MEINE DATEN KRIEGT IHR NICHT!

Unterrichtseinheit: Datenschutz

Herausgegeben von: HmbBfDI

Hamburg

Vorwort

Die Initiative „Meine Daten kriegt ihr nicht!“ ist Anfang letzten Jahres mit einem viel beachteten Pilotprojekt an der Gesamtschule Walddörfer gestartet. Ausgangspunkt des gemeinsamen Projekts war die Erkenntnis, dass das Leben in der digitalen Gesellschaft erlernt und eingeübt werden muss und dass gerade den Schulen die zentrale Funktion für die Datenschutzkompetenzförderung junger Menschen zukommt. Klar ist auch, dass die digitale Gesellschaft keine Schonzeit kennt: Das Eintrittsalter in die sozialen Netzwerke liegt noch unterhalb der persönlichen Schuldfähigkeit im Strafrecht. Die Angebote, die Kinder im Netz erwarten, beginnen nicht selten schon im Grundschulalter. Gerade auch für den schulischen Alltag nutzen Schüler das Internet als Nachschlags- und Wissensquelle. Es besteht dringender Handlungsbedarf.

Es ist daher wichtig, dass die Initiative auf dem eingeschlagenen Weg zügig weiter voranschreitet. Beim Eintritt in die zweite Projektphase gilt es nun, der Initiative ein breiteres Anwendungsfeld vor Ort zu sichern. Der Schlüssel zum Ziel, alle Hamburger Schulen mit dem Bildungsangebot zu erreichen, führt nur über die Weitergabe der Qualifikationen und Kompetenzen zur Informationsvermittlung an diejenigen, die für eine Transformation des Wissens vor Ort von Berufs wegen eintreten: Gemeint sind alle Lehrkräfte an Hamburgs Schulen. Ihre individuelle Motivation, ihr Wissen, aber auch ihre pädagogischen Fähigkeiten sind gefragt! Daher hatte es oberste Priorität, dass die Ansätze und Ideen in den vergangenen Monaten zu einem Konzept der Lehrerfortbildung verfestigt wurden.

Die vorliegende Broschüre ist als Handreichung für Lehrerinnen und Lehrer konzipiert. Sie soll diesen künftig erleichtern, eigenständig einen Unterricht zur Förderung der Datenschutzkompetenz an ihren Schulen zu entwickeln und vor Ort anzubieten.

Prof. Dr. Johannes Caspar
Der Hamburgische Beauftragte
für Datenschutz und Informationsfreiheit

Erstellt wurde die Broschüre durch Herrn Norbert Finck, einem engagierten Lehrer, der bereits wesentlich an der Initiative der Gesamtschule Walddörfer beteiligt war. Die Federführung der Arbeiten lag bei Herrn Volker Wegner vom LI. Die wissenschaftlich-pädagogische Unterstützung für die Handreichung kam von Herrn Prof. Dr. Norbert Breier vom Lehrstuhl für Erziehungswissenschaft unter besonderer Berücksichtigung der Didaktik der Informatik von der Universität Hamburg mit seinem Team. Beratend bei der Umsetzung des ursprünglich hier erstellten Entwurfs wirkte die Behörde für Datenschutz und Informationsfreiheit der Freien und Hansestadt Hamburg mit.

Ziel in der zweiten Projektphase ist es, in den kommenden Monaten möglichst viele Lehrerinnen und Lehrer an den Hamburger Schulen zu erreichen und damit die Bedingungen für eine hamburgweite Umsetzung der Datenschutzkompetenzförderung für alle Schülerinnen und Schüler zu schaffen.

Dass laut neuester JIM-Studie (Jugend, Information, ([Multi-] Media) gerade die Jugendlichen erhöht darauf achten, ihre persönlichen Informationen stärker zu schützen, kann für die Initiative „Meine Daten kriegt ihr nicht!“ nur ein Ansporn sein. Ein Problembewusstsein ist vorhanden. Information, Aufklärung und Selbstreflektion werden jedoch benötigt, damit jeder Einzelne einen selbstverantwortlichen Umgang mit den eigenen Daten und einen respektvollen Umgang mit den Daten anderer erlernen kann.

Allen Beteiligten darf ich noch einmal meinen herzlichen Dank für ihr großes Engagement bei der gemeinsamen Arbeit an unserem Projekt und an der Erstellung dieser Broschüre aussprechen. Ich wünsche der Handreichung eine möglichst weite Verbreitung. Mit der Veröffentlichung ist ein neuer wichtiger Schritt getan zur Datenschutzkompetenzförderung in Hamburg, aber auch an all den anderen Orten, an denen eine Verankerung des Datenschutzes bei der schulischen Umsetzung angestrebt wird.

Senator Dietrich Wersich
Präses der Hamburger Behörde
für Soziales, Familie, Gesundheit und Verbraucherschutz

Geleitwort

In den letzten Jahren sind viele neue Datenautobahnen entstanden mit mehr Verzweigungen, die neue Möglichkeiten eröffnen. Gleichzeitig ist aber auch die Gefahr gestiegen, die Orientierung zu verlieren. Schon aus meiner Arbeit als Jugend- und Familiensenator weiß ich, dass besonders Jugendliche sich in diesen virtuellen Verkehrswegen oft unbekümmert bewegen, ohne die möglichen Probleme zu kennen. Hier muss auch die Schule ihren Beitrag zur Entwicklung von Medienkompetenz bei Schülerinnen und Schülern leisten. Dafür benötigen wir jedoch auch Lehrkräfte, die das notwendige Know-how zum verantwortungsbewussten Umgang mit Internet und WEB 2.0 mit in die Schule bringen.

Ich begrüße es deshalb sehr, dass der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit in Kooperation mit dem Landesinstitut für Lehrerbildung und Schulentwicklung, der Medienanstalt Hamburg/Schleswig-Holstein und weiteren Kooperationspartnern ein Fortbildungsmodul für Lehrkräfte entwickelt hat, das sich zentral mit dem Datenschutz befasst.

Mit dieser auf der Fachkompetenz von Experten aufgebauten Fortbildung wird die Grundlage für einen zeitgemäßen, auf Prävention bei der Internetnutzung ausgerichteten Unterricht gelegt. Besonders wirkungsvoll ist das direkte Ausprobieren in der Realität des Internets mit fiktiven Personen.

Der vorliegende, aus dieser Initiative hervorgegangene und durch das Engagement von Mitarbeiterinnen und Mitarbeitern in Schule, Universität und Behörden entwickelte Leitfaden ist eine gelungene Grundlage für den Unterricht im Rahmen des Aufgabengebietes Medienerziehung.

Ich wünsche diesem hochaktuellen Gemeinschaftsprojekt einen großen Erfolg mit hoher Wirksamkeit. Mit der Förderung der Medienkompetenzentwicklung werden die Schülerinnen und Schüler dann auch in der Lage sein, ihren persönlichen Umgang mit dem Internet in ihrer Freizeit mit der erforderlichen Umsicht zu gestalten.

Inhalt

1. Einleitung

Durchschnittlich zwei Stunden pro Tag – so viel Zeit verbringen Jugendliche am PC, ein großer Teil davon im Internet. Sie nutzen das Internet vielfältig, teilweise zum Spielen und zum Versenden von Nachrichten, teilweise für schulische Aufgaben wie Internet-Recherchen, teilweise kreativ zum Aufbau eigener Seiten mit eigenen Ideen, zunehmend aber auch zum „Chillen" in sozialen Netzwerken („online-communities" oder „social-communities"). Über fünf Millionen Schüler sind beispielsweise bei SchülerVZ angemeldet, sie tauschen private Fotos aus, bilden Gruppen von „Freunden", schreiben diesen E-Mails oder kurze Nachrichten an deren Schwarzen Brettern. Doch jeder Klick hinterlässt Spuren und schon bei der ersten Anmeldung werden persönliche Daten abgefragt, die so schnell nicht mehr aus dem Netz zu löschen sind. Das Internet hat kein Radiergummi!

Wir als Lehrer müssen uns damit auseinander setzen, auf welchen Internetseiten unsere Schüler unterwegs sind. Wir müssen uns ihre virtuellen Lebenswelten zeigen lassen und sie als Experten in Teilbereichen anerkennen. Wir müssen ihnen aber auch vermitteln, wie sie bestimmte Gefahren in ihrem, vielleicht sorglosen Umgang im Internet und insbesondere in sozialen Netzwerken vermeiden können. „Sicher in sozialen Netzwerken", diesem Ziel soll die vorgelegte Handreichung dienen.
Das Projekt „Meine Daten kriegt Ihr nicht!" ist ein Gemeinschaftsprojekt des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit in Kooperation mit der Behörde für Schule und Bildung, dem Landesinstitut für Lehrerbildung und Schulentwicklung, der Medienanstalt Hamburg / Schleswig-Holstein, der Polizei Hamburg und dem Norddeutschen Rundfunk.

In der vorliegenden Unterrichtseinheit wird ein Unterricht aus einem Kurs im Jahrgang 7 vorgestellt, der im Frühjahr 2010 an der Gesamtschule Walddörfer durchgeführt wurde. Bei der Übernahme dieser Unterrichtseinheit im Jahrgang 7 anderer Schulen ist ein Zeitrahmen von etwa 12 Unterrichtsstunden sinnvoll, besondere Vorbereitungen oder Vorkenntnisse sind (fast) nicht erforderlich, lediglich ein zuverlässiger Internet-Zugang ist nötig. Die Schüler werden an zwei praktischen Beispielen Internet-Recherchen zu fiktiven und realen Personen durchführen und dabei auch sensible - also schützenswerte - Informationen erfahren. An diese praktischen Arbeiten werden sich jeweils Reflexionsphasen anschließen, Ergänzungen zu weiteren Fragen des Datenschutzes im Internet sind möglich. In der vorgelegten Handreichung werden die Unterrichtsabschnitte mit zentralen Fragen und Arbeitsaufträgen genannt, Arbeitsblätter sind angefügt, die Schilderungen werden durch Erfahrungen aus dem Unterrichtsversuch ergänzt. Zusätzlich wird auf TV-Berichte über das Pilotprojekt und auf weitere online-Quellen hingewiesen.

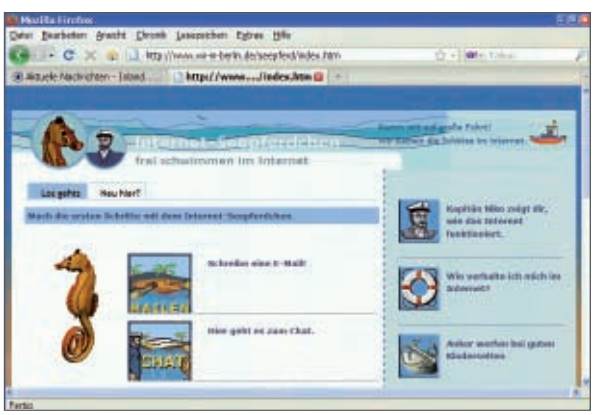
Ich danke der Medien-Abteilung des Landesinstituts für die organisatorische Unterstützung und dem Datenschutz-Team für zahlreiche Anregungen und Ideen sowie für die kontroversen Überlegungen zu virtuellen Figuren im Internet, ich danke dem Studenten Nico Lange für seine sehr sorgfältigen Unterrichtsmitschriften und Einschätzungen und Anregungen und konstruktiven Vorschläge sowie Frau Ines Lessing – Didaktische Leiterin der Stadtteilschule Walddörfer – und Herrn Prof. Dr. Norbert Breier – Universität Hamburg, Didaktik der Informatik – für die zahlreichen Gespräche und Anregungen und insbesondere für die Hinweise auf das Planspiel und auf weitere Internet-Quellen.

