# Schutz der Privatsphäre im Internet

Arbeitsmaterialien für den Unterricht
Aus der Reihe: IT-Sicherheit macht Schule in Nordrhein-Westfalen

Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

**Impressum**

Herausgeber:
Agentur »secure-it.nrw«
bei der IHK Bonn / Rhein-Sieg
Bonner Talweg 17
D-53113 Bonn
Telefon: +49 (0) 228 / 2284 - 184
Telefax: +49 (0) 228 / 2284 - 5184
E-Mail: info@secure-it.nrw.de
Internet: www.secure-it.nrw.de
www.branchenbuch-it-sicherheit.de

In Zusammenarbeit mit:
Landesbeauftragte für Datenschutz
und Informationsfreiheit Nordrhein-Westfalen (LDI NRW)
www.ldi.nrw.de

Autor: Wolfgang Dax-Romswinkel
Redaktionelle Bearbeitung: Manfred Kasper,
Journalismus und PR
Gestaltung: Conny Koeppl, viceversa Köln
Bildnachweis: www.istockphoto.com, www.photocase.com

# Schutz der Privatsphäre im Internet

Arbeitsmaterialien für den Unterricht
Aus der Reihe: IT-Sicherheit macht Schule in Nordrhein-Westfalen


## Thematisch-didaktische Einführung für Lehrkräfte

Die im Folgenden aufgeführten Materialien stellen ein Angebot für Lehrkräfte aller Schulformen dar. Sie geben den Stand von August 2008 wieder. Dieser Hinweis ist notwendig, weil nichts rascher fortschreitet als die Entwicklung und das Wissen im Bereich der Informationstechnologie.

Die Materialien eignen sich für den Unterricht aller Schulformen ab Klasse 8 in den Fächern bzw. Lernbereichen Ethik, Informatik, Medienbildung, ökonomische Bildung, Politik und Sozialwissenschaften. Sie können als Hilfe für den Ersteinstieg ins Thema oder zur Vertiefung, beispielsweise in Schülerreferaten, genutzt werden.

Die vorliegenden Arbeitsmaterialien dienen als Kopiervorlage. Als Erläuterung zu Fachbegriffen bietet die Landesinitiative »secure-it.nrw« auf ihrer Website (www.secure-it.nrw.de) ein Glossar an. Hier finden Sie auch Verweise auf weitere Links zum Thema.

## Das Thema: Schutz der Privatsphäre im Internet

Zunächst einmal gilt es, die Begriffe „Datenschutz“ und „Datensicherheit“ zu unterscheiden. Während es bei der Datensicherheit um den Schutz wichtiger Daten geht, stehen beim Datenschutz die Rechte einzelner Personen an ihren Daten im Mittelpunkt.

Dies ist besonders wichtig, da wir uns auf dem Weg in eine Informationsgesellschaft befinden, in der das Recht auf die freie Entfaltung der Persönlichkeit nicht eingeschränkt werden darf. Der Datenschutz gibt jedem von uns Möglichkeiten an die Hand, sich selbst um den Schutz der Privatsphäre zu kümmern. Denn schließlich ist das Internet kein rechtsfreier Raum. Fühlt man sich durch einen verantwortungslosen Umgang mit persönlichen Daten im Internet betroffen, ist jede Bürgerin und jeder Bürger berechtigt, sich an die Landesbeauftragten für Datenschutz und Informationsfreiheit oder an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zu wenden.

## Datensammler sind überall

Als es noch keine elektronische Datenverarbeitung gab, waren alle personenbezogenen Informationen über Bürgerinnen und Bürger auf Papier gespeichert und meist in Archiven gelagert. Familiendaten, Zeugnisse oder Rechnungen wurden an verschiedenen Stellen von verschiedenen Menschen getrennt verwaltet. Weil alles auf Papier geschrieben stand, war es kaum möglich, Querbezüge herzustellen. Dazu bedurfte es in jedem Fall einer intensiven Nachforschung an unterschiedlichen Stellen. Jede dieser Stellen hatte damals wie heute Vorschriften über die Vertraulichkeit der Informationen.

