

Themenmodule zur Verbraucherbildung

Internet – aber sicher!

Unterrichtseinheit von Thomas Erkert

Kurzinformationen

Themenbereich	Internet
Titel	Internet – aber sicher!
Autor	Thomas Erkert
Stand	Dez. 2006/Jan. 2007 (alle Internetverweise wurden am 2. und 3. Januar 2007 überprüft)
Fächer:	Informatik, Projekttag,
Zielgruppe:	Sekundärstufe II (17 bis 19 Jahre) Erwachsene Verbraucher
Zeitaufwand:	4 bis 6 Unterrichtsstunden
Vorbereitungsinformation für Lehrende:	Siehe separate Literatur- und Linkliste
Medien:	Computer mit Internetanschluss / Beamer, Bewertungspunkte, Kartei- und Moderationskarten, dicke Stifte, Flipchart
Technische Ausstattung:	4-5 Computer mit Internetzugang Mindestausstattung: 1 PC mit Internetzugang, Beamer
Copyright beim Verbraucherzentrale Bundesverband e.V. (vzbv), erstellt im Auftrag des vzbv.	

Inhaltsverzeichnis

Lernziele	2
Kurzbeschreibung	2
Benötigte Materialien.....	2
Lesehinweis.....	2
Sachanalyse	3
Einführung.....	3
Das Internet nutzen und dabei trotzdem anonym bleiben.....	6
Schlussbemerkung.....	7
Möglicher Unterrichtsverlauf	9
Weiterführende Literaturhinweise	11
Weiterführende Internetseiten	12
Glossare	13
Modul 1: Kenntnisstand der Schüler testen	14
Modul 2: Gruppenarbeit: Welche Gefährdungen kennen Sie?	23
Modul 3: Checkliste Eigenes Verhalten	25
Modul 4: Sicheres Passwort	27
Modul 5: Das Internet nutzen und dabei anonym bleiben	30

Lernziele

Ziel dieser Unterrichtseinheit ist es, Schüler der Sekundarstufe 2 aber auch Erwachsene über aktuelle Gefährdungen des Internets und anderer interaktiver Medien zu informieren und dabei deren Bewusstsein für mögliche Abwehrmöglichkeiten zu schärfen. In dieser aus mehreren Modulen bestehenden Unterrichtseinheit sollen die Schüler in die Lage versetzt werden, die aktuellen Gefahren nicht nur zu erkennen, sondern auch risikoreiches (Online-) Verhalten zu minimieren.

Kurzbeschreibung

Diese Unterrichtseinheit wurde für geübte(re) Internetnutzer konzipiert – nicht für Internet-Anfänger. Grundbegriffe einerseits und Grundfertigkeiten am Rechner andererseits werden vorausgesetzt.

Methodisch soll versucht werden, den Kenntnisstand der Schüler über ein Quiz zu bewerten, um dann die Experten unter ihnen aktiv in den Unterricht mit einzubeziehen. Es geht darum, das verborgene Detail- bzw. Expertenwissen der Jugendlichen zu nutzen, um weniger geübten Mitschülern sicheres Verhalten im Internet zu vermitteln. Dabei sollen zwei Ziele erreicht werden: zum einen soll dabei der Unterrichtende in die Lage versetzt werden, besser oder überhaupt zu verstehen, was gerade aktuell, „in und cool“ ist, zum anderen sollen die weniger geübten Mitschüler von den Schülerexperten und deren Umgang mit dem Internet aber auch mit anderen Medien profitieren. Diese Experten werden gebraucht, um den Mitschülern in den Kleingruppen anhand von Beispielen konkret zu zeigen, wie etwas funktioniert.

Benötigte Materialien

Für diese Unterrichtseinheit benötigt man mindestens einen Rechner mit Internetanschluss und einen Beamer zur Projektion der Seiten für die Lerngruppe. Im Optimalfall verfügt die Gruppe über mehrere Rechner mit Internetanschluss. 3-6 Schüler sollten sich dabei einen Rechner teilen. Darüber hinaus werden folgende Materialien für die Gruppenarbeiten benötigt: Flipchart und Papier, Farbstifte, Bewertungspunkte, Kartei- und Moderationskarten.

Umsetzung

Die Unterrichtseinheit wurde in mehrere aufeinander abgestimmte Module eingeteilt. Das erste Modul, ein einführendes Quiz, dient dem Erfassen des Kenntnisstandes der Schüler. Die anderen Module haben jeweils einen thematischen und methodischen Schwerpunkt. Sie bauen aufeinander auf und sind dadurch didaktisch geschlossen.

Lesehinweis

Weiterführende Informationen und Hintergrundinformationen sind als „Tipp“ gekennzeichnet und mit einem Rahmen umrandet.

Alle Internetverweise sind zuletzt am 2. und 3. Januar 2007 überprüft worden.

Sachanalyse

Einführung

Das Internet ist endgültig zum Netz der Netze geworden. Mehr als 40 Mio. Anwender, nahezu jeder 2. Bewohner der Bundesrepublik, nutzt das Netz für private oder berufliche Zwecke. Egal wie intensiv jemand das weltweite Netz nutzt, er muss sich heute mit dem Thema „Sicher im Netz bewegen“ beschäftigen. Warum ist das so?

In den letzten Jahren gab es wohl kaum mehr einen Rechner, der nicht einem „schädlichen Angriff“ ausgesetzt war oder ist. Am drastischsten verdeutlicht dies vielleicht eine Studie des Internet Storm Centers (ISC) aus dem Sommer 2004 (<http://www.sans.org>). Demnach dauert es durchschnittlich nur 20 Minuten, bis ein ungeschützter Windows-Computer im Internet schädlichen Programmen (so genannter Malware) zum Opfer fällt. Es ist also keine abstrakte Gefahr, vor der man sich, seine Daten und seinen PC schützen muss, sondern eine höchst reale.

Zu den häufigsten und bekanntesten Gefahren im Internet zählen derzeit:

- Datenspionage durch trojanische Pferde und damit verbunden offene Ports (vgl. z.B.: http://www.br-online.de/bayern3/pc_co/news/artikel/pluspunkt-online/2007/01/15-gez-trojaner/index.xml)
- Virus- bzw. Wurm-Befall/Missbrauch des eigenen PCs durch Eingriffe von außen
- Missbrauch von persönlichen Daten (und/oder Kreditkartennummern)
- Identitätsdiebstahl durch Spyware-Programme oder durch Pishing-Attacken
- Datenmissbrauch für unerwünschte Werbung (Spam-Mail)
- Technische Manipulationen am PC durch Eingriffe von außen
- Vermögensschäden bei Online-Geschäften (betrügerische Auktionen, fragwürdige Abonnements auch beim Handy) (vgl. z.B. http://www.br-online.de/bayern3/pc_co/news/artikel/pluspunkt-online/2007/01/09-fuehrerscheintest/index.xml)
- Unerwünschte Kontaktaufnahme in Chatrooms, Foren oder per Email.

Tipp: Unter <http://isc.sans.org/> kann tagesaktuell ein Gefahrenreport des Internet Storm Centres heruntergeladen werden. Dort wird anhand einer Farbskala die aktuelle Gefährdung durch Viren, Würmer und Trojaner gezeigt.

Neben den nur ärgerlichen, zumeist ungefährlichen „SPAM–Mails“, also Werbemails, sind im Jahre 2006 mehr und mehr so genannte „Pishing-Mails“ aufgetaucht. Pishing ist ein Kunstwort, das sich aus den beiden englischen Wörtern „password“ und „fishing“ zusammensetzt. Bei diesen Pishing-Mails versucht der Absender möglichst viele Kennwörter und andere sensible Informationen, wie z.B. PINs und TANs zu „fischen“, indem er einen „Köder“ in Form einer mehr oder weniger gut gemachten, offiziell ausschauenden Mail auswirft. Bei solchen Attacken ist schon eindeutig von einem betrügerischen Hintergrund auszugehen.

Einhergehend mit dem Anstieg der Internetnutzer ist in den vergangenen fünf Jahren leider auch die Zahl der Straftaten im Internet drastisch angestiegen. Allein im Jahr 2005 wurden laut polizeilicher Kriminalstatistik (PKS) in Deutschland 62.168 Fälle des Computerbetruges registriert. Darunter fiel zwar eine erhebliche Zahl an Betrugsfällen mit Kreditkarten, aber mit 15.875 registrierten Fällen eben auch eine große Anzahl von Straftaten, die nur im Internet begangen wurden - wobei viele gar nicht erst erfasst wurden. „Die Dunkelziffer liegt um ein Vielfaches höher als die in der PKS ausgewiesenen Zahlen“, stellte das Bundeskriminalamt so auch fest. Denn viele Taten werden von den Betroffenen gar nicht erst zur Anzeige

gebracht – entweder weil sie nicht bemerken, dass sie Opfer geworden sind oder weil sie für den Gang zur Polizei mit seinen Formalitäten zu bequem sind oder einfach, weil sie sich schämen oder sich nicht als unerfahrene Laien „outen“ wollen. Wie häufig Kinder und Jugendliche Opfer von diversen Angriffen aus dem Netz sind, taucht in den offiziellen Statistiken leider nicht auf. Betrachtet man aber die Nutzungszeiten, die Vielfalt der Angebote und das spielerische Interesse der Kinder und Jugendlichen, dann ist zu vermuten, dass ein Großteil, vor allem der nicht registrierten Vorfälle, Kinder und Jugendliche betraf (vgl. <http://www.bka.de>).