Kurs Naturwissenschaft und Technik im Jahrgang 7 der Gesamtschule Walddörfer – Pilotgruppe des Projekts „Meine Daten kriegt Ihr nicht !"

2. Datenschutz als Teil der Medienerziehung

– Kompetenzen im Datenschutz –

In den Bildungsplänen der Behörde für Schule und Berufsbildung werden bereits für die Jahrgänge 5-6 die Anforderungen „Die Schülerinnen und Schüler (...) benennen Gefahren, die im Internet durch Viren, Hacker, Phishing u. a. bestehen, und kennen grundlegende Schutzmöglichkeiten (auch für die eigene Person) (...) und gehen bewusst mit persönlichen Daten und Passwörtern um“ (Bildungsplan, noch für die Primarschule, Aufgabengebiete, 2010) und dafür wird das Themenfeld „Sicher im Internet unterwegs“ vorgeschlagen. Für diese Jahrgänge ist eine Lernumgebung wie das „Seepferdchen“ altersgemäß und besonders geeignet. Eine Behandlung datenschutzrechtlicher Aspekte in den Jahrgängen 5 und 6 ist in jedem Fall dringend erforderlich, denn die Gespräche mit diesen Schülern zeigen, dass bereits einige von ihnen schon die sozialen Netzwerke nutzen, und dabei haben sie vielleicht schon gleich bei der Anmeldung schon zu viele Daten angegeben, die später nicht mehr zu löschen sind.



http://www.wir-in-berlin.de/seepferd/index.htm

Für die ersten Bildungsabschlüsse werden die Mindestanforderungen wie folgt formuliert: „Die Schülerinnen und Schüler kennen Chancen und Risiken sowie die wesentlichen Schutzmaßnahmen und rechtlichen Grundlagen (Datenschutz, (...) Persönlichkeitsrecht) (...) bewegen sich unter Beachtung der rechtlichen Grundlagen sicher in virtuellen Räumen, schätzen Möglichkeiten und Gefahren realistisch ein (...)“ (Bildungspläne Stadtteilschule und Gymnasium Sek I, Aufgabengebiete, Medienerziehung, 2010).
Gefordert ist hier also einerseits das Wissen um die Folgen für das eigene Handeln und andererseits die Einstellung und Bereitschaft zu einem bewusster Umgang mit den Angeboten virtueller Räume. Die Anforderungen der Rahmenpläne bestehen also nicht aus einer Vermeidung des Internet‘ und der sozialen Netzwerke, vielmehr sollen Internet und soziale Netzwerke kritisch, bewusst und selbstbewusst genutzt werden.

3. Nutzung von Daten realer Personen im Unterricht?

Vorüberlegungen und Vorbereitungen vor der Unterrichtseinheit

Vor Beginn der Unterrichtseinheit sind zwei planerische Fragen zu klären:

- Sollen reale Daten aus dem realen Internet für den Unterricht genutzt werden?
- „… nicht alle Angaben müssen stimmen …" – Ein Lernziel für Soziale Netzwerke? Ist hier nicht ein Widerspruch zwischen einerseits dem Erziehungsauftrag der Schule nach Ehrlichkeit und Wahrhaftigkeit und andererseits der Notwendigkeit des Daten- und Persönlichkeitsschutzes?

Sollen reale Daten aus dem realen Internet für den Unterricht genutzt werden?

Würden reale Daten von Schülern und Lehrern, die ja im Internet vorhanden und schnell zu finden sind, einfach für den Unterricht genutzt werden, so wäre keine weitere Vorbereitung durch den Lehrer mehr erforderlich. Ich empfehle aber den aufwändigeren Weg, auf diese realen Daten zu verzichten.

Diese realen Daten und Informationen sollen als Negativ-Beispiel bloß gestellt werden, das ginge gerade nicht mit Informationen der Mitschüler und der Lehrer. Die Daten der Schüler wären nur mit schriftlicher Einverständniserklärung der Eltern nutzbar, das Verständnis dafür stünde aber erst am Ende der Unterrichtseinheit. Wir Lehrer durchblicken die sozialen Netzwerke nicht hinreichend und können deshalb nicht entscheiden, ob nach einem Zugang auf privaten Seiten nicht doch Link-Verweise auf problematische oder jugendgefährdende Inhalte vorhanden sein könnten.

Natürlich lässt sich die Recherche nach Freunden und Geschwistern nicht aus dem Unterricht heraus halten, aber sie dürfen nicht als Lerngegenstand genutzt werden. Natürlich lassen sich die Informationen über fiktive Personen nur über einen gewissen Zeitraum steuern, aber letztlich werden sie auch nur für kurze Zeit benötigt.

Das Einstellen und das Nutzen fiktiver Personen ins Internet wäre eine Möglichkeit, auf die Nutzung realer Daten zu verzichten.

Bitte prüfen Sie, ob Sie fiktive Personen im Internet platzieren möchten.

Bitte prüfen Sie, ob Sie Ihre Schüler vorher darüber informieren, dass die genutzten Personen fiktiv sind. Ich habe darauf verzichtet und bin darauf erst im Verlauf der Unterrichtseinheit eingegangen.

Hier folgen drei Stellungnahmen mit Begründungen zum Verzicht auf die Nutzung realer Daten und Informationen in dieser Unterrichtseinheit.

„Ich empfehle, im realen Internet nur mit den Daten fiktiver Personen zu arbeiten, denn die Arbeit mit realen Daten von Mitschülern und Lehrern steht im Widerspruch zum eigentlichen Ziel der Unterrichtseinheit, dass die Schülerinnen und Schüler lernen sollen, ihre Privatsphäre angemessen zu schützen. Ich kann die realen Personen nicht schützen und gleichzeitig mit deren Daten arbeiten. Rechtlich ungeklärt ist aber noch die Frage, ob es zulässig ist, einen E-Mail-Account mit teilweise oder sogar total falschen Angaben bei Anbietern wie web.de oder gmx.de zu beantragen und gleichzeitig deren Allgemeinen Geschäftsbedingungen

zuzustimmen. Die rechtlichen Folgen könnten das gesamte Projekt in Frage stellen."

Prof. Norbert Breier
Universität Hamburg, Fakultät für Erziehungswissenschaft, Psychologie und Bewegungswissenschaft, Fachbereich 5 / Didaktik der Informatik, Binderstraße 34, 20146 Hamburg, http://www.erzwiss.uni-hamburg.de/personal/breier

„Ein Ausweg wäre es, einen E-Mail-Account unter einem fiktiven Namen bei googlemail anzulegen, da google die Nutzung seiner Dienste unter Pseudonym ausdrücklich zulässt. Auch andere Dienste z.B. soziale Netzwerke müssen die Nutzung unter Pseudonym zulassen (§ 13 Abs. 6 Telemediengesetz). Geschäftsbedingungen, die dagegen verstoßen, sind unwirksam und müssen vom Nutzer nicht beachtet werden. Dies trifft insbesondere auf Facebook zu, wo man sich entgegen den Geschäftsbedingungen unter falschem Namen anmelden darf, ohne einen Rechtsverstoß zu begehen."

Prof. Dr. Johannes Caspar
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6, 20095 Hamburg, E-Mail: Johannes.Caspar@datenschutz.hamburg.de

„Die Daten von realen Personen als Negativ-Beispiele zu nutzen stellt meiner Ansicht nach eine Bloßstellung dieser Personen dar. Im ungünstigsten Fall könnten sich darunter sogar Personen aus dem Umfeld der Schüler befinden – welcher Lehrer kennt alle Bekannten oder Freunde seiner Schüler und könnte diese Situation ausschließen? Die Schüler sollen den verantwortungsvollem Umgang mit Daten lernen, sowohl der eigenen als auch der anderer Personen. Reale Beispiele heranzuziehen würde diesem widersprechen, ausgenommen, die Einverständniserklärung der betroffenen Personen wäre eingeholt worden. Es sollte daher mit fiktiven Personen gearbeitet werden.

Ebenso sollte der fiktive Status der genutzten Personen nicht zu Beginn thematisiert werden. Die Frage, ob es im Sinne der Unterrichtseinheit ist, „reale" Personen als Negativ-Beispiele heranzuziehen, kann so im späteren Verlauf der Unterrichtseinheit thematisiert werden. Die Schüler können im realen Internet auf weitere Beispiele realer Personen treffen. Der Umgang mit diesen Informationen muss vom Lehrer genau beobachtet werden. Sollten die Schüler die gefundenen Daten zur Belustigung nutzen, sollte der Umgang damit thematisiert werden. Darüber kann dann auch der fiktive Status der Eingangsbeispiele begründet werden."

Nico Lange
Universität Hamburg, Student der Didaktik der Informatik

„… nicht alle Angaben müssen stimmen …"

Dieser Ausspruch entstammt einem TV-Bericht über dieses Datenschutz-Projekt. Genau diese Situation der Abfrage persönlicher Daten in sozialen Netzwerken und anderen Internet-Diensten bietet gerade einen idealen Ansatz zum Gespräch mit den Schülern über die Pflicht zur Ehrlichkeit und Wahrhaftigkeit einerseits und andererseits der Notwendigkeit des Daten- und Persönlichkeitsschutzes. Mit den Schülern kann hier gemeinsam überlegt und erprobt werden, wie eine Eingabe persönlicher Daten erfolgen könnte. Welche Daten müssen wahrhaftig sein, welche Daten können verkürzt oder unkenntlich eingegeben werden und wo kann auf eine Eingabe von Daten ganz verzichtet werden?

„… nicht alle Angaben müssen stimmen …" – Das ist kein Hindernis, das ist eine Chance!

Erprobt wurde in diesem Pilotprojekt auch die Nutzung von speziellen E-Mail-Adressen („Trash-Mail-Adressen"), die keine Rückverfolgung auf den Nutzer erlauben. Diese E-Mail-Adressen sind wiederum den Netzwerk-Betreibern meist bekannt und werden deshalb abgelehnt. Unabhängig davon kann den Schülern (und Lehrern!) die Nutzung mindestens zweier E-Mail-Adressen vorgeschlagen werden – eine seriöse E-Mail-Adresse und eine „zum Spielen".

4. Vorbereitung: Fiktive Personen im Internet platzieren

In der Unterrichtseinheit hat sich das Arbeiten mit fiktiven Personen im Internet bewährt, die Schüler konnten diese fiktiven Personen im Internet suchen und dabei verschiedene Techniken und Suchdienste erproben.