Mit der wachsenden Bedeutung des Computers hat sich vieles verändert: So ist über jeden von uns eine unglaubliche Datenfülle in zentralen Computersystemen abgespeichert. Würde man diese Daten zusammenführen, so ergäben sie ein umfassendes Bild unserer Person und unserer Gewohnheiten. Dazu einige Beispiele:

- die Kreditkartenrechnung verrät, in welchen Geschäften wir gerne einkaufen, welche Restaurants wir bevorzugen, wo wir tanken und vieles mehr;
- die Telefonrechnung liefert einen Überblick darüber, mit wem wir lockeren und mit wem wir intensiven Kontakt haben;
- wer mit eingeschaltetem Handy unterwegs ist, kann jederzeit lokalisiert werden;
- Suchmaschinen ermöglichen es, aus den Informationen im Internet ein Persönlichkeitsprofil zusammenzustellen.

Die Palette der Beispiele ließe sich fast beliebig fortsetzen: von Krankheitsdaten über elektronische Terminkalender bis hin zu E-Mails. Auf unterschiedlichste Art und Weise werden so wichtige Informationen über jeden von uns preisgegeben.

Diese sind vor allem für zwei Gruppen interessant:

1. für den Staat, z.B. die Finanz- oder Strafverfolgungsbehörden bzw. die Geheimdienste;
2. für die Wirtschaft, die die Informationen zu Werbe- und Marketingzwecken verwendet.

## Wie anonym ist das Internet wirklich?

Ziemlich hartnäckig hält sich die Vorstellung, dass Menschen das Internet im Verborgenen und somit auch anonym nutzen. Sicherlich ist es so, dass Kommunikationspartner, beispielsweise in Chats, Newsgroups, Communities oder Foren, nicht so ohne weiteres ermittelt werden können, dennoch ist das Internet keineswegs ein anonymer Raum. Wo und wie wir beim Surfen im Internet Spuren hinterlassen und welche Informationen dabei über uns gespeichert werden, verdeutlichen die Übungen im zweiten Teil der Arbeitsmaterialien.

Zum einen geht es dabei um so genannte Logfiles. Denn jeder Aufruf einer Seite wird mitprotokolliert und ist so letztlich identifizierbar. In den Arbeitsmaterialien erfahren die Schülerinnen und Schüler, was technisch alles möglich ist und welche rechtlichen Grenzen es gibt.

Während wir bei Logfiles selbst entsprechende Spuren im Netz hinterlassen, greifen Cookies, aktive Inhalte und Spyware auf unseren Rechner zu. So werden Daten über uns bekannt, die eigentlich nicht bekannt werden sollten. Denn hinter „Cookies“ verbirgt sich etwas völlig anderes als der Name verspricht. Was zunächst nach süßen Leckereien klingt, sind in Wirklichkeit Spionage-Dateien, die ein Rechner beim Surfen auf die Festplatte schreibt. Besuchen wir bestimmte Seiten erneut, werden sie wieder ausgelesen. In der Werbebranche hofft man mit Cookies Informationen darüber zu bekommen, welche Leute welche Internetseiten besuchen.

Von einem anonymen Internet kann also eigentlich keine Rede sein.

## Schutz der Privatsphäre im Internet als Unterrichtsthema: Hinweise für Lehrerinnen und Lehrer

Die Ausführungen dieser Arbeitshilfe sind als Einstieg in die Thematik gedacht. Die Aufgaben knüpfen an die Einführungstexte an. Sie setzen bei den Schülerinnen und Schülern eine relativ hohe Internetkompetenz sowie ein technisches Grundverständnis voraus.

Prinzipiell kann gesagt werden: Fragen des Datenschutzes im Allgemeinen und des Schutzes der Privatsphäre im Besonderen eigenen sich hervorragend als Themen für Referate mit anschließender Diskussion. Vor diesem Hintergrund erscheint die Arbeit in gemischten Gruppen, in die die einzelnen Schülerinnen und Schüler unterschiedliche Kompetenzen einbringen, besonders sinnvoll.

In jüngster Zeit sind insbesondere die sozialen Netzwerke bei Jugendlichen immer beliebter geworden und verdienen daher besondere Aufmerksamkeit.

Die folgenden Links eignen sich zur thematischen Vertiefung sowie zum Verständnis von technischen und inhaltlichen Zusammenhängen hinsichtlich des Datenschutzes im Internet. Fast alle Arbeitsaufträge können mit Hilfe der Links ausgeführt werden:

**www.datenschutz.de**
Das virtuelle Datenschutzbüro – ein umfangreiches Portal zum Datenschutz mit zahlreichen Links zu Datenschutzorganisationen und vielen interessanten Websites. Hier findet sich auch ein Link zur Seite der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen: www.ldi.nrw.de sowie zur Seite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (www.bfdi.bund.de).

