilt sicherlich noch vielfach die Regel „Nichts von Fremden annehmen“).

Die richtige Verbindung der Sätze auf dem Arbeitsblatt:

- Das neueste Tokio-Hotel-Lied ganz umsonst per Download könnte Werbung der Musikfirma sein, was aber sehr unwahrscheinlich ist.
- Die Harry-Potter-Postkarten zum Ausdrucken könnten vielleicht wirklich Werbung des Verlages sein. Aber Achtung, es könnte auch ein Abo dahinter stecken.
- Der neueste Kinofilm ist vielleicht auf DVD zu kaufen, aber niemals im Internet kostenlos.
- Teure Software-Programme kosten manchmal Hunderte Euro und sind bestimmt nicht kostenlos.
- Das neueste Computerspiel für den PC gibt es bestimmt nicht umsonst, auch wenn es viele kleine Spiele kostenlos gibt.

Der zweite Arbeitsauftrag erfordert etwas Abstraktionsvermögen oder praktische Beispiele, die für Kinder oft schwer zu finden sind. Wenn man die Sätze und ihre Zuordnungen als Beispiele besprochen hat, so kann man diese einsetzen. Wenn kein Internetzugang besteht, können die Tipps an den Nachbarn auch auf ein normales Papier geschrieben werden.



Der Einstieg soll eine typische Situation skizzieren und zum Problem der illegalen Downloads hinführen. Die Schülerinnen und Schüler sollen selbständig den Urheberrechtsparagrafen 53 recherchieren, wobei

sie bei den juristischen Formulierungen vielleicht Hilfe benötigen. Mit den Kommentaren zu den Zitaten sollen sie das Gelernte anwenden und die Diskussion unter den Freunden juristisch richtig stellen. Klar ist, dass es nicht erlaubt ist, aus offensichtlich illegalen Quellen etwas herunter zu laden. Auch Rechtsschutzversicherungen treten dabei nicht unbedingt in die Haftung, weil das Strafrecht berührt ist. Die Punkte „Interessiert doch eh keinen“ und „Da kann nichts passieren“ entsprechen manchmal der behördlichen Realität durch die fehlende Ahndung der Strafverfolgungsbehörden, weil die Taten bei diesen vermeintlichen Bagatelldelikten von der Staatsanwaltschaft eingestellt oder gegen Sozialstunden für die Jugendlichen gehandelt werden. Darauf verlassen sollte man sich nicht, vor allem wenn die mächtige Musik- oder Videoindustrie mobil macht. Den größten Eindruck macht auf Jugendliche oft die Aussage von Polizisten, dass bei Tatverdacht das Tatwerkzeug, sprich der Computer, eingezogen werden kann.



Gerade die Tauschbörsen erleben seit Jahren ein Auf und Ab und eine ständige Wandlung. Im Jahre 2004 ist erstmals ein Nutzer einer Tauschbörse in Deutschland verurteilt worden, was die Szene zuvor für nicht möglich hielt. Mit der Änderung des Gesetzes müssen die Provider ab 1.1.2008 die Zugangsdaten für sechs Monate speichern, d. h., für sechs Monate kann nachvollzogen werden, von welchem Internetzugang aus etwas Illegales herunter geladen wurde. Das Rollenspiel im Anschluss soll der Tatsache gerecht werden, dass viele Jugendliche zwar die Rechtslage kennen, aber wenig Unrechtsbewusstsein (glücklicherweise nur in der digitalen Welt) haben.

Möglichkeiten zur Weiterarbeit „Lust auf mehr“

Gerade bei diesem Thema bietet sich ein Rückgriff vom Digitalen in das Reale geradezu an. Denn die Rechtslage ist eigentlich nicht anders, nur die Möglichkeiten einen Diebstahl oder Betrug zu begehen und die Chancen, dabei erwischt zu werden. Spannende Diskussionen und Unterrichtsgespräche ergeben sich bei dem Thema, ob man etwas Unrechtes tut, wenn man nicht erwischt werden kann.



Arbeitsblatt vom

Name:

Umsonst im Internet – bist du misstrauisch

Was würdest du sagen, wenn jemand vor dem Schulhof steht und Eis verteilt, ohne dass du dafür bezahlen musst. Würde dir das seltsam vorkommen? Obwohl ... so ein leckeres Eis ... ganz umsonst ...