Das Herstellen dieser fiktiven Personen erfordert aber Zeit und Technik. Zunächst ist ein Name auszudenken, der möglichst nicht im Telefonbuch zu finden ist. Das Alter, eine fiktive Schule und weitere biographische Daten müssen ergänzt werden. In den unterschiedlichen sozialen Netzwerken könnten wir diese fiktiven Personen mit unterschiedlichen Altersangaben anmelden, richtig wäre 14, in anderen Netzwerken geben wir fälschlicherweise die 18 an. Als E-Mail-Adresse sollte hier jetzt eine neu angelegte Adresse genutzt werden. Notieren Sie sich alle Daten und Kennwörter der Zugänge.

Bevor eine Person in einem Netzwerk, Forum etc. angelegt wird, sollte Sie sich vergewissern, ob ein späteres Löschen auch tatsächlich möglich ist. Die Hürden für die Kündigung einer Mitgliedschaft sind bei den verschiedenen Angeboten unterschiedlich hoch. Schreiben Sie unter diesem Namen dann in öffentliche Blogs, Foren und soziale Netzwerke, meist können Sie nach kurzer Anmeldung zu bestimmten Themen unter „Kommentar schreiben" einen passenden Text eintragen. Achten Sie bitte darauf, dass der Kommentar – auch wenn er fiktiv ist – doch den üblichen Kommunikationsregeln „Netiquette" entsprechen sollte. Nutzen Sie die Netzwerke, für die Sie einen Zugang haben, laden Sie diese fiktive Person mit den fiktiven Daten ein.

Ein reales Photo kann natürlich nicht genutzt werden, eine Photo-Montage ist sehr sinnvoll, aber technisch sehr aufwändig, eine Comic-Figur wäre zu offensichtlich, ich selbst verwende eine Karikatur. Auf Verwertungsrechte Dritter ist zu achten. Hier wird angeregt, die Karikaturen selbst oder durch die Klasse erstellen zu lassen.

Dieser beschriebene Vorgang ist – wenn auch aus pädagogischem Interesse – natürlich gemäß der Geschäftsbedingungen der Netzwerke nicht oder nur eingeschränkt zulässig. Auch die Blog-Betreiber haben teilweise ein ehrliches Interesse an ihrem Thema und möchten es nicht missbraucht sehen. Hier ist Sorgfalt gefordert.

Prüfen Sie diese rechtliche Frage für sich. Unterschätzen Sie dabei auch nicht das „Eigenleben" Ihrer fiktiven Personen im Internet, da andere Nutzer mit Kommentaren und E-Mails darauf reagieren.

„Bei der Erzeugung fiktiver Identitäten sollte auf folgendes geachtet werden:

Eine Verwechslung mit existierenden Personen ist möglichst auszuschließen. Hierzu sollte ein Name gewählt werden, der im Internet nicht präsent ist (mittels Suchmaschinen prüfen!). Entsprechendes gilt für Telefonnummern und Adressen (besser eine Adresse verwenden, an der ein Hochhaus, kein Einfamilienhaus steht - oder gleich eine Hausnummer, die nicht existiert).

Bevor eine Person in einem Netzwerk, Forum etc. angelegt wird, sollte man sich vergewissern, dass ein späteres Löschen auch tatsächlich möglich ist. Die Hürden für die Kündigung einer Mitgliedschaft ist bei den verschiedenen Angeboten unterschiedlich hoch. Wird eine Kündigung z.B. nur auf dem Offline-Weg (Fax o.Ä.) angeboten, besteht die Gefahr, dass die fiktiven Personen nach Abschluss der Einheit im Netz verbleiben.

In besonderen Fällen könnte eine Identität explizit als „fiktiv – für pädagogische / schulische Zwecke bestimmt“ gekennzeichnet werden, um zu vermeiden, dass Dritte zu stark auf die Person reagieren und dabei intime Details über sich selbst offenbaren (sie tun dies dann zwar in eigener Verantwortung, aber bei besonders drastisch angelegten fiktiven Identitäten könnte es sein, dass sie sich dennoch als getäuscht empfinden und sich beschweren).“

Prof. Dr. Johannes Caspar
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6, 20095 Hamburg, E-Mail: Johannes.Caspar@datenschutz.hamburg.de

Sollte Ihnen der Aufwand des Platzierens fiktiver Personen im Internet unangemessen erscheinen, so können Sie die Schüler nach Informationen zu „Prominenten“ oder Stars der Musik-, Film-, Mode-, Politik- oder TV-Szene sammeln lassen, Peinlichkeiten von „Prominenten“ sind ja im Internet genug zu finden. Damit geht zwar der Lerneffekt verloren, dass private Informationen plötzlich öffentlich werden, aber zumindest bekommen die Schüler einen Eindruck über die Vielzahl der Informationen und über die fehlende Privatsphäre dieser „Prominenten“.

Internetseite des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, auf der rechten Seite ist ein Link zu weiteren Projekt-Unterlagen zu finden.

5. Übersicht über die Unterrichtseinheit

5.1. Erste Internet-Recherche (Recherche fiktiver Daten im realen Internet)
Fiktive Personen im Internet
a) Suchen nach Informationen zu fiktiven Personen
b) Liste: Wer darf was sehen?

5.2. Mögliche Ergänzungen
a) Peinliche Bilder
b) Cybermobbing
c) AGB der sozialen Netzwerke
d) Abofalle
e) Passwort-Fishing „Phishing"

5.3. Zweite Internet-Recherche (Recherche realer Daten im fiktiven Internet)
Planspiel „Internet"
a) Planspiel nutzen
b) Nutzungsverhalten auswerten

5.4. Ergebnissicherung
a) Leitfaden: So melde ich mich sicher in sozialen Netzwerken an.
b) „Schüler helfen Schülern": Ihre Schüler erläutern jüngeren Schülern den sicheren Zugang zu sozialen Netzwerken

Bitte wählen Sie unter den Ergänzungen aus dem 2. Abschnitt nur einzelne Themen aus. Nach den umfangreichen Vorüberlegungen und Vorbereitung erfordert nun der nachfolgende Unterricht kaum noch weitere Vorbereitungen.

5.1. Erste Internet-Recherche
(Recherche fiktiver Daten im realen Internet)

a) Suchen nach Informationen zu fiktiven Personen

Die Schüler erhalten den Auftrag, möglichst viele Informationen zu den fiktiven Personen zu sammeln, in dem durchgeführten Unterricht waren es „Anna Sprellner" und „Jan Rettstett". Die Schüler werden vermutlich nur über die gängigen Suchmaschinen wie Google und möglicherweise über die Such-Routinen der sozialen Netzwerke recherchieren, wir müssen sie zusätzlich auf die speziellen Personen-Suchmaschinen wie www.yasni.de, www.pipl.com, www.123people.de hinweisen.

Die Ergebnisse werden auf Zuruf an der Tafel gesammelt.

Text- und Bildinformationen am Beispiel von www.yasni.de

Die anschließende Auswertung kann nach diesen Arbeitsaufträgen und Fragen erfolgen:

- Nennt Eure Informationen über Anna Sprellner und Jan Rettsteet.
- Nennt davon die Informationen, die Anna und Jan unangenehm sein könnten.
- Würdet Ihr solche Informationen über Euch selbst im Internet veröffentlichen?
- Würdest Du dieses Photo oder diese Information auch im Klassenraum aufhängen?
- Dürfen alle Mitschüler diese Photos kommentieren?

Diese Fragen führen die Schüler von den virtuellen Personen zur eigenen Person zurück. Die Hilfsfrage mit dem „Klassenraum" ist dann angebracht, wenn die Schüler das Internet als „anonym" oder „viel zu groß" für eine Veröffentlichung sensibler Informationen und Photos ansehen.

b) Liste: Wer darf was sehen?

Die gesammelten Informationen und Photos sollen nun strukturiert werden. Einige Schüler wissen, dass sie Informationen und Bilder in den Netzwerken wie Facebook und SchülerVZ als „privat" und damit nicht für alle sichtbar geschaltet werden können. Weiterhin ist ja üblich, bestimmte Informationen und Bilder vertraulich zu halten und nur den Freundinnen und Freunden zu zeigen. Wenn wir als Lehrer die Tabelle vorgeben und in der linken Spalte „Das dürfen … sehen" und die Unterscheidungen „alle" und „niemand" notieren, werden die Schüler das Kriterium „nur meine Freunde" nennen, in meinem Kurs sind die SchülerVZ-Erfahrenen auch auf das Kriterium „auch die Freunde meiner Freunde" gekommen, zu Verschärfung müssen wir als Lehrer bei Bedarf die beiden „nicht"-Kriterien ergänzen. Arbeitsteilig sollen die Informationen notiert und in die Tabelle einsortiert werden. In der Spalte (A) können Daten zu der fiktiven Person aus diesem Unterricht notiert werden, alternativ wären auch „(B) Daten über den Star ...," gemeint sind hier die Informationen zu „Prominenten", die die Schüler in der Internet-Recherche vielleicht alternativ oder zusätzlich gesammelt haben.

Das dürfen... sehen	Daten über Person (A)	Daten über Person (B)	Daten über mich
alle			
nur meine Freunde			
auch die Freunde meiner Freunde			
nicht meine Lehrer			
nicht meine Eltern			
niemand			

5.2. Mögliche Ergänzungen

a) „Peinliche“ Bilder

Dieser Unterrichtsabschnitt ist recht schwierig zu gestalten, denn bei diesen „peinlichen“ Bildern ist die Balance zwischen „noch lustig“ und „nicht mehr akzeptabel“ schwer zu halten. Es ist darauf zu achten, dass das Recht der Betroffenen am eigenen Bild zu wahren ist.

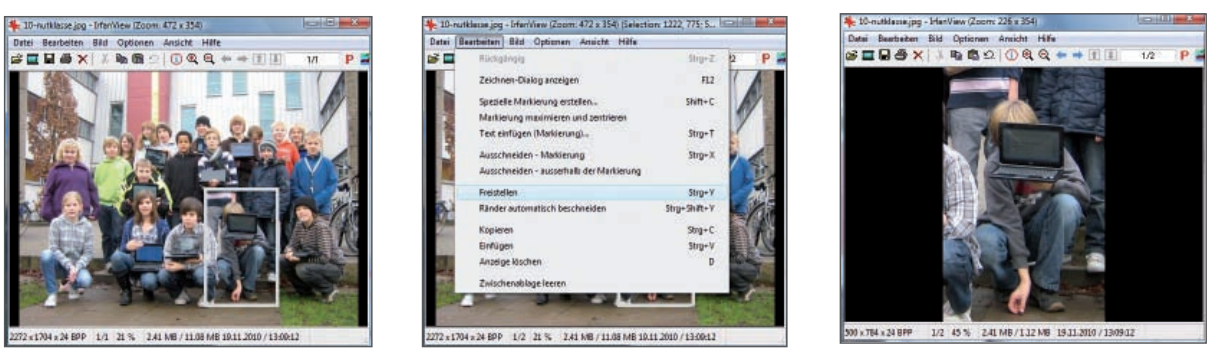
Die Vorbereitung ist einfach. Auch Sie haben von Ihren Klassen und Lerngruppen sicher zahlreiche Digitalphotos, die sie aber nicht weiter verwenden, weil dort einzelne Schüler – in ihren Worten – „blöd gucken“. Für diesen Unterrichtsabschnitt habe ich nun genau diese Bildausschnitte freigestellt und im Unterricht präsentiert.

