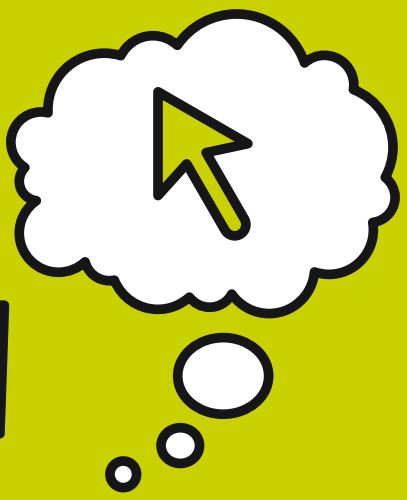
Unterrichtsmaterialien

erst denken,
dann klicken.



Schutz der Privatsphäre im Internet

Mit Übungen für den Unterricht

bm:uk efit21 BUNDESKANZLERAMT ÖSTERREICH DSK Microsoft Saferinternet.at Das Internet sicher nutzen!

Schüler/innen-Broschüre „DU bestimmst ...“

mit Tipps und Fakten zum Thema Datenschutz

Herausgegeben von der Österreichischen Datenschutzkommission
www.dsk.gv.at

Bestellungen (auch in Klassenstärke) per E-Mail unter **dsk@dsk-gv.at** oder telefonisch unter **01 531 15/2525.**

Schutz der Privatsphäre im Internet

Sehr geehrte Lehrende, sehr geehrte Direktor/innen!

Soziale Netzwerke, Instant Messenger oder Blogs sind aus dem Online-Alltag nicht mehr wegzudenken. Kein Wunder, bieten sie doch faszinierende Möglichkeiten: Kontakte pflegen, sich im Netz präsentieren, neue Leute kennenlernen und der einfache Austausch von Fotos und Videos sind ja auch wirklich gute Gründe, sich aktiv im Netz einzubringen. Doch gleichzeitig ergeben sich dadurch neue Herausforderungen für den Schutz der Privatsphäre: Die Verwendung des „Mitmach-Internet" macht nur Sinn, wenn man etwas von sich preisgibt. Umgekehrt kann allzu große Freizügigkeit unangenehme Folgen haben.

Dieses Unterrichtsmaterial informiert Sie praxisnah über die verschiedenen Facetten des Privatsphärenschutzes im Internet und gibt Ihnen konkrete Unterstützung bei der Behandlung des Themas im Unterricht. Das Material richtet sich vor allem an Lehrende und Schüler/innen der Sekundarstufe 1, Sie finden darin aber auch Übungsvorschläge z. B. für Volksschulen und Sekundarstufe 2. Je früher Schüler/innen diese Kompetenz erlernen, desto eher kann Problemen vorgebeugt und das Internet uneingeschränkt mit all seinen Vorzügen genutzt werden.

In den Kapiteln 1 bis 3 finden Sie und Ihre Schüler/innen eine Einführung in das Thema sowie Informationen über rechtliche Rahmenbedingungen zum Datenschutz. Kapitel 4 enthält zahlreiche praktische Tipps und beschreibt anhand konkreter Internet-Anwendungen, worauf bei der Veröffentlichung privater Informationen geachtet werden sollte und welche technischen Einstellungen es für einen besseren Schutz der Privatsphäre gibt. Weiterführende Links in Kapitel 5 und zahlreiche Übungen inklusive Arbeitsblättern zum Kopieren in Kapitel 6 helfen Ihnen bei der Verwendung im Unterricht. FAQs zum Datenschutz in der Schule und 10 Sicherheitstipps als Zusammenfassung runden das Material ab.

Die Informationsteile (Kapitel 1–5) können als Kopiervorlagen für die Verteilung an die Schüler/innen verwendet werden. Deshalb wurde im Fließtext die „du"-Form gewählt.

Diese Unterrichtsmaterialien wurden auf Initiative von Saferinternet.at, Microsoft Österreich und erfahrenen Lehrenden mit Unterstützung des Bundesministeriums für Unterricht, Kunst und Kultur, des Bundeskanzleramts und der Datenschutzkommission erstellt. Die Inhalte basieren u. a. auf Workshops von Saferinternet.at mit Schüler/innen an österreichischen Schulen.

Unter **www.saferinternet.at/broschuerenservice** können sie diese Unterlagen kostenlos downloaden oder nachbestellen. Neben weiteren Unterrichtsmaterialien finden Sie dort auch viele praktische Informationen zur sicheren Internet- und Handynutzung.