Tipp: Unter <http://www.bka.de/pks/pks2005/index2.html> kann die offizielle Kriminalitätsstatistik des Bundeskriminalamts eingesehen werden.

Eltern denken bei den Gefahren in erster Linie an ungeeignete Inhalte im Internet: Gewaltvideos, pornographische oder rassistische Inhalte tauchen immer wieder und in immer unvorstellbarerem Ausmaß im Internet, aber auch auf Handys, auf. Über besonders scheußliche Beispiele wird dann auch in den Medien berichtet. So z. B. im Sommer 2006 als Gewaltvideos auf Handys von Jugendlichen zum viel beachteten Thema wurden. Diese wanderten auf den Schulhöfen von Handy zu Handy und verbreiteten sich so rasend schnell. Zusätzliche Informationen zu diesen Gewaltvideos können unter http://www.polizei-beratung.de/mediathek/merkblaetter/index/content_socket/merkblaetter/display/160/ per Download abgerufen werden. Dort wird unter anderem auch beschrieben, wie diese Videos sich so schnell ausbreiten konnten. Ein Problem ist, dass sich Eltern oder Betreuungspersonen oft gar nicht darüber im Klaren sind, womit sich Kinder und Jugendliche konkret beschäftigen. Ein weiteres Hauptproblem ist, dass viele Eltern kaum in der Lage sind, die Medien Ihrer Kinder vor allem auch wenn diese das Jugendalter erreichen, zu überwachen und zu kontrollieren. Technische Maßnahmen können vom viel geübteren Nachwuchs schließlich oft einfach außer Kraft gesetzt werden, oft übrigens so, dass die Eltern überhaupt nichts davon merken.

Tipp: Das Thema ist auch für interessierte Eltern von großer Bedeutung. Im Rahmen eines Elternabends oder von Projekttagen könnte diese Thematik unter dem Motto „Internet – aber sicher“ angeboten werden. Dieser Elternabend könnte zum Beispiel in Zusammenarbeit mit den Schülerexperten vorbereitet werden.

Die beste Möglichkeit, sich vor den Gefahren zu schützen, ist ständig an seiner eigenen Medienkompetenz zu arbeiten. Medienkompetenz ist die Schlüsselkomponente, um einen sicheren und verantwortungsbewussten Umgang mit den neuen Medien zu ermöglichen. Das gilt auch für die Mobiltelefone und andere moderne Kommunikationsinstrumente wie Smart Phones, Organizers, MP3-Player, GPS-Empfänger, mobile Navigationsgeräte. Für alle diese Geräte gibt es übrigens bereits Schädlinge (vgl. z. B. <http://www.heise.de/security/news/meldung/84411/from/rss09>).

Tabelle 1: Gefährdungen durch PC, Handy und andere Medien

		Medium					
		PC				Handy	TV
		online					
		Internet	E-Mail	Chat	Messenger	PC-Spiel	
	Gefährdung durch ungeeignete Inhalte, z.B.:						
1	Gewaltverherrlichung	x				x	x x
2	Pornographie	x				x	x x
3	(Rechts-)extremistische Darstellungen	x				x	x
4	(Kostenpflichtige) Glücksspiele	x					x
5	Illegale Tauschbörsen	x					
6	verbaler Missbrauch, z.B. durch:						
7	Kontaktaufnahme Pädophiler		x	x	x		
8	Kontaktaufnahme anderer Krimineller		x	x	x		
9	Herunterladen kostenpflichtiger Angebote	x					x
10	Viren, Würmer, Trojaner	x			x		x
11	Pishing (Ausspionieren)		x				

Neben den Internetschädlingen und den damit verbundenen Gefahren soll vor allem auch auf die Gefährdungen hingewiesen werden, die durch das Surfen im Internet mehr oder weniger gewollt abgerufen werden können und deren Inhalte zum Teil nicht jugendfrei sind. Internetseiten mit Gewalt verherrlichendem, pornographischem oder (rechts-)extremistischem Inhalt sind allgegenwärtig im Netz der Netze.

Ziel dieser Unterrichtseinheit ist es, herauszufinden, wie man sich gegen diese Gefahren schützen kann. Schon jetzt sei betont: der beste Schutz ist Wissen! Medienkompetenz ist der Schlüssel zu einem sicheren Umgang mit dem Internet und anderen Medien. Jeder Nutzer kann sich mit einfachen Schritten gegen Schädlinge oder andere Gefährdungen schützen. Neben den technischen Hilfsmitteln ist vor allem das persönliche Nutzungsverhalten ausschlaggebend für einen gefahrlosen Umgang mit den neuen Medien im Allgemeinen und mit dem Internet im Besonderen. Nach dieser Unterrichtseinheit sollen die Schüler in der Lage sein, nicht nur die Gefahren zu erkennen – sondern sich auch so zu verhalten, dass Sie sich gefahrlos im Internet bewegen können: Internet – aber sicher!

Bei der Risikominimierung wird auf zwei komplett unterschiedliche Bereiche eingegangen: zum einen auf die technischen Hilfsmittel wie Antivirenprogramme, Antispam-Programme und andere, zum anderen auf das eigene Verhalten. Es gilt zu erarbeiten, dass ein Großteil der Gefährdungen auf fahrlässiges Verhalten der Anwender zurückzuführen ist. Andererseits gilt es herauszuarbeiten, dass derjenige, der bestimmte Verhaltensregeln beachtet, das Gefährdungsrisiko erheblich minimieren, wenn nicht sogar ausschalten kann.

Im Folgenden werden 10 Regeln aufgestellt, die von den Schülern unbedingt befolgt werden sollten. Das Risiko durch Internetschädlinge oder durch eigenes Fehlverhalten betroffen zu werden, wird bei Einhaltung dieser Regeln erheblich minimiert (vgl. <http://www.bsi-fuer-buerger.de> und Knowware Broschüre: „Sicherheit im Internet“).

1. Setzen Sie eine Firewall und Virenschutzsoftware ein und bringen Sie diese ständig auf den aktuellen Stand. Führen Sie Updates sofort aus.
2. Führen Sie regelmäßig Softwareaktualisierungen, vor allem auch für Ihr Betriebssystem durch!
3. Arbeiten Sie am Computer nicht mit Administratorenrechten. Richten Sie sich ein Benutzerkonto mit eingeschränkten Rechten ein. So schränken Sie auch die Möglichkeiten für Computerhacker ein.
4. Stellen Sie sicher, dass die Funktionen „Aktive Inhalte (ActiveX)“ und „Java Script (Java Applets)“ deaktiviert sind.
5. Seien Sie immer besonders vorsichtig, wenn Sie über Eingabemasken dazu aufgefordert werden, „JA“ oder „OK“ einzugeben. Vergewissern Sie sich, welche und zu welchen Konditionen Ihnen Inhalte angeboten werden.
6. Seien Sie sehr vorsichtig bei Mails mit Anhängen. Öffnen Sie Anhänge nur von Mails, bei denen Sie sich absolut sicher sind, dass Sie dem Sender vertrauen können.
7. Back-ups von Ihren wichtigsten Daten sollten Sie automatisiert und regelmäßig anfertigen. Anders als vor noch wenigen Jahren kostet Speicherplatz heute eigentlich fast nichts mehr. Als Medien bieten sich externe zusätzliche Festplatten, ZIP-Drives, CD/DVD oder auch kostenloser „Online-space“ an. Prüfen Sie Ihre Back-ups bevor Sie diese archivieren. Sonst kann es passieren, dass man - im Glauben ein Back-up zu haben – feststellen muss, dass man dieses nicht zurückspielen kann.
8. Erhalten Sie Daten von Freunden und Bekannten über Memorystick, CD/DVD, stellen Sie zunächst sicher, dass es sich um virenfreie Daten oder Programme handelt. Gewöhnen Sie sich an, automatisch einen Virenskan vorzunehmen.
9. Wenn Sie aus dem Internet Software herunterladen, stellen Sie möglichst sicher, dass die Quellen nicht verseucht sind. Nutzen Sie keine illegale Software. Allzu oft handelt es sich dabei nur um die perfekten Brutstätten für Viren, Trojaner und Würmer.
10. Gehen Sie sorgfältig mit Ihren Zugangsdaten um: Halten Sie Kennwörter und Benutzernamen sowie Zugangscodes für Dienste (z. B. beim Online-Banking) unter Verschluss.

Das Internet nutzen und dabei trotzdem anonym bleiben

Viele Angriffe im Internet haben das Ziel, den Anwender auszuspionieren. Mit den gewonnenen Informationen kann auf unterschiedliche Art und Weise umgegangen werden: entweder um Sie gezielter zu bewerben, um ihre E-Mail-Adresse zum Versenden von Spam-Mails zu missbrauchen oder um – im Extremfall – Ihr Konto für verschiedene finanzielle Transaktionen zu nutzen.