Die Fragen „Können wir diese Photos auf der Homepage unserer Schule zeigen?“ wurden von den Schülern zunächst aber nicht ernsthaft und reflektiert beantwortet („Mein Photo nicht, aber die anderen Photos sind witzig!“). Die Frage könnte noch verschärft werden „Wollen wir diese peinlichen Bilder im Klassenraum aufhängen?“.

Mit der Frage „Habt Ihr schon davon gehört, dass peinliche Photos von privaten Feiern plötzlich im Internet auftauchen, weil sie irgend ein Party-Gast hoch geladen hat?“ können Erfahrungen von älteren Geschwistern in die Diskussion einbezogen werden.

Photos sind heute über Mobiltelefone „Handy-Kameras“ sofort verfügbar, diese Photos lassen sich dann zusätzlich mit einfachen Programmen verändern und schnell auf die Plattformen sozialer Netzwerke hoch laden. Mit der Verschärfung der Fragen wird bezweckt, das peinliche Bild aus der scheinbaren Anonymität des Internets in die konkrete Umwelt der Schule (Klassenraum, Treppenhaus) oder des eigenen Zuhauses (Wohnung, Straße) zu holen.

Hinweis zur Vorbereitung: So stellen Sie einen Bildausschnitt frei. Sie benötigen ja nicht das vollständige Klassenphoto, lediglich ein Schüler mit unglücklichem Gesichtsausdruck soll frei gestellt werden. Mit den gängigen Grafikprogrammen lassen sich Bildausschnitte mühelos freistellen, hier wird das Freistellen mit dem Programm IrfanView (kostenfrei, www.irfanview.at) gezeigt. Die Bild-Datei wird geladen, mit gedrückter linker Maustaste wird – aus der Sicht des gewünschten Bildausschnitts – von oben links nach unten rechts gezogen, ein Rahmen um den Bildausschnitt entsteht, durch Drücken der Tasten <Strg> und <Y> oder über das Menü **Bearbeiten** und **Freistellen** (siehe Bilder unten) werden die Bildteile außerhalb des Rahmens gelöscht, der Bildausschnitt ist freigestellt und sollte jetzt – mit neuem Datei-Namen – gespeichert werden: **Datei** und **Speichern unter**.



Drei Schritte zum Freistellen eines Bildausschnitts, hier am Beispiel von IrfanView.

b) Cybermobbing

Hier sollten Sie Ihre Schüler befragen, ob eigene Erfahrungen oder Erfahrungen aus dem Bekannten- und Freundeskreis vorhanden sind: „Sind Freunde von Euch schon einmal im Internet beleidigt worden? Sind Freunde von Euch schon einmal mit peinlichen Bildern im Internet blamiert worden?".

Der Begriff „Cybermobbing" lässt sich also vereinfacht beschreiben als Beleidigen und Stimmung-machen zwischen Internet-Nutzern durch beleidigende Texte und durch Veröffentlichen entwürdigender und „peinlicher" Bilder.

Wenn keine konkreten Erfahrungen vorliegen, so bieten sich die Internet-Adressen im Anhang an, die Arbeitsaufträge und Fragen dazu wären:

- Notiere die genannten Beispiele des Cybermobbings.
- Wie würdest Du solche Angriffe auf Dich empfinden?
- Wie würdest Du auf solche Angriffe auf Dich reagieren?
- Notiere mögliche Schutzmaßnahmen gegen Cybermobbing.
- Wem kannst Du Dich anvertrauen?
- Notiere mögliche Hilfsorganisationen.

„Vertrauen" und hier „anvertrauen" sind hier die wichtigen Begriffe, denn eine wichtige Gegenwehr ist das Ansprechen vertrauenswürdiger Personen wie Freunde, Eltern, Lehrer oder – bei besonderem Verdacht – auch der Polizei.

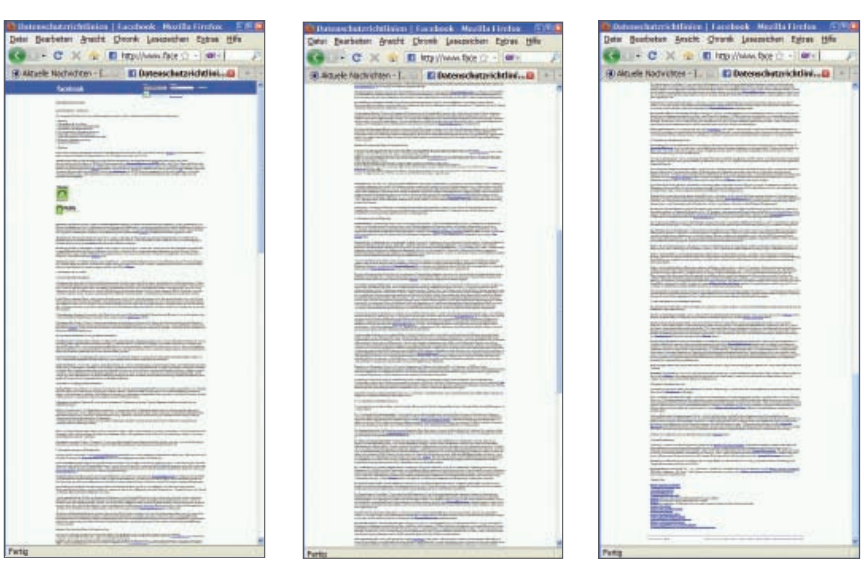
Sollten Sie in Ihrer Lerngruppe beispielsweise in diesem Unterrichtsabschnitt einen konkreten Vorfall des Cybermobbings vermuten oder davon Kenntnis erhalten, so sollte dieser Vorfall sofort außerhalb des Unterrichts mit der Schulleitung oder dem Beratungsdienst besprochen werden, weitere Informationen finden Sie unter den Adressen im Anhang.

c) AGB der sozialen Netzwerke

Auf der Startseite von SchülerVZ finden Sie der Allgemeine Geschäftsbedingungen AGB, bei Facebook entsprechend die Nutzungsbedingungen und Datenschutzrichtlinie. Wenn Sie in dieser Unterrichtsstunde keinen Internet-Zugang nutzen möchten, so finden Sie diese Nutzungsbedingungen auf einem Arbeitsbogen im Anhang.

Die Texte sind klein gedruckt und schwer verständlich, die Arbeitsaufträge und Fragen für die Schüler sind

- Notiere Deine Pflichten beim Schreiben von Texten und Hoch-Laden von Bilder.
- Notiere Deine Rechte, wenn Du Dich von Texten oder Bildern belästigt fühlst.
- Wem gehören die Bilder und Texte, wenn sie hoch geladen sind?



Die Rechte und Pflichten von Facebook – ein sehr langer und schwer verständlicher Text, der deshalb im Unterricht kaum in voller Länge besprochen werden kann. Die Hinweise zum Datenschutz sind dort hingegen übersichtlicher formuliert.

d) Vorsicht vor Abofallen

Auf die Nachfrage eines Schülers hin haben wir im Kurs die „Abo-Fallen“ untersucht.

Abo-Fallen sind Internet-Seiten, die einem Internetnutzer den Bezug kostenloser Software suggerieren und dabei einen seriösen Eindruck erwecken. Nach Eingabe der persönlichen Daten erhält man dann auch diese Software, hat jedoch ungewollt einen Vertrag für ein Abonnement abgeschlossen. Auf diesen Vertrag wird zwar auf der Startseite hingewiesen – allerdings eher am Rande. Eine Umfrage bei Schülern, Eltern und Lehrern (!) zeigte eine überraschend hohe Anzahl an Abofallen-Opfer.

Vorbereitung: Da sich die Ergebnisse der Suchdienste wie Google in diesem Bereich mindestens wöchentlich ändern, muss am Tage vor dem Unterricht noch einmal der genaue Suchbegriff geprüft werden. Das Suchergebnis – zum Beispiel von „antivir download“ – muss kostenfreie und kostenpflichtige (Abofallen, meist sponsored links) aufzeigen. Das kann sich aber auch schon wieder geändert haben und die Abofallen tauchen in der Liste der Suchergebnisse erst weiter unten auf. Bitte notieren Sie sich gegeben falls die Adresse dieser Abofalle. Direkt vor der Stunde müssen also der Suchdienst und die genaue Schreibung des Suchbegriffes geprüft werden.

Ausgehend von der allgemeinen Frage, wie und wo im Internet kostenlose Programme zum Download zur Verfügung stehen, werden verschiedene Möglichkeiten gezeigt. Bei einem intuitiven Zugang über einen Suchdienst wie google.de oder yahoo.de zum Beispiel mit dem Suchbegriff „antivir free download“ wird eine Vielzahl von Internetadressen und damit von Download-Möglichkeiten angegeben. Einige Adressen führen zu „sicheren“ Seiten, andere in „Abofallen“.

Die Schüler erhalten jetzt zwei Arbeitsaufträge:

- Vergleicht die Abofalle mit einer sicheren Download-Adresse, was ist gleich und worin unter scheiden sie sich?
- Findet Informationen zu dem Abonnement (Kosten, Dauer, …) und notiert alle Angaben zu der Firma, die diese Abofalle betreibt.

Eine sinnvolle Arbeitsform ist die Arbeit in Partner-Gruppen, in der ein Schüler eine Abofalle (vermutlich sponsored link) anwählen und ihr folgen soll. Der andere Schüler einer sicheren Download-Adresse folgen soll. Die Informationen zum zweiten Arbeitsauftrag finden sich in den AGB Allgemeine Geschäftsbedingungen.

Zum ersten Arbeitsauftrag lassen sich folgende Ergebnisse finden:
Abofallen sind häufig oben in der Trefferliste des Suchdienstes, aber farbig als sponsored link markiert. Die Abofallen sehen meist seriös aus und verwenden ähnliche Farben und ähnliches Bildschirm-Layout wie die offiziellen Seiten. Die richtigen Download-Links verweisen häufig auf sichere Server wie CHIP, PC-Welt, Heise, Computer-BILD, ….

Die Schüler finden einen wesentlichen Unterschied zwischen sicheren und unsicheren Angeboten heraus und müssen ihn formulieren: „Bei der Abofalle muss man erst seine Daten angeben und erhält dann vielleicht das Programm, bei dem sicheren Link kann man das Programm herunterladen und kann freiwillig seine Daten angeben, das Programm funktioniert aber auch ohne Angabe persönlicher Daten. Auf einer sicheren Seite müssen keine Daten eingegeben werden.“

Auch bei sicheren Download-Adressen sind allerdings zwei Missverständnisse seitens der Schüler möglich: Auf diesen sicheren Seiten werden häufig neben kostenfreien „Basis-“Programmen auch kostenpflichtige Voll- oder „Premium-“Versionen angeboten. Zudem sind manche Software-Angebote für private Kunden frei („Freeware“), für gewerbliche Kunden hingegen kostenpflichtig.
Bei der praktischen Arbeit mit Abofallen taucht wieder die Frage der Ehrlichkeit auf, denn zur Bearbeitung des zweiten Arbeitsauftrag muss das jeweilige Portal erst einmal betreten werden und dazu ist die Eingabe von Daten nötig – sinnvollerweise von falschen Daten. Sinnvoll ist hier die Vorab-Festlegung dieser Daten, möglicherweise müssen die Schüler mit unterschiedlichen fiktiven E-Mail-Adressen arbeiten.