**www.bsi-fuer-buerger.de**
Das Bundesamt für Sicherheit in der Informationstechnik hat ein eigenes Angebot für Nicht-Techniker zusammengestellt. Es bietet leicht verständliche Informationen und vor allem auch Tipps zu Konfiguration und Verhalten.

**www.heise.de**
Der Heise-Verlag liefert mit seinen Angeboten c't, Security und Telepolis technische Hintergrundinformationen, die teilweise „ans Eingemachte" gehen und ein Muss für Experten sind. Auch der Laie findet hervorragende Quellen. Herausragend sind das Download-Archiv www.heise.de/software und die Angebote zum Browser- und E-Mail-Check.

**www.hirnbrauser.de**
Der „Hirnbrauser" zeigt, welche Informationen über jeden von uns gesammelt werden können. So sollte man sich nicht wundern, wenn man seinen Standort, die Konfiguration der Grafikkarte oder andere Informationen über seinen Rechner plötzlich in seinem Browser ablesen kann. Der „Hirnbrauser" verrät auch, wie man sich davor schützen kann, dass diese Informationen per E-Mail mühelos und unbemerkt an andere verschickt werden.

**www.gurusheaven.de**
Auf Gurusheaven werden alle in dieser Schrift behandelten Fragen vertiefend erläutert und auch Gegenmaßnahmen empfohlen. Sehr lesenswert.

**www.knopper.net**
KNOPPIX ist ein komplettes Linux-Betriebssystem, das per CD oder DVD startet und ein sicheres Surfen im Internet ermöglicht. Fährt man KNOPPIX wieder herunter, so hinterlässt es keinerlei Spuren auf der Festplatte. Während des Surfens kann also nichts aus dem PC ausgelesen werden, ein Speichern auf dem System ist ebenso wenig möglich.

**www.firefox-browser.de**
Firefox ist der aktuelle Browser der Mozilla-Foundation. Er ist schnell, sicher und stabil und bietet vieles, das sich Nutzer des Internet-Explorers schon immer gewünscht haben, wie z.B. wirksame Werbeblocker. Firefox gibt es für Windows, Linux, Mac OSX und einige andere Betriebssysteme.

**www.wikipedia.de (alternativ: de.wikipedia.org)**
Die freie Enzyklopädie im Internet ist die erste Adresse für wissbegierige Surfer. Zu jedem der hier verwendeten Fachtermini gibt es auf Wikipedia die passende, verständliche Erklärung.
Da jeder Nutzer auch Informationen in Wikipedia einstellen kann, sollte man diese vor Verwendung noch einmal überprüfen.

**www.irights.info**
Das unabhängige Informationsportal zu allen Rechtsfragen für Internetnutzer zeichnet sich durch erstklassige Informationen aus, die außerdem sehr verständlich aufbereitet werden.

**www.klicksafe.de**
Hinter Klicksafe verbirgt sich eine umfangreiche Initiative zur Verbesserung der Internetsicherheit und der Medienkompetenz. Sie wird im Auftrag der europäischen Kommission von der Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz, der Landesanstalt für Medien Nordrhein-Westfalen (LfM) und dem Europäischen Zentrum für Medienkompetenz (ecmc) getragen.

# Arbeitsmaterialien für den Unterricht

## Thema Logfiles und Zugangsdaten

### Wie du den Abrufer einer Webseite ermitteln kannst

Nehmen wir einmal an, wir würden ein Diskussionsforum betreiben und einer unserer User würde dort per Posting eine strafbare Handlung begehen. Dies könnte eine massive Beleidigung, eine Volksverhetzung oder der Aufruf zu einer Straftat sein. Wie können wir nun den Täter ermitteln?