Tipp: vgl. <http://www2.oncomputer.t-online.de/dyn/c/10/26/55/74/10265574,si=0.html>

Unter dem Link „sechs Fakten zur Cyberkriminalität“ gibt es verschiedene Beispiele für kriminelle Machenschaften im Internet, u.a. über die „Die Jagd nach Geld“. So geht es Viren-Autoren heute nicht mehr um die Herausforderung, einen Schutz zu umgehen oder sich irgendwo einzuloggen. Betrüger sind heutzutage nur noch auf das schnelle Geld aus, das sie mit per Trojaner abgefangenen Daten verdienen. Im ersten Halbjahr 2006 wurden viermal so viele Trojaner ins Netz gebracht als Viren. Ein weiterer Trend: Die Cyberkriminellen verschlüsseln Daten auf den eroberten Rechnern und geben diese nur nach einer Lösegeldzahlung wieder frei.

Kaum einer wird wohl ein solches Risiko eingehen wollen. Was kann also getan werden? Am nahe liegendsten wäre doch – was eigentlich eine Selbstverständlichkeit sein sollte – sich anonym im Internet bewegen zu können. Zu Zeiten der „Cookies“, der „ActiveX“ und anderer interaktiven Elemente ist dies allerdings im Regelfall nur noch schwer möglich.

Tipp: Unter <http://www.anonym-surfen.com/anonym-surfen/test> können Sie dazu jederzeit einen Test machen. Sie werden erstaunt sein, was Sie auf dieser Seite alles über sich erfahren können. Auf <http://www.anonym-surfen.com> finden Sie darüber hinaus detaillierte Informationen zu diesem Teilaspekt.

Wie kann man nun verhindern zum „gläsernen Surfer“ zu werden? Wer nicht möchte, dass große Werbefirmen legal die Internetnutzung erfassen, der sollte sich Gedanken über Gegenmaßnahmen machen. Was kann man konkret tun? Das Hauptaugenmerk gilt es darauf zu legen, das eigene (PC-)System „sauber“ zu halten. Dazu gehört das Löschen von Cookies, des Cache, der History und vieles mehr. Dadurch, dass sämtliche Hinweise vernichtet und der PC vom Provider in aller Regel dynamische IP-Adressen zugewiesen bekommt, ist es keinem Webseitenbetreiber möglich, den jeweiligen PC und dadurch den Anwender später wieder zu erkennen. Somit ist jede Internetsitzung in sich abgeschlossen und es entstehen keine Querverweise. Diese Spuren gilt es nach jeder Internetsitzung zu entfernen, indem der Rechner gesäubert wird. Sowohl im Internetexplorer als auch in den anderen Browsern gibt es die Möglichkeiten, mehr oder weniger komfortabel, alle relevanten Informationen beim Verlassen des Browsers einfach los zu werden.

Tipp: Es gibt auch Tools, die dieses Verwischen der Spuren vereinfachen bzw. bequemer machen. Ein Tool, das Ihnen sehr viel Arbeit erspart, ist z.B. Winsweep (<http://www.shareit.com/product.html?cart=1&productid=188112&languageid=2&backlink=http%3A%2F%2Fwww.anonym-surfen.com%2Fsoftware%2F&nolselection=1&affiliateid=73286>).

Dieses von vielen Fachmagazinen ausgezeichnete Programm ist so was wie ein komplettes Internet-Verschleierungs- bzw. Sicherheitspaket. Anonym und sicher surfen, Surfspuren vernichten, anonyme E-Mails und Dateiverschlüsselung sind nur einige Bestandteile des Programms. Eine „Surfspuren-Reinigung“ beim Systemstart oder beim Beenden der Internetsitzung kann damit eingerichtet werden. Darüber hinaus blockieren dieses oder ähnliche Programme einen Großteil der bekannten Reklame- und Spywareserver. Diese Surfspuren-Vernichter löschen Verlaufslisten, Protokolle, Cookies und den Internet-Cache bequem und automatisch.

Schlussbemerkung

Sicher und anonym im Internet surfen, ist durchaus möglich. Wenn die in dieser Unterrichtseinheit behandelten Maßnahmen beherzigt werden, dann ist das „Netz der Netze“ (relativ) gefahrlos zu benutzen. Mit wenig technischem Aufwand kann das System (fast) sicher gemacht werden. Die technischen Hilfsmittel wie Antivirenprogramm, Firewall, Antispyware, etc. bieten einen guten Schutz. Es ist erstaunlich wie schnell die Anbieter dieser Programme auf Gefährdungen reagieren können.

Tipp: Kommerzielle Anbieter von Antiviren-Programmen finden Sie unter:
<http://www.kaspersky.com/af/globalstore?AID=1110836&PID=778434>
http://www.f-secure.com/home_user/ (mit Virusweltkarte und Bedrohungseinschätzung)
<http://www.symantec.com/index.htm>
<http://www.mcafee.com/de/>
Kostenfreie Angebote finden Sie unter anderem unter: <http://www.free-av.de/>

Wie in anderen Bereichen auch scheint der Faktor Mensch allerdings die größere Schwachstelle zu sein: nicht installierte Schutzprogramme, nicht oder zu spät durchgeführte Aktualisierungen oder vergessene Säuberungen des Systems sind häufig der Grund für einen Virenbefall oder den „gläsernen“ Surfer, dessen Rechner regelmäßig ausspioniert wird. Zu noch dramatischeren Auswirkungen kann jedoch ein falsches Verhalten der Nutzer

führen. Gegen immer ausgefeiltere Tricks von Betrügern hilft nur eine immer größere Medienkompetenz. Es ist von großer Bedeutung, immer sensibler gegenüber potentiellen Gefahren zu werden. Es gilt ein Gefühl für kritische Bereiche zu erlangen, so wie das beispielsweise viele Reisende haben. Genauso wenig wie ein kritischer Reisender in problematischen Stadtbezirken spazieren gehen würde, würde der versierte Internetnutzer sich in Bereiche vorwagen, die ihm gefährlich werden könnten. Er würde z.B. keinesfalls seine persönliche Daten unbedarft an Fremde weitergeben oder unüberlegt auf dubiose Kontakte reagieren.

Zum Schluss soll noch einmal auf Gefahren bei anderen Medien hingewiesen werden, die in dieser Unterrichtseinheit und dem dazugehörigen Fachbeitrag nur ansatzweise behandelt werden konnten. In Zukunft werden alle interaktiven neuen Medien verstärkt gefährdet sein. Mobiltelefone, Organizer, Internettelefone, GPS-Empfänger, Navigationsgeräte etc. werden mehr und mehr zu Spielfeldern diverser Hacker und Betrüger. Würmer und Trojaner haben sich mittlerweile auch in diesen Geräten längst eingenistet (vgl. <http://www.heise.de/security/news/meldung/84411/from/rss09> oder <http://www.viruslist.com/de/news?id=200185271>).

Möglicher Unterrichtsverlauf

Für diese Unterrichtseinheit sollten insgesamt etwa fünf bis sieben Schulstunden eingeplant werden. Es ist wichtig, genügend Raum für praktische Beispiele und Übungen zu lassen. Generell wird die Großgruppe in Kleingruppen unterteilt; nach Möglichkeit sollten diese Kleingruppen nicht größer als 5 Schüler + 1 Schülerexperte sein. Die Kleingruppen sollten sich im Idealfall jeweils um einen internetfähigen Rechner gruppieren. Für die Gruppenarbeiten sollten darüber hinaus jeweils Tische mit Flipchartpapier, Stifte, Karteikarten und Bewertungspunkte bereitliegen.

Die Unterrichtseinheit wurde in fünf aufeinander abgestimmte Module unterteilt. Das erste Modul, ein einführendes Quiz, dient dem Erfassen des Kenntnisstandes der Schüler. Die anderen Module haben jeweils einen thematischen und methodischen Schwerpunkt. Sie bauen aufeinander auf und sind dadurch didaktisch geschlossen.

Im zweiten Modul werden in Gruppenarbeiten Internetschädlinge und andere Schadprogramme erarbeitet. Das dritte Modul hat das Erarbeiten einer Checkliste zum Inhalt. Wer sich an diese Checkliste hält, dürfte sich mit hoher Wahrscheinlichkeit sicher im Internet bewegen. Ein großes Sicherheitsproblem stellen unbedacht gewählte Passwörter dar. Deshalb wird das vierte Modul dieser Thematik gewidmet. Ziel ist es dabei, sichere Passwörter zu entwickeln und diese auch sicher zu verwahren. Im abschließenden Modul 5 werden explizit Möglichkeiten erarbeitet, wie man sich im Internet anonym bewegen kann. Praktische Tests, die auch am eigenen Rechner zu Hause durchgeführt werden können, dienen dabei als Erfolgskontrolle. Allen Modulen gemein ist die enge Verknüpfung zwischen theoretisch zu erarbeitenden Inhalten mit der Präsentation der konkreten Handlungsanweisungen. Zeigen Sie konkret in den einzelnen Modulen, wie etwas gemacht wird. Nutzen Sie dazu entweder den Lehrerrechner mit Beamer oder lassen Sie die einzelnen Schritte durch die Schülerexperten in den Kleingruppen durchführen. Zeigen Sie konkret wie man z.B. Cookies in den verschiedenen Browsern löscht oder den Pufferspeicher (Cache) leert.