Der zweite Arbeitsauftrag kann unterschiedliche Firmennamen und -adressen (Impressum oder Kontakt

oder AGB, teilweise waren es ausländische Adressen) liefern. Die Schüler finden die Kosten, die von diesem Anbieter für eigentlich kostenfreie Programme verlangt werden. In den Jahren 2008 – 2010 konnte ich bei unterschiedlichen Anbietern ein unfreiwilliges 24-Monate-Abonnement mit einem Preis von 96 Euro pro Jahr, die zumeist im Voraus zu zahlen sind, recherchieren. In einem Fall im Jahre 2008 war bei einer solchen Abofalle die Kündigungsfrist sogar nur wenige Stunden bis Mitternacht und die Geschäftsadresse lag in den Vereinigten Arabischen Emiraten. Erfahrungen von Schülern und Kollegen in den Jahren 2008 und 2009 zeigten, dass bei Nichtbeachtung der Rechnung folgendes Verfahren ablief: Wenn nicht gezahlt wird, kommen zwei Mahnungen über 150 und 200 Euro mit Androhungen von Gerichtsverfahren und als dritte Mahnung ein „Vergleichsangebot", mit einer etwas niedrigeren Forderung, danach meldet sich die Firma nicht mehr. Weitere Informationen dazu finden Sie im Internet unter dem Stichwort „Abofalle".

Recherche über eine Abofalle, hier zum Download des eigentlich kostenfreien Programms AntiVir

e) Passwort-Fishing „Phishing"

Phishing werden Versuche genannt, über gefälschte WWW-Adressen an Daten eines Internet-Benutzers zu gelangen. Der Begriff ist ein englisches Kunstwort, das sich an fishing („Angeln", „Fischen"), evtl. in Anlehnung an Phreaking auch password fishing, bildlich das „Angeln nach Passwörtern mit Ködern", anlehnt. Häufig wird das „h" in dem Begriff mit Harvesting erklärt, so dass der Begriff Phishing dann Password harvesting fishing lautet. Es handelt sich meist um kriminelle Handlungen, die Techniken des Social Engineering verwenden. Phisher geben sich als vertrauenswürdige Personen aus und versuchen, durch gefälschte elektronische Nachrichten an sensible Daten wie Benutzernamen und Passwörter für Online-Banking oder Kreditkarteninformationen zu gelangen. Phishing-Nachrichten werden meist per E-Mail oder Instant-Messaging versandt und fordern den Empfänger auf, auf einer präparierten Webseite oder am Telefon geheime Zugangsdaten preiszugeben. Versuche, der wachsenden Anzahl an Phishing-Versuchen Herr zu werden, setzen unter anderem auf geänderte Rechtsprechung, Anwendertraining und technische Hilfsmittel. [Quelle: Wikipedia]

Dieses Thema ist für die Schüler noch abstrakt, da sie noch keine Girokonten, Kreditkarten und Verbraucherkonten führen.

Als kleine Ergänzung gerade im Zusammenhang mit eBay könnte das Thema aber interessant sein, ein Arbeitsbogen dazu „Welcome to eBay – Verify your identity" finden Sie im Anhang, die Fragestellungen dazu sind wieder

- Wer schreibt warum solche E-Mails?
- Woran ist trotz des scheinbar seriösen Aussehens die Fälschung zu erkennen?

Vielleicht haben einige Schüler schon Erfahrungen mit dem Schreiben (HTML, PHP) von Internetseiten und wissen, dass sie die gezeigten eBay-Bilder und VisaCard-Texte problemlos im Internet kopieren und eigene Seiten einbinden können. Bei der Phishing-E-Mail „eBay" ist die Internet-Adresse http://www.dramavarna.com/e verdächtig, weiterhin fehlt ein Schlüssel in der oberen Menüzeile mit Hinweis auf eine SSL-Verschlüsselung, im zweiten Beispiel „VISA Card" finden sich einige Rechtschreibfehler.

Die Schüler sollen sich abschließend überlegen, warum ein ehrliches Unternehmen eine solche Überprüfung mit Eingabe aller Daten schreiben sollte. Es gibt keinen Grund! Richtig, und deshalb würde das Unternehmen solche E-Mails auch nicht schreiben!

5.3. Zweite Internet-Recherche

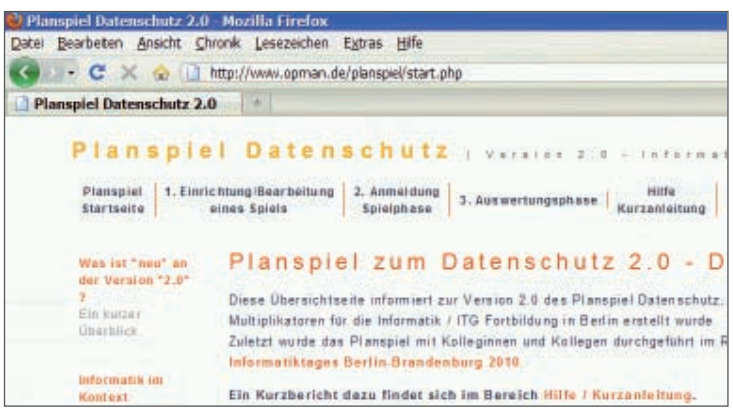
(Recherche realer Daten im fiktiven Internet) – Planspiel „Internet“

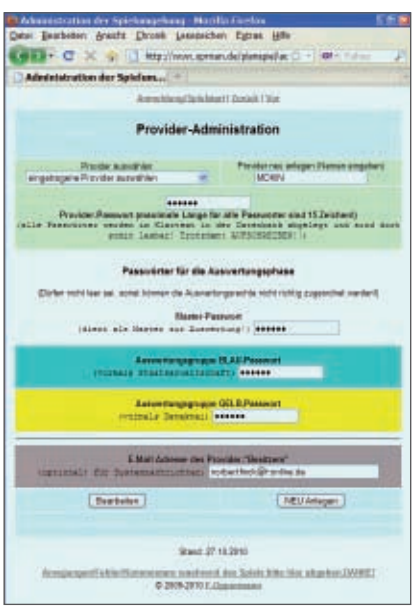
Ich danke der Initiative der Berliner Arbeitsgruppe „Informatik im Kontext“ für den Aufbau und Betrieb dieses sehr hilfreichen Planspiels, das laufend erweitert und modifiziert wird.

Dieser Unterrichtsabschnitt erfordert nur eine kurze Vorbereitung. Laden Sie bitte die Seite http://www.opman.de/planspiel/start.php

Unter „1. Einrichtung / Bearbeitung eines Spiels“ können Sie für Ihre Lerngruppe ein neues Spiel – hier „Provider“ genannt – einrichten. Bitte notieren Sie sich die Kennwörter für die einzelnen Auswertungsstufen, die Kennwörter werden dann im späteren Unterricht nacheinander benötigt. Diese Auswertungsstufen sind die besondere Stärke dieser Lernumgebung, denn im realen Internet haben die Schüler und Sie – außer Sie haben eine eigene Internetseite – nur ein sehr eingeschränktes Lese- und Schreibrecht als Nutzer, viele gespeicherte Daten bleiben bei normaler Nutzung verborgen. Dieses Planspiel als neue Lernumgebung zeigt nun auch diese verborgenen Daten und so werden Protokolle von Internet-Nutzungen und mögliche Nutzer-Profile deutlich.

Die Internetseite www.opman.de/planspiel ist sehr übersichtlich strukturiert, bietet alle Arbeitsbögen zum Download an und hat viele Hilfe-Seiten.





Einrichten eines neuen Planspiels „Provider“ im Planspiel Datenschutz 2.0

Ich empfehle Ihnen nach der Einrichtung eines eigenen Spiels zunächst die Nutzung der vorgefertigten Rollenbeschreibungen, die Sie lediglich kopieren und arbeitsteilig in Ihrer Lerngruppe verteilen müssen. Sollten Sie weniger Schüler als Rollen-beschreibungen haben, so verteilen Sie bitte die Beschreibungen in der Reihenfolge A1, A2, A3, B1, B2, B3, C1,.... Die Rollen mit gleichem Anfangsbuchstaben beziehen sich dann im Planspiel aufeinander. Damit ist aber die Vorbereitung auch schon beendet.

a) Planspiel nutzen

In dieser Unterrichtsstunde sollen die Schüler dieses Modell-Internet „normal“ nutzen, (Chat, Ego-Shooter, Blog, E-Mail, eShop, …). Die Schüler wählen ebenfalls die Seite http://www.opman.de/planspiel/start.php und dann den Menüpunkt „2. Anmeldung Spielphase“ und dann den vorher eingerichteten „Provider“, also das Spiel für diese Lerngruppe. Sie tragen ihre Namen ein und wählen ihre Rollenbeschreibungen aus.

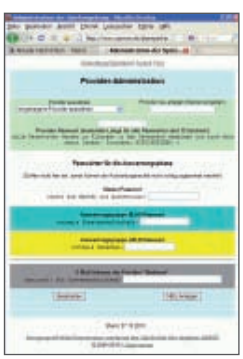
Eine Internet-Nutzung über mehrere Tage soll nachgespielt werden, es gibt jedoch keine realen Spiele (Ego-Shooter), lediglich Spielname und Spieldauer werden eingetragen. Die Schüler sollen sich zunächst eng an die sinnvollen Rollenvorlagen halten.

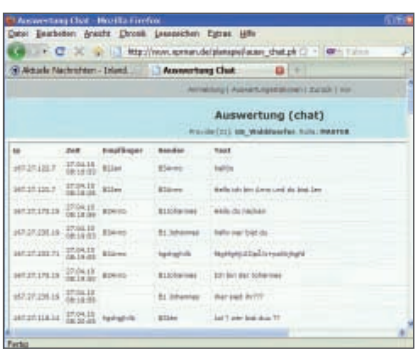
Spielstart des Planspiels Datenschutz 2.0 am Beispiel des Providers MDKIN (Meine Daten kriegt Ihr nicht!)

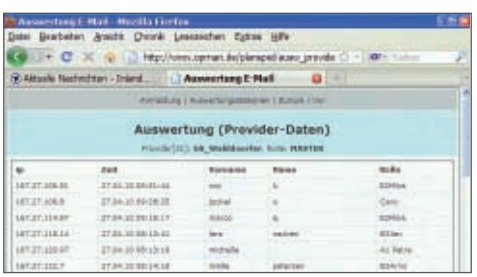
b) Nutzungsverhalten auswerten

In dieser Unterrichtsstunde werden alle Vorgänge recherchiert. Der Nutzer selbst hat vorher kaum einen Einblick, welche Daten-Spuren er hinterlässt. Nun werden sie sichtbar.