Auf jedem Webserver können alle Zugriffe in sogenannten Logfiles gespeichert werden. Hier ein fiktives und leicht abgewandeltes Beispiel:

| | |
|---|---|
| **IP-Adresse:** | **217.95.181.179** |
| **Datum/Zeit:** | **[07/Oct/2004:11:11:57 +0200]** |
| **Befehl:** | **„GET forum/index.html HTTP/1.1“** |
| **Referer-URL:** | **„http://www.google.de/search?hl=de &q=forum%2C+”Juden in Bonn“** |
| **Browser:** | **„Mozilla/4.0 (compatible; MSIE 5.5; Windows 98)“** |

Zunächst einmal erfahren wir Datum und Uhrzeit sowie die IP-Adresse des Aufrufenden. Hinter der IP-Adresse verbirgt sich die Internet Protocol-Adresse, eine eindeutige Nummer, die jeden Computer im Internet identifizierbar macht. Danach folgen noch zwei weitere wichtige Informationen: welche Datei abgerufen wurde (Befehl GET) und über welche Seite der Besucher kam. Schließlich erfahren wir auch noch etwas über den verwendeten Browser und das Betriebssystem.

Anhand der Informationen können wir nun jeden Dateizugriff des Besuchers auf unserem Webserver nachverfolgen. Wir müssen seine Daten nur aus dem Logfile filtern und auswerten. Dazu gibt es verschiedene Programme, im Zweifel reicht jede Tabellenkalkulation aus.

Nun wissen wir jedoch noch nicht, wer sich konkret hinter der IP-Adresse verbirgt. In aller Regel wird einem Nutzer bei der Einwahl ins Internet eine IP-Adresse dynamisch – das heißt vorübergehend – von seinem Zugangsprovider zur Verfügung gestellt. Alle Provider verfügen über einen Adressbereich, in dem festgestellt werden kann, über welchen Anbieter der Besucher ins Internet gegangen ist. In unserem Fall handelt es sich um einen Nutzer von T-Online.

Bei den Providern werden die Zugangsdaten ebenfalls gespeichert – allein schon, um die Internetnutzung mit den Kunden abrechnen zu können. Dort benötigt es nur wenige Mausklicks, um festzustellen, welcher User am 7. Oktober 2004 um 11.11 Uhr und 57 Sekunden die IP-Adresse 217.95.181.179 zugewiesen bekommen hatte.

Das heißt: Durch die Kopplung von Server-Logfiles und Providerdaten lassen sich die Besucher von Internetseiten ermitteln. Dies gilt nicht bei der Verwendung von zwischengeschalteten Proxy-Servern. Da diese in der Regel jedoch auch „gelogged“ werden, ist die Ermittlung des Users in solchen Fällen zwar aufwändiger, aber nicht unmöglich.

Gesetzliche Regelungen verbieten das jedoch in den meisten Fällen – oder anders herum ausgedrückt: Nur in bestimmten Fällen ist dies zulässig, zum Beispiel bei der Verfolgung von Straftaten.

Die Zugangsdaten der Provider dürfen außerdem nur für einen begrenzten Zeitraum gespeichert werden. Auf der anderen Seite müssen die Daten den Strafverfolgungsbehörden zugänglich gemacht werden, wenn dies erforderlich ist. Im Grunde haben wir hier die typische Situation des Anspruchs von Bürgerinnen und Bürgern auf den Schutz ihrer Privatsphäre und der Notwendigkeit des Staates, zu Zwecken der Strafverfolgung in diese einzudringen.

# Aufgaben zum Thema „Logfiles“

1. Im Internet gibt es sogenannte Anonymisierdienste. Recherchiere nach derartigen Angeboten und erläutere die Funktionsweise.

2. Ein Musikverlag erhält davon Kenntnis, dass an einem bestimmten Tag zu einer bestimmten Uhrzeit ein User einer Tauschbörse hunderte von Musiktiteln zum Download angeboten hat. Wie kann der Verlag herausfinden, welche Person sich hinter dem Anbieter verbirgt? Sollte der Provider deiner Meinung nach die Zugangsdaten herausgeben?

3. Was versteht man unter „Vorratsdatenspeicherung“? Recherchiere im Internet, welche Daten von wem wie lange gespeichert werden müssen.

# Arbeitsmaterialien für den Unterricht

## Thema Cookies

### Was uns die „Datenkekse" erzählen

Cookies sind Informationen, die ein von dir besuchter Webserver auf deiner Festplatte speichert und bei Bedarf auch wieder abfragt. Sie werden verwendet, um den Besucher einer Webseite eindeutig zu identifizieren. Das kann auch noch Monate oder Jahre nach deinem letzten Besuch der Fall sein – vorausgesetzt, du nutzt den gleichen Computer. Denn eigentlich identifizieren Cookies den Computer, nicht dessen Nutzer.