Folgender Zeitbedarf sollte für die einzelnen Module kalkuliert werden:

Modul	Thema	minimal	maximal
1	Einführung, Kenntnisstand der Schüler testen, Quiz	45	60
2	Gefährdungen	45	60
3	Checkliste Eigenes Verhalten	60	90
4	Sicheres Passwort	30	45
5	Anonym im Internet	45	60
alle	Summe	3h 45min	6h15min

Abschließend soll noch einmal darauf hingewiesen werden, dass das Einbeziehen der Schülerexperten, von entscheidender Bedeutung für diese Unterrichtseinheit ist. Die Selektion über das Quiz (Fragebogen) ist nur eine Möglichkeit, die Internetkenner zu selektieren – und birgt unter Umständen das Risiko, dass zwar theoretisch viel bekannt ist, dass aber die praktische Umsetzung zu wünschen übrig lässt. Dies sollten Sie vorab klären. Andere Auswahlformen bzw. zusätzlich zu berücksichtigende Aspekte liegen natürlich im Verantwortungsbereich des Lehrenden. Die Rolle der Schülerexperten ist vielfältig: sie sind für Sie nicht nur Multiplikatoren sondern vor allem auch Informationsquelle. Über sie erfahren Sie auch, was gerade up-to-date ist. Umgekehrt sind diese Schülerexperten Ihre Assistenten in der Vermittlung der Unterrichtseinheit und vor allem für die praktischen Übungen.

Tipp: Es ist durchaus auch sinnvoll, die Auswahl „Ihrer“ Internet-Experten“ vom Quiz zu trennen und diese in Ruhe vorzunehmen. Überlegen Sie sich, ob es nicht vorteilhaft wäre, diese Schülerexperten verstärkt auch schon in der Vor- und Nachbereitung der Unterrichtseinheiten, beispielsweise im Rahmen von Projekttagen, mit einzubeziehen. Diese Experten könnten später auch als Problemanlaufstelle fungieren und so dazu beitragen, die allgemeine Medienkompetenz nachhaltig zu verbessern.

Weiterführende Literaturhinweise

- Computerkriminalität, Nordrhein-westfälisches Landeskriminalamt (LKA) & Initiative "secure-it.nrw. (Hrg.) August 2006
- Janssen, Ludwig: Internet – Sicherheit. Reihe Themenblätter im Unterricht, Band 33. Bundeszentrale für Politische Bildung, 2004. Das Themenblatt erläutert die wichtigsten Sicherheitsrisiken im Internet und stellt ein entsprechendes Sicherheitskonzept vor. Es kann unter <http://www.bpb.de> kostenfrei per Download bezogen werden.
- „Klicks-Momente – So unterstützen Sie Ihr Kind bei der Medienkompetenz“ ist eine Publikation der Polizei. Diese Broschüre kann kostenlos bei jeder (Kriminal-) Polizeilichen Beratungsstelle abgeholt werden. Außerdem kann diese auch kostenfrei aus dem Internet geladen (download) werden – unter: <http://www.polizei-beratung.de/mediathek/kommunikationsmittel/broschueren/>
- Jugendmedienschutz – Filterlösungen im Schulischen Umfeld. Publikation der Initiative Schulen ans Netz e.V. 2006. Die Nutzung des Internets an Schulen wird ein immer wichtigerer Bestandteil einer zeitgemäßen Unterrichtskultur. Schulträger, Schulleitungen und Lehrkräfte stehen vor der gemeinsamen Herausforderung, die gesetzlich verankerte Aufsichtspflicht auch bei der Nutzung des Internets im Unterricht sicherzustellen. Diese Broschüre kann per Download bezogen werden (<http://itworks.schulen-ans-netz.de/publikationen/index.php>).
- Liesching, Marc: Surfen? - Mit Sicherheit! - Risiken im Internet. Herausgeber: Weisser Ring e.V., 2004. Auch diese Broschüre kann kostenlos aus dem Internet geladen werden – unter: http://www.weisser-ring.de/bundesgeschaeftsstelle/aktuell/publikationen/broschueren/surfen_mit_sicherheit_risiken_im_internet/index.php
- Ministerium für Innovation, Wissenschaft, Forschung und Technologie des Landes NRW: Internet-Fibel für die Grundschule. Unterrichtsmaterialien für die Grundschule. 2006. Download unter http://www.secure-it.nrw.de/media/pdf/schule/UM_Grundschule_einzel.pdf. Diese Broschüre bietet eine Vielzahl an Informationen nicht nur für die Grundschule.
- Sicherheit im Internet. Reihe Basics, Band 183. Verlag Knowware, 2004. <http://www.knowware.de>
- Viren, Hacker, Firewalls. Reihe Basics, Band 170. Verlag Knowware, Überarbeitete Auflage 2007. <http://www.knowware.de>
- Wischniewski, Thomas: „Sicherheit im Internet“- Datenschutz- und Datenschutzsicherheitsrisiken erkennen und minimieren, Reihe Themenmodule zur Verbraucherbildung, vzbv, 2004. Dieser Beitrag kann per Download bezogen werden: http://www.verbraucherbildung.de/projekt01/media/pdf/FB_Sicherheit_Internet_Wischniewski_1004.pdf

Tipp: Eine sehr umfassende Liste aktueller Broschüren und Materialien und deren Bezugsquellen (Kauf oder Download) kann auf der Seite <http://www.klicksafe.de/projekte/ratgeber.php> abgerufen werden.

Weiterführende Internetseiten

- <http://www.br-online.de/bayern3/pc>: Sehr aktuelle und informative Seite für Jugendliche der Online-Redaktion von Bayern 3.
- <http://www.bsi-fuer-buerger.de>: Eine sehr gut gemachte und aktuelle Seite des Bundesamts für Sicherheit in der Informationstechnik.
- <http://www.buerger-cert.de/default.aspx>: Das Bürger-CERT ist ein gemeinsames Projekt des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und Mcert Deutsche Gesellschaft für IT-Sicherheit. Das Bürger-CERT informiert und warnt Bürger und kleine Unternehmen schnell und kompetent vor Viren, Würmern und anderen Sicherheitslücken – kostenfrei und absolut neutral.
- <http://www.computer-greenhorn.de>: Diese Seite setzt sich ganz besonders für die Belange von "echten PC-Laien" ein. Die Autoren wissen, „dass es einem als Anfänger schwer fallen kann, eine für Profis vermeintlich leichte Frage zu stellen. Auf dieser Seite müssen Anfänger keine Panik davor haben, ausgelacht oder bloß gestellt zu werden, mag die Frage auch noch so simpel klingen“. Ziel der Autoren ist es, Laien näher an das interessante Thema Internet und Computer heranzuführen.
- <http://www.focus.de/digital/pc>: Aktuelle und einfach geschriebene Ratgeberseite
- <http://www.heise.de/security>: Aktuelle Sicherheitsbedrohungen des Fachmagazins Heise
- <http://www.joergkrusesweb.de/internet>: Sehr umfangreiche und gut gemachte private Informationsseite
- <http://jugendschutz.net>: jugendschutz.net überprüft das Internet auf Verstöße gegen den Jugendschutz und dringt darauf, dass Anbieter auch in diesem neuen Medium die Bestimmungen des Jugendschutzes einhalten und Rücksicht auf Kinder und Jugendliche nehmen. Hinweise auf Verstöße nimmt jugendschutz.net über seine Beschwerdestelle (Hotline) entgegen.
- <http://www.klicksafe.de> : klicksafe.de, ist eine Initiative der Generaldirektion Informationsgesellschaft und Medien der Europäischen Gemeinschaft. Sie will Sicherheit im Internet durch Medienkompetenz fördern.
- <http://www.lehrer-online.de> : Dies ist eine Service- und Informationsplattform von Schulen ans Netz e.V.. Lehrerinnen und Lehrer finden hier kostenfreie Informationen und Materialien rund um den Einsatz digitaler Medien im Unterricht.
- <https://passwortcheck.datenschutz.ch>: Hier kann die Sicherheit eines Passwort am konkreten Beispiel überprüft werden.
- <http://www.secure-it.nrw.de>: Ende 2001 wurde die Initiative »secure-it.nrw« gestartet. Sie will das Innovationspotenzial in NRW auf dem Gebiet der Sicherheit in der Informationstechnologie aktivieren und die Basis für den Markterfolg solcher Innovationen schaffen. Auf dieser Seite gibt es eine Fülle von Informationen gerade auch für Schulen.
- <http://www.sicherheit-online.net>: Eine privat und unabhängig betriebene Webseite mit einer Fülle von Informationen zum Thema „Sicherheit im Internet“.