Die Schüler laden die Seite http://www.opman.de/planspiel/start.php
und dann den Menüpunkt „3. Auswertungsphase“ und dann den vorher eingerichteten „Provider“. Nun erhalten die Schüler auch die vorher festgelegten Kennwörter für die anderen Rollen. Die Rollen GELB-Detektei und BLAU-Staat sehen schon mehr als der User, die Rolle Master kann auch die genutzten Nick-Namen den jeweiligen Rollen zuordnen. Jeder Eintrag ist zurück zu verfolgen.







Auswertung des Planspiels in der Rolle „Master“, Chat-Protokolle sind sichtbar, Rollen lassen sich zurück verfolgen.

Trotz der voran gegangenen Unterrichtsstunden und trotz der mittlerweile kritischen Grundeinstellung haben meine Schüler gerade im Chat-Bereich recht locker formuliert, beeindruckend für sie war aber, dass alle zunächst den Rollennamen und dann den echten Namen und damit den Schüler identifizieren konnten.

Aus den Rollenvorgaben lassen sich jetzt noch mehrere Aufgaben oder Fälle formulieren:

- Ausbildungsplatz in einer Apotheke. Wer kann anhand der Internet-Daten für diesen Platz genommen werden und wer nicht?
- Diebstahl eines Camcorder‘ aus dem Auto einer Lehrerin. Wer ist anhand der Internet-Daten verdächtig und wer nicht?
- Cybermobbing gegen einen Lehrer
- Cybermobbing gegen eine Schülerin
- Soll ich mich mit dem Jungen aus dem Chat treffen?

5.4. Ergebnissicherung

a) Leitfaden: So melde ich mich in sozialen Netzwerken an.

Für die Schüler ist dieser Leitfaden möglicherweise der erste Text mit eingefügten „Screenshots", also abphotographierten Bildschirm-Bildern. Die Anleitung und der Muster-Leitfaden im Anhang können dabei helfen. Zum Herstellen dieser Leitfäden mit Text und Bild benötigen Ihre Schüler die Kompetenz, die nach Rahmenplan für das Ende der Jahrgangsstufe 6 vorgesehen ist, Bilder in Texte einzubinden. Schwierig für die Schüler, die sich jetzt schon recht sicher im Internet bewegen, ist die adressatengerechte Sprache und Bebilderung dieses Leitfadens, denn der Leitfaden soll später von jüngeren Schülern gelesen und verstanden werden.

Die Schüler sollen die Leitfäden etwa im Umfang von 2-6 Seiten schreiben, jeden Schritt mit einem Bild erläutern und Rechtschreibfehler vermeiden. Kopfzeilen mit Schülernamen, Themen und Seitenzahlen erleichtern die Sortierung der zahlreichen Leitfäden

Die Schüler können nur Leitfäden für die Portale und sozialen Netzwerke schreiben, für die sie Einladungen per E-Mail erhalten haben. Hier hat es sich bewährt, dass sich die Schüler untereinander oder sich selbst – dann aber mit anderem Namen – einladen. Problematisch wären in dieser Unterrichtsphase die wahren E-Mail-Adressen der Schüler, hier müssen sie notfalls auf neue E-Mail-Adressen einrichten und nutzen.

Der Arbeitsbogen 6 im Anhang bietet sich hier für zusätzliche Informationen an, dieser Arbeitsbogen kann aber auch frei in der Unterrichtseinheit auch zur Binnen- differenzierung eingesetzt werden, auch eine arbeitsteilige Gruppenarbeit bietet sich an.

b) „Schüler helfen Schülern"

Ihre Schüler erläutern jüngeren Schülern den sicheren Zugang zu sozialen Netzwerken

Mit einigen technischen Schwierigkeiten, aber insgesamt doch befriedigend hat sich als Abschluss und als Lernerfolgskontrolle bewährt, dass die Schüler dieser Lerngruppe einer jüngeren Lerngruppe den Zugang zu sozialen Netzwerken zeigen. Die Gruppen werden gemischt und haben etwa 30 Minuten Zeit für alle Erklärungen und Vorführungen, hilfreich ist jetzt der angefertigte Leitfaden. Die älteren und erfahrenen Schüler zeigen ihren jüngeren Mitschülern einfach nur das Anmeldeverfahren und dabei die Punkte, an denen sie nicht mehr als nötig persönliche Daten in den Eingabe-Masken der Anmeldung eintragen sollten.

Schüler des NuT-Kurses des Jahrgangs 7 erläutern jüngeren Schülern aus dem Jahrgang 5 den sicheren Zugang zu sozialen Netzwerken

Abschluss-Auswertung

Alle Schülerinnen und Schüler der Lerngruppe haben die gesamte Unterrichtseinheit positiv bewertet, auch wenn sie gerade als Pilot-Gruppe recht lange an dem Thema gearbeitet haben, und sie sagen, dass sie sich jetzt sehr viel bewusster in sozialen Netzwerken bewegen. Das kann ich auch bestätigen, denn ihre SchülerVZ- und Facebook-Seiten enthalten nur unproblematische Informationen und Photos. Das wird wohl auch in Zukunft so bleiben, die Schüler dieser Lerngruppe agieren vorsichtig und sind sicher: „Meine Daten kriegt Ihr nicht !"

6. Anhang

A1: Arbeitsbogen mit Liste „Öffentlich oder geheim – Wer darf im Internet was sehen?“
A2: Arbeitsbogen mit AGB von Facebook „Rechte und Pflichten – Muss ich das wissen?“
A3: Arbeitsbogen „‚Welcome – Verify your identity‘ – Was bedeutet diese E-Mail?“ (Phishing)
A4: Anleitung „‚Screenshots‘ – So fügst Du Bildschirmbilder in Deinen Text ein.“
A5: Muster-Leitfaden „Ein Leitfaden zur Anmeldung – So könnte er aussehen...“
A6: Internet-Adressen zum Datenschutz „Acht tolle Internet-Adressen mit weiteren Tipps“

Informationen auf www.hamburg.de/datenschutz

Zum Projekt „Meine Daten kriegt Ihr nicht!“ finden Sie weitere Informationen und Hintergrundmaterialien auf der Internetseite des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit: www.hamburg.de/datenschutz.

Autor

Norbert Finck (norbert.finck@t-online.de)

Lehrer für Mathematik, Physik, Naturwissenschaft und Technik sowie Informatik
an der Stadtteilschule Walddörfer (ehemals Gesamtschule Walddörfer),
Ahrensburger Weg 30
D-22359 Hamburg-Volksdorf

Fon 040 – 428 854 – 02
Fax 040 – 428 854 – 210.

Projekt „Meine Daten kriegt Ihr nicht !“

Schule: _____ Kurs oder Klasse: _____

Name: _____ Datum: _____

Arbeitsbogen 1: „Öffentlich oder geheim – Wer darf im Internet was sehen?“

Du hast in Deiner Internet-Recherche viele Daten, Informationen und Bilder über die folgenden Personen gesucht, notiere hier Deine Informationen

Person (A): _____

_____

Person (B): _____

_____

Entscheide bei den gesammelten Daten, welche Gruppen (Freunde, Eltern, Lehrer) diese Daten, Informationen und Bilder sehen dürfen (oder auch nicht).

Das dürfen... sehen	Daten über Person (A)	Daten über Person (B)	Daten über mich
alle			
nur meine Freunde			
auch die Freunde meiner Freunde			
nicht meine Lehrer			
nicht meine Eltern			
niemand			

Projekt „Meine Daten kriegt Ihr nicht !“

Schule: _____ Kurs oder Klasse: _____

Name: _____ Datum: _____

Arbeitsbogen 2: „Rechte und Pflichten – Muss ich das wissen?“

Du siehst hier eine Erklärung der Rechte und Pflichten von Facebook-Nutzern (Stand November 2010), die Du auf www.facebook.de findest.

- Fasse diesen Text mit Deinen Worten zusammen.
- Notiere Deine Pflichten beim Schreiben von Texten und Hoch-Laden von Bilder.
- Notiere Deine Rechte, wenn Du Dich von Texten oder Bildern belästigt fühlst.

Die vorliegende Erklärung der Rechte und Pflichten („Erklärung“) beruht auf den Facebook-Grundsätzen und reguliert unsere Beziehung zu den Nutzern und anderen, die mit Facebook interagieren. Mit deiner Nutzung von Facebook oder dem Zugriff darauf stimmst du dieser Erklärung zu.

1. Privatsphäre
Deine Privatsphäre ist uns sehr wichtig. In unseren Datenschutzrichtlinien machen wir wichtige Angaben dazu, wie du Facebook zum Teilen von Inhalten mit anderen Nutzern verwenden kannst, und wie wir deine Inhalte und Informationen sammeln und verwenden können. Wir fordern dich auf die Datenschutzrichtlinien zu lesen und sie zu verwenden, um fundierte Entscheidungen zu treffen.

2. Der Austausch deiner Inhalte und Informationen
Dir gehören alle Inhalte und Informationen, die du auf Facebook postest. Zudem kannst du mithilfe deiner Privatsphäre- und Anwendungseinstellungen kontrollieren, wie diese ausgetauscht werden. Ferner:

2.1. Für Inhalte, die unter die Rechte an geistigem Eigentum fallen, wie Fotos und Videos („IP-Inhalte“), erteilst du uns vorbehaltlich deiner Privatsphäre- und Anwendungseinstellungen die folgende Erlaubnis: Du gibst uns eine nicht-exklusive, übertragbare, unterlizenzierbare, unentgeltliche, weltweite Lizenz für die Nutzung jeglicher IP-Inhalte, die du auf oder im Zusammenhang mit Facebook postest („IP-Lizenz“). Diese IP-Lizenz endet, wenn du deine IP-Inhalte oder dein Konto löscht, außer deine Inhalte wurden mit anderen Nutzern geteilt und diese haben sie nicht gelöscht. (...)

2.4. Wenn du die Einstellung „Alle“ bei der Veröffentlichung von Inhalten oder Informationen verwendest, können alle Personen, einschließlich solcher, die Facebook nicht verwenden, auf diese Informationen zugreifen, sie verwenden und sie mit dir (...) assoziieren. (...)

3.6. Du wirst andere Nutzer weder tyrannisieren noch einschüchtern oder schikanieren.

3.7. Du wirst keine Inhalte posten, die: verabscheuungswürdig, bedrohlich oder pornografisch sind, zu Gewalt auffordern oder Nacktheit sowie Gewalt enthalten. (...)

4.1. Du wirst keine falschen persönlichen Informationen auf Facebook bereitstellen oder ohne Erlaubnis ein Profil für jemand anderes erstellen.(...)

5.1. Du wirst keine Inhalte auf Facebook posten oder Handlungen auf Facebook durchführen, welche die Rechte einer anderen Person oder das Gesetz verletzen.

5.2. Wir können sämtliche Inhalte und Informationen, die du auf Facebook gepostet hast, entfernen, wenn wir der Ansicht sind, dass diese gegen die vorliegende Erklärung verstoßen.