Mit freundlichen Grüßen

DI[in] Barbara Buchegger, M.Ed.
Saferinternet.at/Österreichisches Institut
für angewandte Telekommunikation
Margaretenstraße 70, 1050 Wien
Website: www.saferinternet.at
E-Mail: office@saferinternet.at
Telefon: 01 595 21 12-0

Gerhard Göschl, MSc
Sicherheits-Sprecher,
Microsoft Österreich Gmbh
Am Europaplatz 3, 1120 Wien
Website: www.microsoft.com/austria/protect
E-Mail: gerhard.goeschl@microsoft.com
Telefon: 01 610 64-0

Schutz der Privatsphäre im Internet

Ziele

- Private Daten von öffentlichen Daten unterscheiden lernen
- Die Bedeutung des Schutzes der Privatsphäre im Internet erkennen
- Die Preisgabe von Daten im Internet reflektieren
- Unerwünschte Online-Inhalte über sich selbst vermeiden lernen
- Erkennen, wie schnell im Internet falsche Identitäten und Eindrücke entstehen können
- Sensibel werden für mögliche Auswirkungen des eigenen Handelns auf andere

Inhalt

FAQs zum Datenschutz in der Schule

Dürfen Fotos oder Videos von Schüler/innen auf der Schulwebsite veröffentlicht werden?
Haben die Eltern und die Schüler/innen selbst (ab 14 Jahren relevant) eine Einverständniserklärung gegeben, dann können Fotos auf der Schulwebsite genutzt werden. Fotos der gesamten Klasse veröffentlichen Sie z. B. am besten nur mit Klassennennung, aber ohne die Namen der einzelnen Schüler/innen anzugeben.

Beispiele für Einverständniserklärungen von Eltern. Diese können für Schüler/innen entsprechend adaptiert werden:

Variante 1: Ich, Frau/Herr _____, erkläre mich damit einverstanden, dass auf der virtuellen Lernplattform/dem Internetauftritt der Schule Fotos aus dem Schulalltag, auf der möglicherweise auch mein Sohn/meine Tochter _____ zu sehen ist, im Internet veröffentlicht werden. Die Fotos zeigen Schüler/innen beim Arbeiten oder im Schulalltag. Es werden keine Porträts oder Bilder mit vollständigem Namen der Schüler/innen veröffentlicht.

Variante 2: Ich, Frau/Herr _____, bin einverstanden, dass mein Sohn/meine Tochter _____ im Zuge von Schulveranstaltungen fotografiert/gefilmt wird und diese Fotos/Videos (ohne Nennung des Namens) auf der Schulwebsite und in sonstigen Publikationen der Schule veröffentlicht werden dürfen.

Achtung: Die Eltern und die Schüler/innen können ihre Einverständniserklärungen jederzeit widerrufen. Dann muss das entsprechende Foto auf Wunsch auch wieder aus dem Netz genommen werden. Fotos, die für Schüler/innen oder andere abgebildete Personen nachteilig sein könnten (z. B. freizügig bekleidet, betrunken), dürfen nicht veröffentlicht werden. Sie verletzen das „Recht am eigenen Bild". Zu beachten sind auch die Urheberrechte des Fotografen bzw. der Fotografin.

Dürfen Geburtsdaten von Schüler/innen, z. B. im Zuge von Sportveranstaltungen, veröffentlich werden?
Empfehlenswert ist, davon abzusehen! Dies kann einerseits das Persönlichkeitsrecht der Schüler/innen verletzen, aber auch z. B. zur Erstellung von Persönlichkeitsprofilen, zu Identitätsklau und Belästigungen führen. Wenn Sie die Daten trotzdem veröffentlichen möchten, holen Sie dafür eine Einverständniserklärung bei den Eltern und den Schüler/innen ein.

Dürfen Schüler/innen im Zuge von Unterrichtsprojekten einander fotografieren oder filmen und die Ergebnisse in der Projektdokumentation nutzen?
Auch hier gilt, dass vorab eine Einverständniserklärung der Eltern bzw. der Schüler/innen vorliegen muss, damit dies rechtlich abgesichert erfolgen kann. Diese kann einmal pro Jahr, z. B. am Schuljahresbeginn, unterschrieben werden. Darüber hinaus sollte die Veröffentlichung eines Fotos/Videos immer mit allen abgebildeten Personen abgestimmt sein.