Ein Beispiel: Du bestellst bei einem Internetversandhaus einen Film, mit dem du deinen Vater zu Weihnachten überraschen willst. Als dein Vater einige Zeit später am gleichen Computer selbst etwas bei dem Versandhaus bestellen möchte, wird er mit deinem Namen begrüßt und sieht, was du bereits eingekauft hast.

Es gibt verschiedene Arten von Cookies. Man unterscheidet sie nach dem Ablaufdatum und danach, ob sie vom besuchten Webserver oder einem externen Server (Drittanbieter) angelegt werden. Harmlos sind Cookies, wenn sie nach dem Verlassen der betreffenden Webseite auf deinem Rechner sofort wieder gelöscht werden. Beim nächsten Besuch der Seite können sie dann nicht mehr identifiziert werden.

Die Realität sieht jedoch häufig anders aus: Viele Shop-Systeme arbeiten mit Cookies. Dies ist erforderlich, damit die in einen Warenkorb abgelegten Waren dem Kunden eindeutig zugeordnet werden können. Andererseits haben gerade die Shop-Systeme ein Interesse, den jeweiligen Kunden identifizieren zu können.

Hast du zum Beispiel bei deinem letzten Besuch in einem Shop nach Digitalkameras gesucht und vielleicht sogar eine gekauft, so könnte dir nun direkt auf der Startseite ein passendes Zubehörteil angeboten werden. Das geht aber nur, wenn eine entsprechende Information auf deinem PC gespeichert ist und diese vom Shop-System ausgelesen werden kann.

Was hier noch als Kundenpflege verstanden werden kann, wird spätestens dann zweifelhaft, wenn Cookies von einem externen Server auf deinem PC angelegt werden. Es gibt große Intenet-Vermarktungsfirmen, die die Werbebanner ihrer Kunden auf vielen verschiedenen Internetseiten einblenden. Dabei wird dann gleich ein passendes Cookie auf dem Rechner des Users hinterlassen.

Der Vermarkter kann anhand der Cookies feststellen, auf welchen Internetseiten seiner Kunden ein bestimmter User welche Informationen abgerufen hat. Führt er die Angaben zusammen, so kann er ein genaues Benutzerprofil erstellen, mit dessen Hilfe gezielt Werbebanner und Angebote für den einzelnen User auslieferbar sind. Man bezeichnet diesen Vorgang auch als „zielgenaues Marketing".

### Cookies: Eine Einschätzung

Cookies identifizieren nicht Nutzer, sondern Computer. Cookies sind durchaus nützlich, für einige Anwendungen sogar fast unentbehrlich. Auf der anderen Seite können Cookies missbraucht werden, wie die Beispiele zeigen.

### Cookies: Was tun?

Jeder Browser verfügt über Einstellmöglichkeiten für die Behandlung von Cookies. In der Regel solltest du Cookies von Drittanbietern – also von externen Servern – nicht akzeptieren. Darüber hinaus kannst du deinen Rechner so einstellen, dass alle Cookies nach Ende deines Internet-Besuches automatisch gelöscht werden. Du kannst die Cookies am Ende deiner Internetsitzung auch manuell löschen. Anleitungen hierzu findest du im Hilfesystem des Browsers.

**Tipp: Stell deinen Browser so ein, dass du grundsätzlich gefragt wirst, ob du ein Cookie akzeptieren willst oder nicht. Du erhältst dann einen Überblick, welche Seiten Informationen über dich sammeln oder speichern wollen.**

# Arbeitsmaterialien und Übungen – Kopiervorlage für den Unterricht

## Aufgaben zum Thema „Cookies“:

1. Recherchiere bei www.a9.com, welche personalisierten Dienste angeboten werden und wie Informationen über Nutzer mit anderen Anbietern ausgetauscht werden. Du findest die Informationen im Kleingedruckten ganz unten auf der Startseite unter Privacy Policy.

2. Kann man mit Hilfe von Cookies feststellen, welche Waren ein Besucher eines Online-Shops bisher in diesem Shop gekauft hat? Welche technischen Möglichkeiten dazu sind dir bekannt?

3. Wie weit darf deiner Meinung nach das Verhalten von Nutzern auf Internetplattformen für Marketingzwecke ausgewertet werden?

4. Erstelle eine Anleitung, wie bei den gängigen Browsern (Internet-Explorer, Mozilla, Firefox, Netscape, Opera, Safari oder Konqueror) das Verhalten der Cookies eingestellt wird.