5.3. Wir werden dir Hilfsmittel zur Verfügung stellen, mit denen du deine Rechte an geistigem Eigentum schützen kannst. Mehr dazu erfährst du auf der Seite zum Melden von Beschwerden über eine Verletzung an geistigem Eigentum. (...)

10. Über Werbung und andere kommerzielle Inhalte, die von Facebook zur Verfügung gestellt oder aufgewertet werden
Unser Ziel ist es Werbeanzeigen nicht nur für Werbetreibende sondern auch für dich wertvoll zu gestalten. Damit dies möglich ist, erklärst du dich mit Folgendem einverstanden:

10.1. Du kannst über deine Privatsphäre-Einstellungeneinschränken, inwiefern dein Name und dein Profilbild mit kommerziellen, gesponserten oder verwandten Inhalten (wie z. B. der Marke, die dir gefällt) verbunden werden können, die von uns zur Verfügung gestellt oder aufgewertet werden. Du erteilst uns die Erlaubnis, vorbehaltlich der von dir festgelegten Einschränkungen, deinen Namen und dein Profilbild in Verbindung mit diesen Inhalten zu verwenden.

Projekt „Meine Daten kriegt Ihr nicht !“

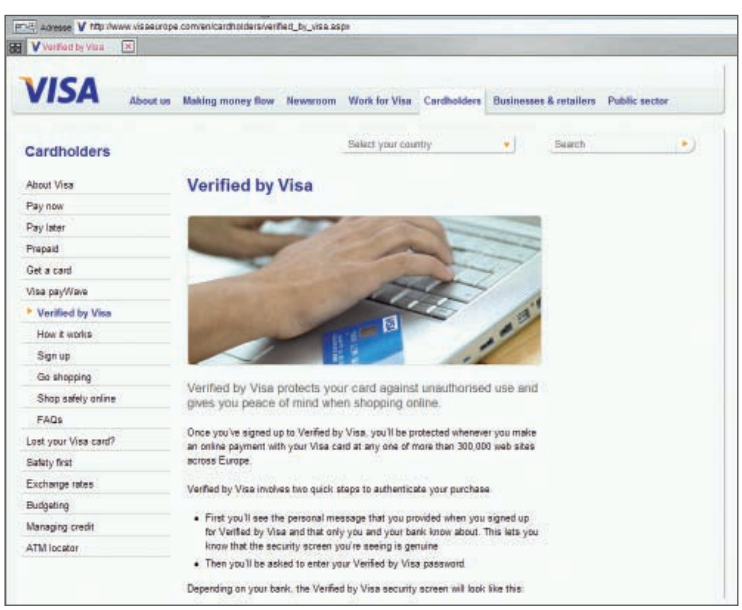
Schule: _____ Kurs oder Klasse: _____

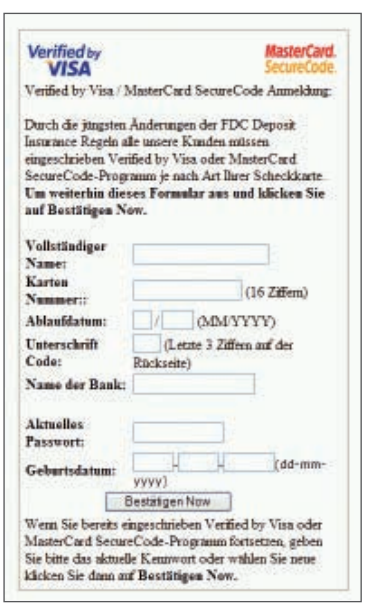
Name: _____ Datum: _____

Arbeitsbogen 3: „Welcome – Verify your identity“ – Was bedeutet diese E-Mail?“

Unten siehst Du zwei gefälschte E-Mails zu eBay (oben) und VISA Card (unten).

- Informiere Dich, welche Dienstleistungen die Firmen eBay und VISA anbieten.
- Informiere Dich (im Internet) und notiere die Bedeutung von „Phishing“.
- Notiere, woran Du trotz des scheinbar seriösen Aussehens die E-Mails und die nachfolgenden Dokumente als Fälschungen erkennen kannst.
- Überlege und notiere: Wer schreibt warum solche E-Mails?





Projekt „Meine Daten kriegt Ihr nicht !“

Schule: _____ Kurs oder Klasse: _____

Name: _____ Datum: _____

Arbeitsbogen 4: „Screenshots – So fügst Du Bildschirmbilder in Deinen Text ein.“

Für Deinen Leitfaden „So melde ich mich sicher in sozialen Netzwerken“ benötigst Du einige Bilder des Bildschirms, damit die Leser Deinen Text besser verstehen können.

Du benötigst lediglich drei Programme:

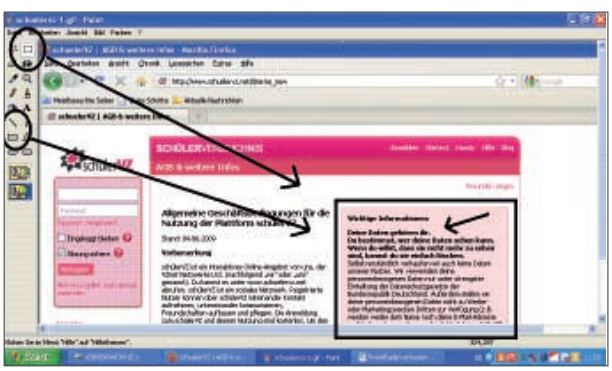
- einen Internet-Browser (Mozilla Firefox, MS Internet Explorer, ..),
- ein Textverarbeitungsprogramm (MS Word, OpenWriter, ...) und
- ein Grafikprogramm (Paint, IrfanView, ...).

Öffne im Internet-Browser die Internet-Seite, an der Du etwas zeigen möchtest (hier: www.schuelervz.net).

Drück auf die Taste <Druck> oder <PrtScr>, die Du auf der Tastatur oben rechts findest.

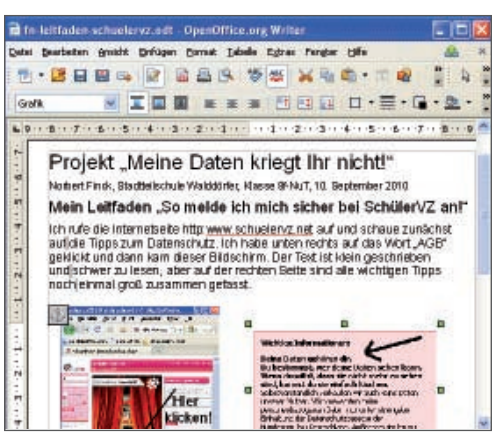
So wird das aktuelle Bildschirm-Bild in die Zwischenablage kopiert und dort zwischengespeichert.

Öffne das Grafikprogramm und wähle im Menü **Bearbeiten** den Punkt **Einfügen** und schon ist das gesamte Bildschirmbild geladen. Du kannst jetzt mit den Werkzeugen „Pinsel“ oder „Linien“ den wichtigen Bildausschnitt hervorheben. Danach wählst Du „Auswahl“ – das Rechteck in der Werkzeug-Leiste – und schneidest um den Bildausschnitt herum.



Nun wählst Du im Menü **Bearbeiten** und **Kopieren.**

Jetzt öffnest Du das Textverarbeitungsprogramm und dort kannst Du diesen Bildausschnitt mit **Bearbeiten** und **Einfügen** in Deinen Text einfügen.



Wenn Du schon etwas sicherer im Umgang mit Textverarbeitungsprogrammen bist, dann kannst Du das Bild mit der rechten Maustaste anklicken, dann **Bild** oder **Grafik** formatieren wählen und die Eigenschaften Umbruch, Umlauf, Anordnung und Verankerung verändern

Projekt „Meine Daten kriegt Ihr nicht !“

Schule: _____ Kurs oder Klasse: _____

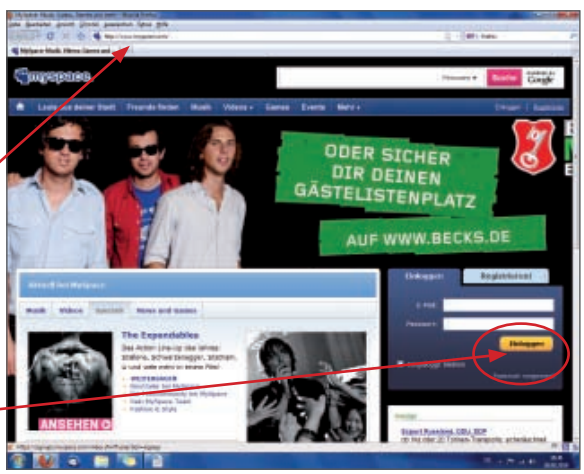
Name: _____ Datum: _____

Arbeitsbogen 5a: „Ein Leitfaden zur Anmeldung – So könnte er aussehen...“

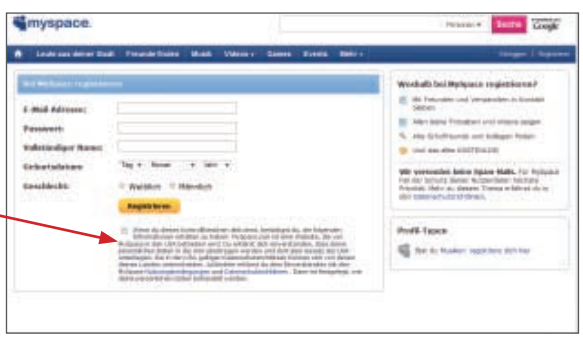
Persönliche Daten bei MySpace

Mit diesem Leitfaden wird gezeigt, wie man MySpace so verwendet, dass die eigenen persönlichen Daten geschützt sind.

Registrierung: Als erstes muss man sich bei MySpace registrieren, um das Angebot nutzen zu können. Dazu gibt man die Adresse „www.myspace.de“ in das Adressfeld des Internetbrowser ein. Anschließend erscheint die Startseite von MySpace, sie könnte etwa so aussehen.



Es muss nun auf „Registrieren“ geklickt werden. Es öffnet sich eine Seite, auf der die persönlichen Daten angeben werden müssen.



Im Kleingedruckten ist zu lesen, dass die persönlichen Daten in die USA übertragen werden und dort andere Datenschutzbestimmungen gelten können als hier in Deutschland. Weitere Angaben zum Datenschutz sind über einen Link in dem Kleingedruckten zu erreichen.

Wir tragen hier lieber nicht unsere echten Daten ein, weil wir **nicht** genau wissen, was dann mit unseren Daten gemacht wird. Als E-Mail-Adresse sollte eine genutzt werden, die auch nicht mit unseren richtigen Personendaten eingerichtet wurde. Wenn alles ausgefüllt wurde, sieht das in etwa so aus: Es muss dann noch auf „Registrieren“ geklickt werden. Daraufhin öffnet sich ein Fenster, indem eine Bestätigung eingetippt werden muss. Dazu sind die Zeichen aus dem Bild in das Feld einzugeben und danach auf „Fortfahren“ zu klicken. Das wird von vielen Anbietern im Internet gemacht, um sicher zu gehen, dass auch wirklich ein Mensch die Anmeldung durchführt und kein Programm – ein Programm könnte die Zeichen in dem Bild nämlich nicht erkennen.