Dürfen Schüler/innen Lehrer/innen fotografieren und diese Fotos veröffentlichen?
Auch dies ist selbstverständlich nur mit Zustimmung möglich, ansonsten besteht zumindest ein Anspruch auf Löschung von der betreffenden Website. Zusätzlich zu allgemeinen zivil- oder urheberrechtlichen Bestimmungen ist nach dem Datenschutzgesetz (DSG) in den meisten Fällen schon die unbefugte Aufnahme von Bildern, die (identifizierbare) Personen abbilden, verboten.

Gegebenenfalls empfiehlt es sich, Schüler/innen darauf hinzuweisen, dass die Veröffentlichung insbesondere von herabwürdigenden Bildern oder Filmen Schadenersatzpflichten (§ 33 DSG 2000) oder sogar strafrechtliche Konsequenzen (§ 51 DSG 2000) nach sich ziehen kann.

Darf die Schule eigenständige Werke der Schüler/innen veröffentlichen?

Um von den Schüler/innen eigens erstellte Werkr (z. B. Fotos, Videos, Audio, Texte) veröffentlichen zu können, müssen der/die jeweilige Schüler/in sowie dessen/deren Eltern vorab damit einverstanden sein. Die/der Urheber/in genießt für ihre/seine Schöpfung – das geistige Eigentum – einen rechtlichen Schutz, der im Urheberrechtsgesetz festgehalten ist. Mit einer schriftlichen Einverständniserklärung (siehe nachfolgendes Beispiel) überträgt der/die Urheber/in die Rechte zur Veröffentlichung seiner/ihrer Werke an z. B. die Schule. **Das Urheberrecht an sich verbleibt aber immer beim geistigen Schöpfer.** Die Eltern und die Schüler/innen können ihre Einverständniserklärung demnach jederzeit widerrufen.

Trotz Einverständniserklärung empfiehlt es sich, die Veröffentlichung eines Werkes im konkreten Fall immer nochmals mit dem/der Schüler/in bzw. den Eltern abzustimmen. Denken Sie im Übrigen auch daran, den Urheber/die Urheberin der veröffentlichten Werke zu nennen!

Beispiel für eine Einverständniserklärung von Eltern. Diese kann für Schüler/innen entsprechend adaptiert werden:

Ich, Frau/Herr _____, bin damit einverstanden, dass die Schule _____, die während des Schulunterrichts entstandenen Werke meines Sohnes/meiner Tochter, _____, in Publikationen der Schule sowie in sonstigen im schulischen Kontext stehenden Publikationen veröffentlichen darf.

Nützliche FAQs speziell zum Urheberrecht an Schulen finden Sie unter:
www.bmukk.gv.at/medienpool/15917/faq_haller.pdf bzw. weitere Artikel auf **www.mediamanual.at**.

Darf man E-Mail-Adressen auf der Schulwebsite veröffentlichen?

Generell dürfen nur solche Daten auf der Website veröffentlich werden, für die es die Zustimmung der betreffenden Personen (bzw. deren Eltern) gibt. Werden E-Mail-Adressen online gestellt, z. B. um die Kontaktaufnahme der Eltern mit Lehrenden zu erleichtern, veröffentlichen Sie die E-Mail-Adresse entweder als Bilddatei oder ohne den Klammeraffen (z. B. name (at) schule.at), um Spam für die betreffenden Personen zu vermeiden. Private Telefonnummern sollten prinzipiell nicht auf eine Website gestellt werden.

Dürfen Schulen Logfiles der Schulcomputer und der Aktivitäten der Schüler/innen am Computer speichern?

Die Schule darf Logfiles speichern, um sicherzustellen, dass das Netzwerk reibungslos an der Schule läuft[1]. Allerdings ist es wichtig, dass bei dieser Speicherung nicht die Personen (Lehrende wie Schüler/innen) im Mittelpunkt des Interesses stehen, sondern die Abwehr von Schäden am IT-System. Nur dann ist es zulässig, die Daten zu kontrollieren und zu nutzen. Dies kann z. B. der Fall sein, wenn das IT-System Probleme aufweist (z. B. Viren) oder das Herunterladen großer Datenmengen zu Engpässen im Schulnetzwerk führt.

[1] § 14 Abs. 2 Z 7 Datenschutzgesetz

Darf die Schule gespeicherte Logfiles zu pädagogischen Zwecken nutzen?