# Arbeitsmaterialien für den Unterricht

## Thema: Web 2.0 „Think before you post!“

### Soziale Netze und Portale – ein erfolgreiches Geschäftsmodell

Etwa um die Jahre 2003/2004 setzte ein Prozess der dramatischen Veränderung des Internets ein. Die Großen der Branche erkannten, dass sich mit redaktionellen Inhalten kaum Geld verdienen ließ, weil die Internetnutzer nicht bereit waren, außer den Zugangsgebühren für die Nutzung des Internets zu bezahlen. Es mussten also andere Geschäftsmodelle gefunden werden.

Eine Haupteinnahmequelle im Internet ist Werbung, die uns auf Schritt und Tritt begegnet. Das Problem der Werbetreibenden sind die großen Streuverluste, wenn Werbung für bestimmte Produkte mehr oder weniger wahllos in Internetseiten eingeblendet wird. Ein anderes Problem ist, dass nur derjenige erfolgreich werben kann, der möglichst viele Besucher immer wieder auf seine Seiten „lockt“.

Wenn nun also kaum Geld mit redaktionellen Inhalten verdient werden konnte, dann vielleicht mit Inhalten, die die User selbst erstellen und anderen Usern – beispielsweise Freunden – zur Schau stellen möchten. Das Schlagwort vom „User-generated-Content“ machte die Runde und leitete eine erneute Revolution des Internets ein. Es entstanden Blogging-Portale, Foto- und Videoportale sowie soziale Netzwerke. Große Internetfirmen erkannten nach und nach diesen Trend und kauften erfolgreiche Seiten auf, wodurch deren Gründer in manchen Fällen praktisch über Nacht zu Multimillionären wurden.

Die Geschäftsidee hinter diesen Portalen ist einfach: Anstatt Geld für die Einstellung von Inhalten zu investieren, wird eine leere Plattform zur Verfügung gestellt. Die Inhalte stammen von den Usern selbst (Blogs, Videos, Fotos, Podcasts usw.). Wenn eine solche Community groß genug ist und täglich mit neuen Inhalten gefüllt wird, kommen die User immer wieder aufs Neue und schauen nach, ob andere User neue Inhalte veröffentlicht haben oder ob die eigenen Inhalte Resonanz gefunden haben.

**Es gibt eine Reihe von Details, die entscheidend dafür sind, ob eine derartige Plattform kommerziell erfolgreich ist oder nicht:**

1. Wichtig ist eine Kommentarfunktion für Inhalte. Wer diskutiert und kommentiert, schaut auch häufiger nach, ob es Antworten gibt. Weitere Funktionen tun ein Übriges: „Tell a friend“, oder manchmal auch „Invite a friend“.

2. Ziel der Plattformbetreiber ist es, möglichst viele User dazu zu bewegen, einen Account anzulegen und sich einzuloggen. Damit kann der User dann z.B. Favoritenlisten anlegen oder Beiträge bestimmter User abonnieren. Außerdem werden Funktionen wie „zuletzt gesehen“ angeboten.

3. Die „hohe Schule“ im Web 2.0 sind Freundeslisten und Interessengruppen, die man mittlerweile in jedem sozialen Netzwerk findet.

### Portale und personalisierte Werbung

All diese Anwendungen bilden die Grundlage für personalisierte Werbung. Ist ein Nutzer in einer Plattform erst einmal eingelogged und sind seine Interessen und Vorlieben bekannt, dann kann auch Werbung gezielter eingeblendet werden. Hat ein User viele virtuelle Freunde oder sogar seinen E-Mail-Account über den Plattformbetreiber, ist die Wahrscheinlichkeit sehr groß, dass er regelmäßig auf der Plattform nachschaut und sich dabei einlogged. Er kann also regelmäßig mit Werbung konfrontiert werden.
Was jetzt zum Erfolg der Werbetreibenden noch fehlt, ist ein regionaler Bezug. Denn wenn ein Betreiber in der Lage ist, einen Münchner von einem Hamburger User zu unterscheiden, dann kann er auch für lokale Kunden Werbung machen. Aber auch hierfür gibt es Lösungen: Zum Beispiel finden es viele attraktiv, den Ort ihrer Universität oder Schule wahrheitsgemäß im Internet anzugeben, damit sie leichter und schneller Kontakt zu anderen von derselben Uni oder Schule aufnehmen können.