- <http://www.sicher-im-Netz.de> : Seite der Initiative "Deutschland sicher im Netz", die sich in der Verantwortung sieht, Anwender vor Sicherheitsproblemen im Internet zu schützen.
- <http://www.schau-hin.info>: Ziel von „SCHAU HIN!“ ist die Sensibilisierung der Öffentlichkeit für das Thema "Kinder und Medien". Es geht darum, praxisnahe Hilfestellungen für den kindgerechten Umgang mit Medien, konkreten Rat und fundiertes Wissen von Experten an Eltern, Familien und pädagogische Fachkräfte weiterzugeben.
- <http://www.schulen-ans-netz.de>: ist die Seite des gemeinnützigen Vereins „Schulen ans Netz e.V.“, der das Lehren und Lernen mit neuen Medien im schulischen Umfeld fördert. Ein Hauptziel des Vereins ist „... die eigenverantwortliche und kritische Nutzung von neuen Medien und ihren Inhalten in der schulischen Bildung als eine alltägliche Selbstverständlichkeit für Lehrerinnen und Lehrer sowie Schülerinnen und Schüler zu etablieren.“

Tipp: <http://www.lehrer-online.de>. Diese Plattform unterstützt angehende und praktizierende Lehrerinnen und Lehrer mit einem kostenfrei nutzbaren Internet-Service rund um den schulischen Einsatz digitaler Medien. Im Mittelpunkt stehen dabei Unterrichtseinheiten aus der Schulpraxis der verschiedenen Schulformen und -stufen und Internet-Tools, die pädagogisch sinnvoll und ohne größere Vorbereitungen im Unterricht eingesetzt werden können.

Extra-Tipp: Für die Arbeit mit älteren Verbrauchern finden sie diverse Materialien unter [http://www.50plus-ans-netz.de/content/view/full/8227/\(first_node\)/10778](http://www.50plus-ans-netz.de/content/view/full/8227/(first_node)/10778) (Internet-Quiz) oder <http://www.sozialnetz.de/ca/rv/hqa/>.

Glossare

- <http://www.bsi-fuer-buerger.de/glossar>
- http://www.internet-abc.de/eltern/allgemein/suchen_und_finden/
- <https://www.sicher-im-netz.de/default.aspx?sicherheit/hilfreiches/lexikon>.
- <http://www.bsi-fuer-buerger.de/glossar>
- <http://www.netzmafia.de/skripten/glossar/index.html> .

Tipp: Unter dem letztgenannten Link gibt es ein hilfreiches Abkürzungsverzeichnis.

Modul 1: Kenntnisstand der Schüler testen

Anhand dieses Eingangstest sollen die Unterrichtenden in die Lage versetzt werden, die Köpfer oder Experten aus der Gruppe zu selektieren, um diese später immer wieder aktiv mit in den Unterricht einbeziehen zu können. Die folgenden 25 Fragen sollten am besten mittels eines Fragebogens ausgefüllt werden (vgl. dazu auch <http://www.klicksafe.de/kompetent/quiz.php>).

Tipp: Im Rahmen von einer Projektwoche oder einer ähnlichen Veranstaltung könnte ein solches Quiz auch online aufgesetzt werden. Ein kleiner Preis für die Experten könnte dazu als Anreiz ausgegeben werden.

Methode: Lernquiz, Fragebogen

Lernziel: Die Teilnehmer sollen durch das Quiz in die Thematik eingeführt werden.

Dauer: 20 Min Ausfüllen, 10 Min Auswertung, 5 Minuten Gruppeneinteilung

Material: Karteikarten, Fragebogen

Verlaufsskizze:

Lassen Sie sich zunächst von jedem Schüler ein Codewort und seinen Namen auf eine Karteikarte schreiben. Diese ordnen Sie während die Bogen von den Schülern ausgefüllt werden den einzelnen Schülern zu.

Ziehen Sie die ausgefüllten Fragebögen ein, durchmischen Sie diese und teilen diese wieder aus. Anhand der Lösungsmatrix können die Schüler die anonymen Fragebogen auswerten. Selektieren Sie die 5-6 bestausgefüllten Fragebögen und ernennen „Ihre“ Experten. Teilen Sie nun die Schüler in Kleingruppen ein und teilen Sie jeweils einen „Ihrer“ Experten pro Gruppe zu.

Fragebogen

Codewort: _____

Frage 1: Unter einem Virus versteht man

- 1. ein Programm, das Schäden auf dem Computer anrichten kann
- 2. die Abkürzung für Virtual User
- 3. die Säure, die sich bei Zugluft auf dem Mainboard freisetzt und es beschädigen kann

Frage 2: Unter Phishing versteht man

- 1. Photo-Snapshots in ein Online-Fotoalbum ins Internet stellen
- 2. die Eröffnung eines Internetshops, der Fotos anbietet: Photo-Internet-Shop
- 3. den Versuch, mit seriös wirkenden gefälschten E-Mails, Internetseiten oder per Telefon an die persönlichen Daten anderer zu kommen

Frage 3: Einen Spam-Filter benutzt man

- 1. beim Anschluss des Modems
- 2. zur Aussortierung unerwünschter E-Mails
- 3. zum Blockieren unerwünschter Internetseiten

Frage 4: Als „Trojanische Pferde“ werden bezeichnet:

- 1. Programme oder E-Mail-Anhänge, die Viren, Würmer oder Spionagesoftware verbergen
- 2. speziell für Dreharbeiten von Filmen mit Überlänge gezüchtete Pferde
- 3. Vorreiter in der Entwicklung von Anti-Viren-Software

Frage 5: Internetseiten, die über eine sichere Verbindung angezeigt werden, erkennt man

- 1. am https:// in der Adresszeile und am geschlossenen Vorhängeschloss in der Statuszeile (unterer Browserrand)
- 2. an der Eingabe-Aufforderung von Nutzernamen und Passwort
- 3. an der vollständigen Angabe ihrer Adresse, Telefonnummer und der Eintragsnummer im Handelsregister

Frage 6: Wie verhalte ich mich bei einer Phishing-Attacke?

- 1. Ich gebe die angeforderten vertraulichen Daten nicht heraus
- 2. Ich befolge alle Anweisungen, so wie verlangt
- 3. Ich bitte freundlich, mich zukünftig nicht mehr anzuschreiben oder anzurufen

Frage 7: Wie funktionieren Anti-Viren-Scanner?

- 1. Sie scannen die vorhandenen Viren und legen eine Grafik von ihnen an
- 2. Sie suchen böartige Programme, wie Viren, Trojaner und Würmer, indem sie sie mit ihnen bekannten Viren abgleichen und bereinigen bzw. löschen
- 3. Sie durchsuchen den Computer nach neuen Viren und melden diese bei der Internetpolizei

Frage 8: Es ist egal, wie groß ein E-Mail-Attachment ist, da ...

- 1. die Größen-Beschränkung nur durch den E-Mail-Provider gegeben ist.
- 2. es verboten ist, die Größe von E-Mails einzuschränken.
- 3. aus technischen Gründen eine E-Mail stets auf maximal 5 MB beschränkt ist.

Frage 9: Im Internet kann man

- 1. baden
- 2. surfen
- 3. nordic walken

Frage 10: Um Computer und Daten bei der Internetbenutzung zu schützen, sollte man

- 1. eine Firewall installieren
- 2. sein Handy ausschalten
- 3. nur schnurlose Geräte benutzen

Frage 11: Was sind Hacker?

- 1. Computerfreaks, die unbefugt in Computersysteme eindringen und Sicherheitssysteme knacken
- 2. Kleine Programme, die die Daten auf der Festplatte sortieren und in Segmente einteilen
- 3. Computerfreaks, die jährlich bei einem Treffen veraltete Software- und Spielversionen zerhacken

Frage 12: Gegen Spam-Mails kann ich mich wehren, indem ich

- 1. meine E-Mail-Adresse nicht unüberlegt herausgebe, und mir eine kostenlose Zweitadresse anlege, die ich einfach wieder kündigen kann
- 2. dem Absender zurück schreibe und ihn eindringlich beschimpfe
- 3. die Mail an alle meine Freunde und Bekannten zur Warnung weiterleite

Frage 13: Was ist eine Privacy Policy?

- 1. Eine Privatversicherung vor Gefahren aus dem Internet
- 2. Eine Erklärung darüber, was der Internetanbieter mit meinen Daten macht
- 3. Die Abteilung der Polizei, die sich um die Probleme von Privatpersonen bei der Internetnutzung kümmert

Frage 14: DFÜ ist die Abkürzung für

- 1. Download für Überlänge
- 2. digital fehlgeschlagene Übersetzung
- 3. Datenfernübertragung

Frage 15: Cookies sind

- 1. die kleinen Kekse, die häufig in Internetcafés als Snack ausliegen
- 2. Köche, die ihre Kochkünste und Rezepte über das Internet verbreiten
- 3. kleine Dateien, die auf der eigenen Festplatte gespeichert werden und u.a. Informationen über den Besuch der Internetseite speichern

Frage 16: WLAN-Netze sollten ausschließlich

- 1. verschlüsselt betrieben werden
- 2. mit Glasfaserkabel betrieben werden
- 3. von Erwachsenen genutzt werden

Frage 17: Spyware

- 1. sind Computerspiele, von denen es einem speiübel wird
- 2. funktioniert wie ein Spiegel: das Programm legt Sicherungskopien von Programmen, Dateien etc. an
- 3. bezeichnet Programme, die ohne das Wissen und ohne Zustimmung des Users sein Surfverhalten überwachen.

Frage 18: Was ist Hoax?