Auch wenn die Schule prinzipiell das Recht hat, Logfiles zu speichern, dürfen diese Daten nicht unbedingt dafür genutzt werden, um Schüler/innen zur Rechenschaft zu ziehen. Empfehlenswert ist, alle Betroffenen über eine Protokollierung der Internetnutzung mit Logfiles zu informieren. Schüler/innen müssen mit geeigneten pädagogischen Mitteln dazu gebracht werden, sich an die Anweisungen der Lehrenden oder an eine vorhandene „Internet-Policy" der Schule zu halten. Besteht eine Gefährdung des Schulnetzwerkes über einen längeren Zeitraum hinweg und wurden alle anderen Möglichkeiten ausgeschöpft, dies zu beheben, so können auch die Logfiles genutzt werden. Dies darf aber wirklich nur ein letzter Schritt sein!

Welche Inhalte sollen in einer „Internet-Policy" der Schule festgesetzt sein?

Es ist sinnvoll, eine „Policy zur Nutzung des Internet" in der Schule zu beschließen. Diese kann folgende Punkte umfassen:

1. Das Nutzen von illegalen oder für die Schüler/innen ungeeigneten Inhalten ist in der Schule untersagt. Dazu zählen jugendgefährdende und kinderpornographische Inhalte sowie solche, die dem Verbotsgesetz unterliegen.

2. Die Internetnutzung darf den Betrieb in der Schule nicht beeinträchtigen oder negativ beeinflussen und auch nicht dem Ansehen der Schule/Klasse schaden.

3. Das Herunterladen/Nutzen von urheberrechtlich geschütztem Material (Musik, Filme, Programme, Fotos etc.) darf in der Schule ohne Zustimmung der Urheber/innen nicht erfolgen.

4. Die übermäßige Nutzung von Speicherplatz oder das übermäßige Drucken sind im Sinne einer reibungslosen Nutzung des Schulnetzes zu unterlassen.

5. Persönliche Daten dürfen Schüler/innen im Internet nicht frei zugänglich bekannt geben.

6. Es dürfen nur Bilder/Filme/Aufnahmen von Personen im Internet veröffentlicht werden, die auch damit einverstanden sind und für die es eine Einverständniserklärung der Eltern (bei Schüler/innen) gibt.

7. Werden Dokumente aus dem Internet für Referate, Hausübungen o. ä. verwendet, werden die betreffenden Passagen gekennzeichnet/zitiert und mit der entsprechenden Quellenangabe versehen.

8. Für die Arbeit in einem passwortgeschützten Bereich (z. B. in einem Kurs auf einer Lernplattform) erhält jede/r Benutzer/in ein persönliches Passwort. Die Weitergabe dieses Passwortes sowie die Verwendung von gemeinsamen Passwörtern für mehrere Benutzer/innen sind nicht gestattet. Das persönliche Passwort ist geheim zu halten und gesichert aufzubewahren.

Weiterführende Informationen erhalten Sie in der Broschüre „Recht in virtuellen Lernumgebungen" des BMUKK – zum Downloaden unter www.saferinternet.at/broschuerenservice.

1 Warum ist es wichtig, die eigene Privatsphäre zu schützen?

Quelle: Comic von Thomas Plaßmann

Sich völlig anonym durch den Alltag zu bewegen, ist heutzutage so gut wie unmöglich. Ob beim Telefonieren, beim Einkaufen im Supermarkt, bei der Urlaubsbuchung, beim Arztbesuch oder beim Surfen im Internet – fast immer werden jede Menge persönliche Daten erfasst. Teils offensichtlich, oft aber auch ohne unser Wissen. Für einen Teil der verfügbaren Daten von uns sind wir aber auch selbst verantwortlich, weil wir ausgesprochen freizügig mit Angaben zur eigenen Person umgehen. Wie schnell ist etwa ein Gewinnspielformular mit Name, Adresse, Telefonnummer, Geburtsdatum etc. ausgefüllt? Oder eine Kundenkarte registriert? Oder ein Profil in einer Online-Community angelegt? **Es lohnt sich, darüber nachzudenken, welche Datenspuren man hinterlässt und welche Auswirkungen das haben kann.**

Interessant zu wissen

Insgesamt speichern private und öffentliche Datenverwender in Österreich bis zu 40 verschiedene Datenarten über eine einzelne Person.[2] Früher war es ohne Computer und Internet kaum möglich, so genannte **„personenbezogene Daten"** (= Daten, mit denen unmittelbar auf eine bestimmte Person geschlossen werden kann) aus verschiedenen Quellen zu sammeln und Verknüpfungen herzustellen. Heute lassen sich unterschiedlichste Informationen leicht zu **umfassenden Persönlichkeitsprofilen** zusammenführen. Mit „Persönlichkeitsprofil" ist eine Zusammenstellung von Daten gemeint, die eine Einschätzung wesentlicher Eigenschaften einer Person erlaubt.