### Was erzähle ich im Internet von mir – und was besser nicht!

Stell dir vor, du bewirbst dich bei einem Unternehmen um einen Ausbildungsplatz. Der Personalchef hat – selbstverständlich unter falschem Namen – einen Account in derselben Community wie du. Bei einem Routinecheck stellt er fest, dass du Mitglied in den Gruppen „wieder blaugemacht“ und „Samstag ist Sauftag“ bist. Außerdem findet er einige Bilder von der letzten Party.

**Es ist fraglich, ob du jetzt noch eine Einladung zum Vorstellungsgespräch bekommst.**

Auch die Vermutung, dass sich derartige Eintragungen und Bilder leicht wieder entfernen lassen und somit alles kein Problem darstellt, ist leider falsch. Deine Daten (Bilder, Texte usw.) können

- im Cache von Suchmaschinen gespeichert bleiben,
- von Archivierungsdiensten gespeichert sein,
- längst von anderen herunter- und auf andere Server wieder hochgeladen worden sein,
- von anderen zitiert worden sein (und sind damit bei anderen zu finden)
- für dich nicht mehr verfügbar sein, weil du das Passwort vergessen hast oder dein Account gehackt worden ist.

Sei dir deshalb immer darüber im Klaren, dass alles, was du einmal im Internet preisgegeben hast, von dir anschließend nicht vollständig kontrolliert (=gelöscht oder korrigiert) werden kann. Das gilt erst recht für Einträge in Gästebüchern und Foren und schließt Schimpfworte ebenso mit ein wie jeden Tippfehler. Vielleicht findest du es heute cool, im Internet nicht auf Schreibfehler zu achten, aber solltest du irgendwann einmal eine gehobene Position anstreben, dann sind derlei Peinlichkeiten immer noch im Netz zu finden und werfen ein schlechtes Licht auf dich.

**Merke: Das Netz bewahrt deine Jugendsünden für alle Welt sichtbar auf.**

Das sind nicht die einzigen Gefahren, die im Internet lauern. Es gibt eine Reihe von Personengruppen, die das Web mehr oder weniger gezielt nach persönlichen Informationen durchsuchen. Im Extremfall können dies zum Beispiel Pädophile auf der Suche nach neuen Opfern sein. Sie nutzen es aus, dass Persönlichkeitssuchmaschinen auch in sozialen Netzwerken aktiv sind, indem sie systematisch die Profile der Web 2.0-Communities durchsuchen.

Wenn du wirklich anonym bleiben willst, solltest du konsequent auf alle Angaben, die auf deine Identität schließen lassen, verzichten. Das gilt für das Anlegen deines Accounts, für die Angabe deiner E-Mail-Adresse bei der Anmeldung und auch für private Nachrichten innerhalb der Community. Empfehlenswert kann dabei auch das Verwenden von Rollen oder Pseudonymen sein.

**Merke: Letztlich bist du es, der bestimmt, was offen und was „geheim“ ist.**

## Die Privatsphäre anderer respektieren

Ein anderes Thema: Auf der letzten Klassenfahrt gab es eine wilde Kissenschlacht, die du mit deinem Handy fotografiert hast. Du erstellst davon eine Bildergalerie in einem sozialen Netz, um alle anderen an den Eindrücken der Kissenschlacht teilhaben zu lassen.

In diesem Zusammenhang ist wichtig: Es geht bei sozialen Netzen nicht nur um das, was du von dir selbst preisgibst, sondern auch um das, was du von oder über andere veröffentlichst.

Ein dummer Streich, den man jemandem spielt, weil man es im Moment gerade lustig findet, ist auch nach Jahren noch im Internet zu finden und kann andere bloßstellen. Das gilt auch für jede aus Wut oder Übermut geschriebene Bemerkung oder „lustige“ Fotos von der letzten Party oder Klassenfahrt.