Manchmal ist es nicht einfach, Gut von Böse zu unterscheiden, deshalb gibt es nur einen Tipp:

Sei misstrauisch im Internet!

Hier kannst du es ein wenig üben.

! So passiert es manchmal im Internet: Fremde Menschen bieten teure Spiele, Musik, Videos oder Programme an, ohne dass du dafür bezahlen musst. Das ist natürlich nicht erlaubt! Außerdem gibt es sogenannte „Tauschbörsen“ im Internet. Sie funktionieren, wie der Name es schon vermuten lässt: Du erhältst etwas im Tausch gegen etwas anderes. Getauscht werden Fotos, Musik, Filme oder Programme ... auch das ist meistens nicht erlaubt, denn fremde Sachen darf man – meistens – nicht kopieren und dann weitergeben.

1. Arbeitsauftrag:

Verbinde die Kästchen durch Striche! Du kannst auch die gleichen Zahlen in die Kreise schreiben!

Das neueste Tokio-Hotel-Lied ganz umsonst per Download

Die Harry-Potter-Postkarten zum Ausdrucken

Der neueste Kinofilm

Teure Software-Programme

Das neueste Computerspiel für den PC

ist vielleicht auf DVD zu kaufen, aber niemals im Internet kostenlos.

könnte Werbung der Musikfirma sein, was aber sehr unwahrscheinlich ist.

gibt es bestimmt nicht umsonst, auch wenn es viele kleine Spiele kostenlos gibt.

könnten vielleicht wirklich Werbung des Verlages sein. Aber Achtung, es könnte auch ein Abo dahinter stecken.

kosten manchmal Hunderte Euro und sind bestimmt nicht kostenlos.

2. Arbeitsauftrag:

Schreibe eine Nachricht als E-Mail an deine Sitznachbarin/deinen Sitznachbarn in der du ihr/ihm erklärst, warum du im Internet bei den verschiedenen Download-Möglichkeiten misstrauisch sein solltest. Du kannst die Mail auch auf ein Blatt schreiben und sie deiner Nachbarin/deinem Nachbarn geben!

3. Arbeitsauftrag:

Lest euch eure E-Mails gegenseitig vor und fasst die wichtigsten Punkte in einer gemeinsamen Liste zusammen.



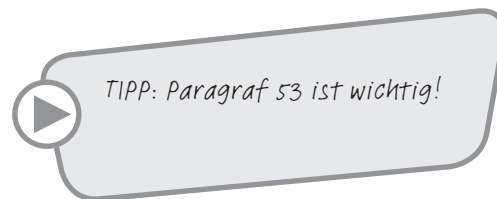
Arbeitsblatt vom

Name:

Legal – Illegal?

Theo ist begeistert: „Wenn ich es euch doch sage: die neuesten Spiele. Alle! Auf Mausclick! Kostenlos!“. Seine Freunde auf dem Schulhof gucken skeptisch. „Aber“, wendet Moritz ein, „das ist doch nicht erlaubt, oder?“ „Ach was“, sagt Theo, „interessiert doch eh keinen und mein Vater hat eine Rechtsschutzversicherung“. „Da lasse ich die Finger von“, sagt Mike, „ich gehe nur noch über die Tauschbörsen. Da kann nichts passieren und ich kriege auch alles, was ich will“.

Stimmt das, was Theo und Mike behaupten? Oder hat Moritz recht?



1. Arbeitsauftrag:

Schau im Gesetz nach, achte unbedingt auf die aktuelle Fassung!

2. Arbeitsauftrag:


Außerdem sind Tauschbörsen in dem neuen Gesetz auch eindeutig geregelt. Recherchiere auch diesen Punkt.

3. Arbeitsauftrag:

Kommentiere die Zitate in der Tabelle, nachdem du alles Nötige zum Urheberrechtsgesetz recherchiert hast:

wer?	Zitat	Kommentar
Theo	Die neuesten Spiele. Alle! Auf Mausclick! Kostenlos!	
Moritz	Das ist doch nicht erlaubt, oder?	
Theo	Interessiert doch eh keinen.	
Theo	Mein Vater hat eine Rechts- schutzversicherung.	
Mike	Ich gehe nur noch über die Tauschbörsen.	
Mike	Da kann nichts passieren.	

4. Arbeitsauftrag:

Informiere dich bei  www.ights.info darüber, was erlaubt ist und was nicht. Erstelle schriftlich eine Übersicht für Theo und Mike (also für deine Klassenkameraden)!