- 1. Bezeichnung für den Internetzugang von zu Hause aus
- 2. Ein spezielles Active-X-Programm
- 3. Eine "Ente"- also Falschmeldung - im Internet

Frage 19: Im Internetchat benutzt man sehr häufig:

- 1. Antonyme
- 2. Akronyme
- 3. Algorithmen

Frage 20: Ein DFÜ-Netzwerk sollte regelmäßig überprüft werden auf:

- 1. Neuzugänge
- 2. Dialer
- 3. geheime Botschaften

Frage 21: Eine Internet-Adresse www.xyz.de...

- 1. muss auf einem deutschen Server liegen
- 2. ist nur im deutschsprachigen Raum über das Internet zu öffnen
- 3. ist überall weltweit online abrufbar

Frage 22: Was sind Pop-Ups?

- 1. Überblendungen, die über nicht jugendfreie Texte gelegt werden
- 2. Fenster, die sich automatisch in einem weiteren Browserfenster öffnen
- 3. Aufblinkende Werbebanner

Frage 23: Was ist im Internet ein "sicherer Server"?

- 1. Ein Server, der eine Verschlüsselung der zu übertragenden Daten erfordert.
- 2. Ein Server, der angekettet ist, damit man ihn nicht stehlen kann.
- 3. Ein Server, auf dem die Daten verschlüsselt gespeichert werden.

Frage 24: Eine häufig verwendete Abkürzung in Chats ist:

- 1. lof
- 2. lol
- 3. tol

Frage 25: Wie funktioniert ein Internet-Filter?

- 1. Eine Membran in der Tastatur schützt diese vor Verschmutzung.
- 2. Der Computer erkennt, ob Kinder davor sitzen und sperrt dann bestimmte Seiten.
- 3. Der Browser zeigt Seiten, auf denen bestimmte Wörter oder Bilder vorkommen, nicht an.

Auswertung

Bitte die richtigen bzw. falschen Antworten ermitteln. Jede richtige Antwort ergibt einen Punkt.

Frage Nr.	Richtig	Falsch
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
Anzahl		
	richtig	falsch

	Codewort			
Der Teilnehmer		hat		von 25 möglichen Punkten

Lösungsmatrix

Nummer	Frage	1	2	3
1	Unter einem Virus versteht man	1		
2	Unter Pishing versteht man			3
3	Spam Filter benutzt man		2	
4	Trojanische Pferde werden bezeichnet	1		
5	Internetseiten, die über eine sichere Verbindung	1		
6	Verhalten bei Pishing-Attacke	1		
7	Funktion von Anti-Viren-Scanner		2	
8	Größe E-Mail-Attchement	1		
9	Im Internet kann man		2	
10	Schutz von PC und Daten im Internet	1		
11	Hacker	1		
12	Spam-Mail-Schutz	1		
13	Private Policy		2	
14	DFÜ			3
15	Cookies			3
16	WLANs	1		
17	Spyware			3
18	HOAX			3
19	Internetchat		2	
20	DFÜ-Netzwerk		2	
21	Internetadresse			3
22	Pop-Ups		2	
23	Sicherer Server	1		
24	Abkürzungen in Chats		2	
25	Internetfilter			3

Folgende Klassifizierung wird vorgeschlagen:

Richtige Antworten	Level	Anmerkungen
00-13	Verbesserungswürdig	
14-16	Durchschnitt	
17-19	Gute Kenntnisse	Dieses Level sollte nach der Unterrichtseinheit erreicht werden.
20-22	Experten	Aus dieser Gruppe können Sie Ihre Experten rekrutieren, die Sie aktiv in den Unterricht mit einbeziehen können.
23-25	Top-Experten	Das sind Ihre Experten, die Sie aktiv in den Unterricht mit einbeziehen sollten.

Tipp: Diese Quiz kann auch online nachgespielt werden.
<http://www.klicksafe.de/kompetent/quiz.php>

Modul 2: Gruppenarbeit: Welche Gefährdungen kennen Sie?

Ziel dieser Gruppenarbeit ist es, Internetschädlinge und andere Gefährdungen zu erarbeiten. Die Schüler sollen erkennen, dass neben technischen Abwehrmöglichkeiten vor allem das eigene Verhalten ausschlaggebend für einen sicheren Umgang mit dem Internet ist.

Methode: Gruppenarbeit

Lernziel: Die Teilnehmer sollen die Gefährlichkeit von Internetschädlingen einschätzen können

Dauer: Teilmodul 2a: 20 Minuten,
Teilmodul 2b: 20 Minuten

Material: Flipchart/Stellwand mit Leerplakat, Stifte, Bewertungspunkte

Verlaufsskizze:

Ziel dieser zweigeteilten Gruppenarbeit ist es zunächst Internetschädlinge (Teilmodul 2a) und später dann andere Gefährdungen (Teilmodul 2b) zu erarbeiten. Bereiten Sie dazu zwei Flipchart-Poster vor:

Die erste sollte ungefähr folgendermaßen aussehen:

Welche Internetschädlinge kennt Ihr?

Lfd. Nr.	Schädling		
1			
2			
usw.			

Lassen Sie sich von den Gruppe verschiedene Schädlinge nennen und schreiben Sie diese auf die Tafel.

In einer zweiten Runde fragen Sie nach den Möglichkeiten, etwas dagegen zu tun. Die Gruppe wird bald merken, dass es für verschiedene Schädlinge keine technischen Hilfsmittel gibt. Hier hilft nur das besonnene eigene Verhalten, der kompetente Umgang mit den Medien.

Nutzen Sie nun das Erfahrungswissen der Schüler, die Sie mittels des Eingangsquiz selektiert haben. Lassen Sie sich von diesen schildern, wie sie beispielsweise mit Hoaxes oder Spams umgehen und tragen Sie diese Tipps in die dritte Spalte ein.

Lfd. Nr.	Schädling	Schutz - Erste Hilfe	
1	Virus	Anti-Virus-Software	
2	Spam	Spam-Filter, Eigenes Verhalten, Zweit-Adresse	
3	Cookies	Eigenes Verhalten	
usw.			

Um die Gefährlichkeit der verschiedenen Schädlinge bewerten zu können, geben Sie allen Schülern Bewertungspunkte in den Farben rot = gefährlich, orange = mittel, grün = weniger gefährlich. Lassen Sie nun die Schüler Ihre Bewertungen für die einzelnen Schädlinge abgeben.

Am Ende dieser ersten Gruppenarbeit sollte das Flipchart ungefähr wie folgt aussehen:

Lfd.Nr	Schädling	Schutz – Erste Hilfe	Risikograd
1	Viren	Anti-Viren-Programme	●●●●●
2	Spam	Spam-Filter, Zweitadresse	●●●●●
3	Aktive Inhalte	Eigenes Verhalten	●●●●●
4	Cookies / Web Bugs	Eigenes Verhalten	●●●●●
5	Dialer	Anti-Dialer-Programme	●●●●●
6	Hoaxes	Eigenes Verhalten	●●●●●
7	Pishing	Eigenes Verhalten	●●●●●
8	Würmer	Anti-Viren-Programme	●●●●●
9	Trojaner	Anti-Viren-Programme	●●●●●

Teilmodul 2b:

Für den zweiten Teil dieses Moduls bereiten Sie bitte eine zweite Flipcharttafel wie folgt vor:

	Gefährdung	PC	Handy	Schutz – erste Hilfe
1				
2				
3				
4				

Ziel der Aufgabenstellung ist es, andere Gefährdungen im Internet/PC aber auch bei Mobiltelefonen zu erkennen. Notieren Sie auf Zuruf die diversen Gefährdungen in der zweiten Spalte und integrieren Sie wieder die Experten, indem Sie jeweils nach deren Erfahrungen fragen. Vielleicht gibt es gar „Opfer“, die bereit sind, über ihre Erfahrungen zu berichten. Erarbeiten Sie parallel dazu, wie man sich gegen solche Gefährdungen schützen kann.

Zum Abschluss dieser Teilaufgabe müsste Ihr zweites Flipchart ungefähr wie folgt ausschauen.

	Gefährdung	PC	Handy	Schutz – erste Hilfe
1	Abzocker	x		Eigenes Verhalten
2	Teure, überteuerte Downloads	x	x	Eigenes Verhalten
3	Kostenfallen (Dialer, Klingeltöne,	x	x	Aufklärung, eigenes Verhalten
4	Unerwünscht, ungewollte Kontakte, Anmache,	x		Eigenes Verhalten
5	Ungeeignete Inhalte	x	x	Filterprogramme
6	Ungeeignete Computerspiele/Handyspiele	x	x	Aufklärung, eigenes Verhalten
7	Fehlendes Unrechtsbewusstsein	x	x	Aufklärung, eigenes Verhalten

Modul 3: Checkliste Eigenes Verhalten

Ziel dieser Gruppenarbeit ist es, Internetschädlinge und andere Gefährdungen zu erarbeiten. Die Schüler sollen erkennen, dass neben technischen Abwehrinstrumenten vor allem das eigene Verhalten ausschlaggebend für einen sicheren Umgang mit dem Internet ist.

Methode: Gruppenarbeit

Lernziel: Die Teilnehmer sollen eine Checkliste für sich erarbeiten, die als Grundlage für einen sicheren Umgang im Internet dienen soll.