Unsere Gesetze ziehen klare Grenzen hinsichtlich der Frage, was hier erlaubt ist und was nicht. Ein Film oder ein Foto, auf dem eine Person erkennbar abgebildet ist, darf grundsätzlich nicht ohne die Zustimmung dieser Person veröffentlicht werden. Eine Ausnahme gibt es, wenn es sich um eine Persönlichkeit der Zeitgeschichte handelt. Dann ist die Veröffentlichung in dem Rahmen zulässig, in dem diese Person eine Bedeutung für die Gesellschaft hat, z.B. eine Sportlerin beim Wettkampf oder ein Politiker bei seiner Amtsausübung. Zudem sollten stets die Vertraulichkeit des gesprochenen Wortes und die Grenzen zwischen Meinungsfreiheit und Beleidigung beachtet werden. Wer diese Grenzen nicht akzeptiert, bringt andere in Misskredit, kann es kaum rückgängig machen und gerät unter Umständen mit dem Gesetz in Konflikt.

## Die Bedeutung der Urheberrechte

In deinem Blog beschreibst du die Anreise zu einem Open-Air-Festival und scannst dafür einen Kartenausschnitt aus einem Straßenatlas ein. Ist dies erlaubt oder nicht?

Prinzipiell würde man denken – ja – denn eigentlich gehört ein Kartenausschnitt aus einem Straßenatlas nicht zum Schutz der Privatsphäre. Beim Thema Web 2.0 aber dürfen wir auch das Urheberrecht nicht unerwähnt lassen.

Dabei gilt: Alles, was du auf einer Plattform anderen zugänglich machst, ist eine Veröffentlichung – es sei denn, du beschränkst den Zugriff auf deine Freunde.

Veröffentlichen darfst du aber nur:

- was du selbst erstellt hast, oder
- wofür du die ausdrückliche Erlaubnis des Urhebers hast.

Alles andere kann sehr teuer für dich werden. Wenn du Pech hast, bekommst du Post von einem Anwalt, der dich auffordert, das Werk des anderen zu löschen und dir eine Unterlassungserklärung beifügt, die du unterschreiben sollst. Gleichzeitig schickt er dir eine Rechnung über mehrere hundert Euro, die du bezahlen musst.

**Also: Vorsicht bei Veröffentlichungen! Prüfe genau, ob du die Rechte zur Veröffentlichung hast, bevor du die Inhalte anderer veröffentlichst.**

# Arbeitsmaterialien und Übungen – Kopiervorlage für den Unterricht

## Aufgaben zum Thema „Web 2.0“:

1. Welche sozialen Netze kennst du und bei welchen bist du registriert?
   Schildere kurz, welche Erfahrung du bislang damit gemacht hast.

2. Welche persönlichen Daten werden bei der Erstellung eines Accounts abgefragt?

3. Begründe, warum die Datenbanken von sozialen Netzen „lohnende“ Hackerziele sind.

4. Wie können Plattformbetreiber von den Userdaten profitieren, obwohl alle Dienste kostenlos sind?

5. Recherchiere, welche Web 2.0-Dienste welchen Firmen und Konzernen gehören.
   Recherchiere auch die Kaufpreise.

6. Recherchiere auf den Seiten von Web 2.0-Diensten Aussagen zu Werbung und zur Weitergabe von Daten (ein Tipp: Du findest sie meist in den FAQs, den AGBs oder unter „Privacy policy“ o.ä.).

7. Erstelle eine Liste von Angaben über dich, die du niemals im Internet weitergibst.

Diese Druckschrift wird im Rahmen der Öffentlichkeitsarbeit der Landesregierung Nordrhein-Westfalen herausgegeben. Sie darf weder von Parteien noch von Wahlwerbern oder Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden.

Dies gilt für Landtags-, Bundestags- und Kommunalwahlen sowie auch für die Wahl der Mitglieder des Europäischen Parlaments.

Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken und Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung.

Eine Verwendung dieser Druckschrift durch Parteien oder sie unterstützende Organisationen ausschließlich zur Unterrichtung ihrer eigenen Mitglieder bleibt hiervon unberührt. Unabhängig davon, wann, auf welchem Wege und in welcher Anzahl diese Schrift dem Empfänger zugegangen ist, darf sie auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl nicht in einer Weise verwendet werden, die als Parteinahme der Landesregierung zu Gunsten einzelner politischer Gruppen verstanden werden könnte.

**Kontakt**

Agentur »secure-it.nrw«
bei der IHK Bonn / Rhein-Sieg
Bonner Talweg 17, 53113 Bonn
Telefon: +49 (0) 228 / 2284 - 184
Telefax: +49 (0) 228 / 2284 - 5184
E-Mail: info@secure-it.nrw.de
Internet: www.secure-it.nrw.de
www.branchenbuch-it-sicherheit.de