Wir erhalten jetzt über unser Mail-Postfach eine Bestätigung von MySpace. Es öffnet sich später eine Seite, auf der uns gleich einige Angebote gemacht werden, um Freunde hinzuzufügen...

Projekt „Meine Daten kriegt Ihr nicht !“

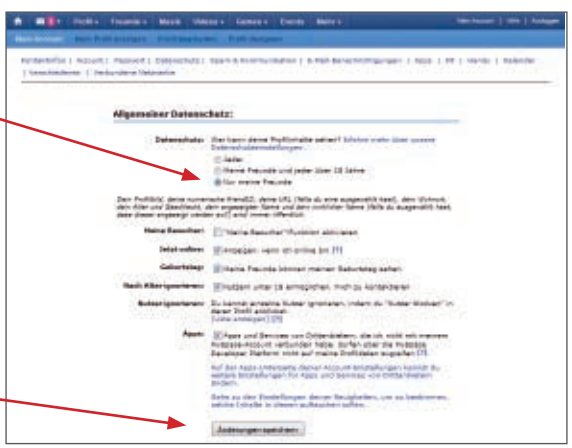
Schule: _____ Kurs oder Klasse: _____

Name: _____ Datum: _____

Arbeitsbogen 5b: „Ein Leitfaden zur Anmeldung – So könnte er aussehen...“

Wichtig ist aber zunächst einmal ein Blick in „Mein Account“ und dort „Datenschutz“.

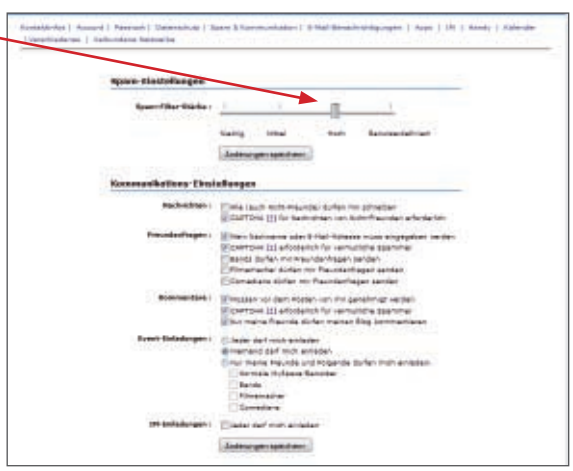
Auf der Datenschutzseite sollten wir zunächst alles nur für Freunde sichtbar machen, das sieht dann etwa so aus.



Bei einigen Punkten gibt es weitere Informationen, wenn wir mit dem Mauszeiger über das Fragezeichen gehen.

Der Punkt „Apps“ am Ende der Datenschutzeinstellungen ist sehr wichtig. Der Haken dort sollte gesetzt sein. Wichtig: Wenn alles eingestellt ist, dann auf „Änderungen speichern“ klicken.

Der nächste Punkt heißt „Spam & Kommunikation“. Die Spam-Einstellungen sollten auf „Hoch“ eingestellt werden, dann speichern.



Der Punkt „E-Mail-Benachrichtigungen“ ist der nächste, den wir uns genauer anschauen. Hier ist zu Beginn alles aktiviert und wir müssen selbst entscheiden, welche Informationen wir per E-Mail erhalten möchten.

Weiter zum Punkt „Apps“. Hier müssen beide Haken **gesetzt** sein, dann „Speichern“.

Weiter geht es zum Punkt „IM“, dahinter verbergen sich die Einstellungen für den Instant Messenger von MySpace.
Unter IM-Datenschutz sollte „Alle meine IM- und MySpace-Freunde“ oder der Punkt „Nur meine IM-Freunde“ markiert sein. Den Kalender sollte ebenfalls niemand sehen. Nicht vergessen: „Änderungen speichern“.

Jetzt ist alles eingestellt, das Profil können wir dann weiter nach unseren Vorstellungen anpassen. Wichtig ist, dass wir keine peinlichen Fotos veröffentlichen, überhaupt dürfen wir keine Fotos von anderen ohne deren Erlaubnis online stellen.

Projekt „Meine Daten kriegt Ihr nicht !“

Schule: _____ Kurs oder Klasse: _____

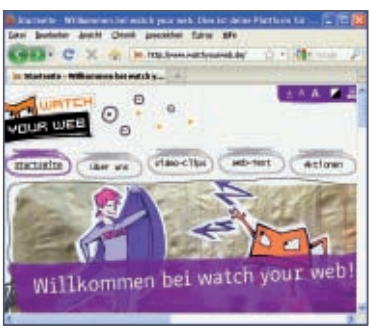
Name: _____ Datum: _____

Arbeitsbogen 6 :„Acht tolle Internet-Adressen mit weiteren Tipps“

Teste die folgenden Internet-Adressen,
dort findest Du wichtige Tipps und interessante Geschichten und Videos.

www.klicksafe.de

www.watchyourweb.de



www.netzcheckers.de

www.time4teen.de

www.datenparty.de

www.123hier.de

www.netzdurchblick.de

www.handysektor.de

Thomas Fuchs
Direktor der Medienanstalt Hamburg/Schleswig-Holstein (MA HSH)

7. Was es sonst noch gibt:

Weitere Medienkompetenzprojekte der Medienanstalt Hamburg / Schleswig-Holstein (MA HSH)

Datenschutz ist ein Aspekt der Medienkompetenzförderung, die von der Medienanstalt Hamburg / Schleswig-Holstein (MA HSH) als gesetzliche Aufgabe vorangetrieben wird. Wir setzen auf Medienkompetenz als präventive und damit wirksamste Form des Jugendmedienschutzes. Denn die Risiken für Kinder und Jugendliche im Internet sind evident, eine lückenlose Aufsicht über dieses Medium ist jedoch unmöglich und repressive Kontrolle stößt hier rasch an ihre Grenzen.

Medienkompetenz, die „vierte" Kulturtechnik, hat zudem starken Einfluss auf die Bildungschancen, die sich Schülerinnen und Schülern eröffnen. Wir möchten deshalb, dass sie selbstbestimmt und eigenverantwortlich mit dem World Wide Web umgehen können. Dazu gehört auch, dass sie die Chancen des Internets schrittweise aktiv und partizipierend nutzen.

Die MA HSH bietet Schülerinnen und Schülern, aber auch Eltern und Lehrkräften vielfältige Projekte zur Medienkompetenzförderung an. Die von uns entwickelten und finanzierten Qualifikationsangebote werden in der Regel von Dritten durchgeführt. Wir suchen dabei gezielt die Kooperation mit medienpädagogischen Einrichtungen, Vereinen, Initiativen und anderen Institutionen.

Insbesondere auf folgende Projekte möchte ich Sie aufmerksam machen:

Eltern-Medien-Lotsen
Viele Eltern stehen den neuen Medien ratlos gegenüber. Eltern-Medien-Lotsen beraten auf Elternabenden oder in Sprechstunden an Schulen und orientieren Erwachsene im virtuellen Dschungel. Suchen Sie einen Eltern-Medien-Lotsen, der eine Informationsveranstaltung an Ihrer Schule durchführt? Die passenden Lotsen werden in Hamburg von der TIDE-Akademie vermittelt. Weitere Informationen unter:
www.tidenet.de/akademie/elternmedienlotse/elternmedienlotse.html
oder Telefon 040 / 325 99 03-60

Aktion Sicheres Internet
Die Aktion Sicheres Internet qualifiziert Multiplikatoren wie Lehrerteams und Elternvertretungen in den Bereichen Internet, Handy und Computerspiele. In drei Informationsveranstaltungen wird über Risiken aufgeklärt und auf pädagogische Handlungsmöglichkeiten hingewiesen. Die Referenten für diese Fortbildungsveranstaltungen können Sie bei der MA HSH kostenlos abrufen.

Telefon 040 / 36 90 05-46, E-Mail medienkompetenz@ma-hsh.de.

PIF! - PC- und Internetführerschein
PC und Internet sind Teil der Lebenswelt von Kindern. Der PIF! qualifiziert 8- bis 13-Jährige, diese Medien sinnvoll und mit Freude zu nutzen und dabei auch den Aspekt der Sicherheit nicht außer Acht zu lassen. Das kostenlose Angebot richtet sich an Kinder in Kitas, Hortgruppen, Grund- und weiterführenden Schulen (Klassen 4 bis 6). Die technische Ausstattung wird mitgebracht. Für Absprachen wenden Sie sich bitte an die Projektleitung unter Telefon 040 / 370 80-171.

Schüler machen Medien - Schnappfisch-Media
Schnappfisch ist das Jugend-Medien-Projekt von TIDE, dem Hamburger Bürger- und Ausbildungskanal. Schülerinnen und Schüler erarbeiten eigene Beiträge für Radio, Fernsehen und Internet. Von Profis angeleitet recherchieren sie Themen, führen Interviews, filmen, führen Umfragen durch und schneiden am Ende das Material für einen Hörfunk- bzw. Fernseh-Beitrag, der dann ausgestrahlt wird. Das Projekt wird von der Hamburger Behörde für Schule und Berufsbildung (BSB) und der MA HSH gefördert.

Weitere Informationen unter: www.schnappfisch.net

netzdurchblick.de
Ohne pädagogischen Zeigefinger unterstützt die Internetseite netzdurchblick.de 12- bis 16-jährige Jugendliche bei einem reflektierten und gezielten Umgang mit dem Internet, unter anderem im Hinblick auf Themen wie Preisgabe privater Daten, Wahrheitsgehalt medialer Informationen, Rechtsfragen beim Download von Musik und Videos, Cybermobbing oder Umgang mit Viren und Spam. Die Plattform wird ab 2011 ergänzt durch Trainingsmodule in Schulen, Bücherhallen und Jugendzentren. Neugierig geworden?

Nähere Informationen unter: www.netzdurchblick.de/

Neben diesen konkreten Projektangeboten kooperieren wir als MA HSH mit den hiesigen Universitäten, Behörden und weiteren Einrichtungen. Wir unterstützen dabei insbesondere die Vernetzung von schulischen und außerschulischen Aktivitäten im Bereich der Medienkompetenzförd erung. Weitere Hinweise, auch auf neue Projekte, finden Sie auf unserer Homepage: www.ma-hsh.de/medienkompetenz.

Kontakt

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6
20095 Hamburg
Tel.: 040/42854-4040 (Geschäftsstelle)
Fax: 040/42854-4000, E-Fax: 040/427911-806

Layout: KAMEKO Design Gbr
Titelfoto: Thomas Krenz
Die Fotos im Innenteil wurden von den beteiligten Institutionen zur Verfügung gestellt
Druck: Günter Plaut Offsetdruckerei GmbH
Diese Publikation kann auch unter www.datenschutz.hamburg.de im Pdf-Format heruntergeladen werden.

Ein Gemeinschaftsprojekt von:

Hamburg | Behörde für Schule und Berufsbildung

POLIZEI Hamburg

NDR

MA HSH

LI HAMBURG

HmbBfDI