Dauer: Gruppenarbeit in Kleingruppen: 15 Minuten
Vorstellung der Ergebnisse im Plenum: 15 Minuten
Zusammenfügen der Ergebnisse: 15 Minuten
Praktische Übungen unter Anleitung der Experten: 15-30 Minuten

Material: Flipchart/Stellwand mit Leerplakat, Stifte, Klebstoff, möglichst für jede Gruppe einen Computer

Verlaufsskizze:

Die eingeteilten Kleingruppen erhalten jeweils Papier und Stifte und sollen in Form einer Checkliste erarbeiten, was sie Ihrer Meinung nach tun können, um sicher im Internet „surfen“ zu können. Planen Sie genügend Zeit ein, damit die Kleingruppen Ihre Ergebnisse dem Plenum präsentieren können. Fügen Sie abschließend die einzelnen Ratschläge zu einer gemeinsamen Checkliste zusammen. In praktischen Übungen sollen die Experten in den Kleingruppen abschließend praktisch zeigen, wie gewisse Vorsichtsmaßnahmen konkret umgesetzt werden können.

Tipp: Lassen Sie die Gruppen jeweils komplette Sätze bilden, die alle mit „Ich“ anfangen. Die Sätze sollen jeweils zeilenweise aufgeschrieben werden. Später können Sie dann die einzelnen Sätze einfacher zu einer gemeinsamen Checkliste zusammenfügen.

Tipp: Spätestens bei diesem Modul sollten Sie immer wieder auf rechtliche Aspekte der Internetnutzung hinweisen. Speziell zum weit verbreiteten Downloaden und Kopieren von illegaler Software, Musik oder Filmen sollten Sie auf die rechtlichen Konsequenzen aufmerksam machen. Informationen dazu unter anderem unter: http://www.symantec.com/de/de/home_homeoffice/library/article.jsp?aid=article2_04_06, http://www.stiftung-warentest.de/online/computer_telefon/meldung/1343451/1343451.html und http://archiv.chip.de/news/c1_archiv_news_17201281.html.

Die gemeinsam erarbeitete Checkliste könnte dann zum Beispiel ungefähr folgendermaßen aussehen:

Was kann ich tun, um sicher im Internet bzw. am PC arbeiten zu können?

Checkliste

- Ich setze eine Firewall und Virenschutzsoftware ein.
- Ich halte diese ständig auf den aktuellsten Stand. Ich führe Updates sofort aus.
- Ich führe regelmäßig Softwareaktualisierungen - vor allem auch für mein Betriebssystem - durch.
- Ich arbeite an meinem Computer normalerweise nicht mit Administratorenrechten. Ich habe ein Benutzerkonto mit eingeschränkten Rechten eingerichtet.
- Ich habe die Funktionen „Aktive Inhalte (ActiveX)“ und „Java Script (Java Applets)“ deaktiviert.
- Ich bin immer besonders vorsichtig, wenn ich über Eingabemasken dazu aufgefordert werde „JA“ oder „OK“ einzugeben.
- Ich vergewissere mich immer, welche Inhalte mir zu welchen Konditionen angeboten werden.
- Ich bin extrem vorsichtig bei Mails mit Anhängen. Ich öffne Anhänge nur von Mails, bei denen ich absolut sicher bin, dass ich dem Sender vertrauen kann.
- Ich fertige Back-ups von meinen wichtigsten Daten automatisiert und regelmäßig an.
- Ich prüfe meine Back-ups bevor ich diese archiviere.
- Erhalte ich Daten von Freunden und Bekannten über Memorystick, CD/DVD, stelle ich zunächst sicher, dass es sich um virenfreie Daten oder Programme handelt. Ich nehme immer erst einen Virenskan vor.
- Wenn ich aus dem Internet Software herunterlade, stelle ich zunächst sicher, dass die Quellen nicht verseucht sind.
- Ich vermeide illegale Software. Ich weiß, dass solche Quellen oft perfekte Brutstätten für Viren, Trojaner und Würmer sind.
- Ich gehe sehr sorgfältig mit meinen Zugangsdaten um: Ich halte Kennwörter und Benutzernamen sowie Zugangscodes für Dienste (z. B. für Online-Banking) an einem sicheren Ort unter Verschluss.
- Meine Passwörter sind nicht leicht zu erraten: sie bestehen aus Zahlen, Buchstaben und Sonderzeichen.

Tipp: In diesem Modul ist es ganz besonders wichtig, dass die den Kleingruppen zugeordneten Experten, Zeit haben, den nicht so versierten Schülern konkret zu zeigen, wie bestimmte Dinge gemacht werden. Lassen Sie die Experten in den Kleingruppen ihren Mitschülern beispielsweise zeigen, wie in den diversen Browsern Activ-X-Inhalte deaktiviert werden oder wie man Cookies löscht!

Modul 4: Sicheres Passwort

Der Internetzugang, das Email-Postfach, Ebay, Online-Banking, Foren oder bestimmte Webseiten: Wer sich regelmäßig im Internet bewegt, braucht im Grunde eine wahre Flut von unterschiedlichen User/Passwort-Kombinationen. Sehr häufig sind Passwörter unklug oder unbedacht gewählt und daher für Hacker und andere Bedrohungen leicht zu entschlüsseln. Die meistverwendete Ausrede ist, dass man sich die unterschiedlichen Passwörter nicht merken kann. Machen Sie aber trotzdem nicht den Fehler, nur eine Kombination für die unterschiedlichen Zugänge zu verwenden. Grundsätzlich gilt: Je sensibler ein Zugang ist (etwa, weil es um Ihr Bankkonto geht), umso mehr Sorgfalt sollte man auf die Verschlüsselung legen. Das bedeutet in der Praxis: Immer, wenn Sie im Internet identifizierbar sind (und ein Täter damit auch auf andere Zugänge von Ihnen schließen könnte), sollten Sie ein unterschiedliches Passwort verwenden. Gute Passwörter erhöhen die Sicherheit erheblich, schlechte Passwörter können von Spezialprogrammen in wenigen Minuten oder gar Sekunden geknackt werden.

Methode: Gruppenarbeit, Arbeit am PC

Lernziel: Die Schüler sollen lernen, sichere Passwörter zu entwickeln. Über clevere „Eselsbrücken“ können auch schwierige Passwörter einfach zu behalten sein.

Dauer: 1. Gruppenarbeit: 10 Minuten 2. Gruppenarbeit: 10 Minuten
Passwortcheck am Rechner: 10-20 Minuten

Material: Flipchart/Stellwand mit Leerplakat, Stifte
PCs (falls vorhanden), Lehrerrechner

Verlaufsskizze:

Dieses Lernmodul beginnt mit der Eingangsfrage nach Beispielen für gute und schlechte Passwörter. Diese werden vom Unterrichtenden in gute und schlechte Passwörter sortiert.

Tipp: Weisen Sie immer wieder darauf hin, dass die Schüler nicht Ihre persönlichen Passwörter nennen.

Lassen Sie sich von Ihren Schülern Passwörter zurufen und sortieren Sie diese auf einer Flipchart nach guten und schlechten Passwörtern.

Beispiele für gute Passwörter	Beispiele für schlechte Passwörter
z. Bsp.: %%Oma896, DSbtu7:35,	z.Bsp.: Babsi, Tobi, Tobi01, 12345678, 99933311, Polly

Aus diesen Beispielen erarbeiten Sie in einem zweiten Schritt, was denkbar ungeeignete Passwörter sind!

Was sind denkbar ungeeignete Passwörter?

Mögliche Antworten:

- Geburtsdatum von Freund oder Freundin, Geschwister
- Eigener Namen oder Namen (auch Kosenamen) von Freund oder Freundin
- Wohnort
- Name des Haustiers
- Fremdwörter
- Telefon- und Handynummern
- Konto- oder Passnummer

Notieren Sie die Antworten ebenfalls auf ein Flipchart.

Tipp: Fragen Sie nach dem Aufbewahrungsort der diversen Passwörter. Verdeutlichen Sie, dass das beste Passwort nichts nützt, wenn es per Post-it am Rechner gut sichtbar befestigt ist oder wenn die Passwörter unter einer Datei password.doc oder ähnlich auf dem PC gespeichert wurden. Über bestimmte Schadprogramme - etwa Trojaner - lassen sich so gespeicherte Passwörter einfach ausspionieren. Wenn Sie sich Ihre Passwörter nicht merken können, notieren Sie diese allenfalls auf einem Blatt Papier und bewahren Sie dieses an einem sicheren Ort auf.

Fragen Sie als nächstes die Großgruppe: Wann gilt ein Passwort als sicher?
Erarbeiten Sie die folgende Antwort:

Als sicher gelten Passwörter, die aus mindestens 8 Zeichen bestehen. Wichtig ist, dass diese 8 Zeichen aus Buchstaben, Zahlen und Sonderzeichen bestehen. Wichtig ist dabei auch, dass Groß- und Kleinbuchstaben verwendet werden.

Machen Sie Ihren Schülern deutlich, wie wichtig ein gut gewähltes Passwort ist.

Lassen die Schüler einen Passwortcheck Ihres persönlichen Passwortes durchführen. Lassen Sie dabei die Schüler über eine online-Suche herausfinden, wo man so einen Test durchführen kann.

Als mögliche Test-Seiten kommen z.B. die folgenden in Betracht:

<https://passwortcheck.datenschutz.ch/>

<https://www.cnlab.ch/codecheck/check.php>

<http://www.php-gfx.net/Scripte/passwortcheck.php?passwort=>

Tipp: Unter der an zweiter Stelle genannten Adresse <https://www.cnlab.ch/codecheck/check.php> können Sie die Qualität der Passwörter miteinander vergleichen, indem Sie die „approximate time to find“ vergleichen. Lassen Sie dazu die Schüler nacheinander (nicht in den Gruppen!) an einem oder mehreren Rechnern diesen Test durchführen. Das Ergebnis in Sekunden/Tage soll auf Karteikarten notiert werden. Dabei stehen grüne Karten für „strong“, also gute Passwörter, orangefarbene Karten für „usable“, also akzeptable Passwörter und rote Karten für „weak“, also unbrauchbare Passwörter.

Tipp: Sie können mit dieser Seite auch anhand von selbst generierten Passwörtern, z.B. nextstep, Nextstep1 und %Nextstep1 die Bedeutung der Sonderzeichen verdeutlichen, indem Sie den Test selbst durchführen und die Ergebnisse mit dem Beamer zeigen.

Zum Abschluss lassen Sie die Kleingruppen gute Passwörter entwickeln. In dieser Teilaufgabe geht es nicht nur darum, dass diese Passwörter sicher sind - das wurde in der Zwischenzeit gelernt - sondern auch, wie man sich diese gut merken kann.

Notieren Sie die Beispiele für solche Passwörter und die dazugehörigen „Eselsbrücken“ auf ein Flipchart. Die Beispiele könnten dann ungefähr so aussehen:

	Passwort	Merksatz, „Eselsbrücke“
1	JKwwW?1990	Jürgen Klinsmann wurde wann Weltmeister?1990
2	DSbtu7:35	Die Schule beginnt täglich um 7:35
3	MFig1m65g!	Meine Freundin ist genau 1 Meter und 65 cm groß!

Modul 5: Das Internet nutzen und dabei anonym bleiben

Ein gutes Passwort verhindert, dass ein Anwender leicht ausspioniert werden kann. Allerdings ist dadurch noch lange nicht gesichert, dass man anonym im Netz surfen kann. Der Mensch fühlt sich sicher, wenn er sich in einer sicheren Umgebung wähnt. Rein technisch betrachtet muss ein Rechner mit einer IP-Adresse wieder lokalisierbar sein. Allerdings ist mit einem Rechner, der eine Internet-Verbindung hat, auch die heimische Wohnung nicht mehr unbedingt eine sichere Umgebung und allein ist der Anwender im Internet schon gar nicht. Eine Vielzahl von Informationen wird versendet, ohne dass der Nutzer dieses bemerkt oder seine Einwilligung dazu gegeben hat.

Methode: Kleingruppenarbeit, Arbeit am PC

Lernziel: Die Schüler sollen lernen, bewusster mit der Datenweitergabe im Internet umzugehen. Ziel dabei ist, sie so wenig Daten wie möglich im Internet weiterzugeben.

Dauer: Einführung: 5-10 Minuten
„Expertenberichte“: 15 Minuten
Sortieren der Ergebnisse: 10 Minuten
Selbsttest: 10 Minuten

Material: Flipchart/Stellwand mit Leerplakat, Stifte,
PCs (falls vorhanden), Lehrerrechner

Verlaufsskizze:

Einleitend sollten Sie Beispiele aktueller Internetkriminalität nennen und am besten der Gruppe über den Beamer zeigen. So verdeutlichen Sie die Notwendigkeit für Anonymität.

Tipp: <http://www2.oncomputer.t-online.de/dyn/c/10/26/55/74/10265574,si=0.html>

Dort können unter dem Link „sechs Fakten zur Cyberkriminalität“ Beispiele von gefassten Internetkriminellen und deren Bestrafung gefunden werden, u.a. „eBays Alptraum“: Im Jahr 2000 machte ein kanadischer Jugendlicher mit dem Spitznamen "Mafiaboy" auf sich aufmerksam: Von seinem Zimmer aus infiltrierte er Webseiten großer Unternehmen wie eBay und Amazon. Diese versah er mit der Nachricht, die Seite könne nicht aufgerufen werden, und hinderte somit die Kunden am Besuch.

Dadurch fügte der 16-Jährige den Firmen finanzielle Schäden in Höhe von 1,5 Milliarden US-Dollar zu und wurde zu acht Monaten Jugendstrafvollzug verurteilt. Das zweite Beispiel „König der Hacker“ zeigt, wie drastisch die Strafen ausfallen können: „Auf der Fahndungsliste der amerikanischen Bundespolizei FBI stand lange Jahre der Name Kevin Mitnick ganz oben. Der Hacker mit dem Decknamen "Condor" knackte tausende Netzwerke, darunter mehrmals das des Pentagon, und narrete die Polizei bei seiner aberwitzigen Flucht. Mit einem Scanner machte er die Funkübertragungen der Polizisten aus und war dadurch seinen Verfolgern stets einen Schritt voraus. 1995 wurde Mitnick doch geschnappt und musste für fünf Jahre hinter Gittern.

Lassen sie zunächst „Ihre“ Experten berichten, was sie tun, um im Internet unerkannt zu bleiben. Sammeln Sie die Antworten mittels farbiger Karteikarten (z.B. blau für Technik und

weiß für eigenes Verhalten) und sortieren Sie diese nach technischen Mitteln (z.B. Software) oder Verhaltensmaßnahmen (z.B. das Löschen von Cookies).

Tipp: Vermutlich werden Sie wesentlich mehr technische Vorschläge bekommen als Verhaltensregeln. Legen sie deshalb wert darauf, dass die „Experten“ gerade von Ihrem eigenen Verhalten berichten.

Sortieren Sie die Antworten auf dem vorbereiteten Flipchart, dass dann in etwa so ausschauen sollte:

Was tun Sie, um im Internet unerkannt zu bleiben?

Technische Möglichkeiten	Eigenes Verhalten
„Winsweep“ nutzen	Die Cookies nach jeder Surfsession löschen
Anonymisierende Proxy-Server oder Proxynetze nutzen	Im Chat, nie meinen richtigen Namen benutzen
Remailer nutzen	History der aufgesuchten Internetseiten löschen
Firewall benutzen	(Gute) Passwörter benutzen
Anti-Spyware	
Verschlüsselte E-Mails senden	

Tipp: Eine gut gemachte Zusammenfassung zu technischen Details finden Sie unter http://de.wikipedia.org/wiki/Anonymit%C3%A4t_im_Internet, <http://hp.kairaven.de/bigb/asurf.html#a1> oder <http://www.netplanet.org/sicherheit/anonym.shtml>

Dort werden unter anderem auch „Remailer“ erläutert: „Ein „Remailer“ entpersonalisiert Nachrichten, indem er E-Mail-Header entfernt, die Rückschlüsse auf den letzten Absender zuließen. Damit ermöglicht er es, jemandem eine E-Mail zu schicken, ohne dass der Empfänger den Namen oder die E-Mail-Adresse des Senders herausfinden kann“.

In einem nächsten Schritt lassen Sie die Schüler in den Kleingruppen einen Test machen, um festzustellen, wie viel Informationen diversen potentiellen Interessenten zur Verfügung stehen. Nutzen Sie dazu den folgenden Link: <http://www.anonym-surfen.com/anonym-surfen/test> . Die Schüler werden erstaunt sein, was Sie auf dieser Seite alles über den jeweiligen Rechner erfahren können. Nutzen Sie dieses Erstaunen aus und erklären Sie dabei, wozu diese Informationen sogar von seriösen Anbietern genutzt werden können. Auf <http://www.anonym-surfen.com> finden Sie darüber hinaus detaillierte Informationen zu diesem Teilaspekt.

Tipp: Klären Sie mit Ihrem Netzwerkverantwortlichen zuvor ab, wie das Netzwerk konfiguriert wurde und ob dieser Test durchgeführt werden kann. Falls das nicht der Fall ist, können Sie diese Aufgabe auch als Hausaufgabe stellen und die Ergebnisse zum Unterricht mitbringen lassen.

Zum Abschluss lassen Sie die Gruppe die Ergebnisse zusammenfassen. Stellen Sie sicher, dass dabei neben den technischen Möglichkeiten das eigene Verhalten im Mittelpunkt steht. Verdeutlichen Sie nochmals, dass Angaben zur Person oder die E-Mail-Adresse oft überhaupt nicht gemacht werden müssen. So werden z.B. bei Gewinnspielen oder anderen

interaktiven Elementen Angaben gefordert, die überhaupt nicht gegeben werden müssen. Daten sollten nur dort herausgegeben werden, wo es unbedingt sein muss. Viele Preisausschreiben, Bonussysteme oder Kundenkarten dienen nur dazu, die Identität der Teilnehmer zu erfahren.

Tipp: Ausführliche Informationen zum anonymen Surfen erhalten Sie auch in einem Beitrag von Thomas Wischniewski, den Sie per Download unter http://www.verbraucherbildung.de/projekt01/media/pdf/FB_Sicherheit_Internet_Wischniewski_1004.pdf beziehen können.