Oft heißt es: „Wer nichts angestellt hat, hat auch nichts zu verbergen". Aber dann wäre es ja eigentlich auch ok, wenn jeder auf Schritt und Tritt mit Videokameras überwacht werden würde. Das wollen die meisten Menschen verständlicherweise dann doch nicht ... Also liegt uns schon irgendwie sehr viel daran, „Privates" für uns zu behalten.

Doch was ist das überhaupt, „privat"? Ist es privat, welches Haustier ich habe? Oder wer meine Freunde sind? Oder welche Spiele ich spiele? Oder in welche Schule ich gehe? Oder wie oft ich meine Zähne putze? Diese Fragen sind nicht einfach zu beantworten, denn jeder denkt anders darüber. In diesem Zusammenhang spricht man übrigens gerne von der „Privatsphäre". Eine Sphäre ist ein Bereich, der wie z. B. eine Gaswolke keine klare Grenze hat. Man könnte sagen:

Die Privatsphäre einer Person bezeichnet den Bereich, der nicht öffentlich ist, sondern der nur die eigene Person angeht.

(Quelle: klicksafe.de)

Du bestimmst also ganz alleine, wer zum Beispiel weiß ...

- ... wieviel Taschengeld du bekommst, indem du es einfach nicht weitererzählst;
- ... was du eingekauft hast, indem du Kundenkarten akzeptierst oder nicht;
- ... wer deine Freunde sind, indem du dein privates Netzwerk in Online-Communitys schützt, sodass Fremde diese Daten nicht einsehen können;
- ... wer Persönlichkeitsprofile von dir anlegen darf, indem du Datenverwendern so wenige Daten wie möglich bekannt gibst;
- etc.

[2] Quelle: AK Wien: „Privatsphäre 2.0. Beeinträchtigung der Privatsphäre in Österreich – neue Herausforderungen für den Datenschutz", erschienen Februar 2009.

Es erleichtert unser Leben sehr, dass nicht alle Menschen alles voneinander wissen und man grundsätzlich selbst bestimmen kann, wer was über einen weiß. Dieser Grundsatz wird auch **„informationelle Selbstbestimmung“** genannt.

Wenn man auf den Schutz der eigenen Privatsphäre Wert legt, muss man deshalb noch lange nichts angestellt haben. Jeder hat ein Recht darauf und sollte von diesem auch Gebrauch machen!

Weitere Argumente für den Schutz der Privatsphäre:

- Die Bedeutung des Schutzes der Privatsphäre zeigt sich schon alleine darin, dass dieser Schutz in der österreichischen Verfassung festgeschrieben ist. Das bedeutet, dass es ein besonders wichtiges Recht ist. **Dein Privatleben gehört dir und darf nur unter ganz bestimmten Umständen durch andere angetastet werden.**
- Jeder Mensch hinterlässt in den unterschiedlichsten Situationen immer mehr Datenspuren von sich. Viele davon sind relativ unbedenklich, **einige Dinge gehen aber einfach niemanden etwas an**, wie z. B. Angaben über deinen Gesundheitszustand, deine Bankdaten, die Höhe deines Ersparten, deine politische Einstellung, mit wem du befreundet bist, dein Familienleben, deine sexuelle Orientierung etc.
- Je mehr persönliche Daten du von dir preisgibst, desto einfacher haben es diverse „Datensammler“, **deine Angaben etwa für Werbezwecke oder sogar Betrügereien zu missbrauchen.**
- Der Schutz der Privatsphäre **spielt auch eine wichtige Rolle für eine funktionierende Demokratie.** Ohne Privatsphäre ist es viel schwieriger, sich frei und unabhängig eine eigene Meinung zu bilden – und ohne freie Meinungsbildung kann es keine funktionierende Demokratie geben. Aus diesem Grund versuchen totalitäre Systeme nicht nur das öffentliche, sondern auch das private Leben ihrer Bürger/innen vollständig zu kontrollieren.

Wie wichtig der Schutz privater Daten (gerade auch im Internet) ist, zeigen folgende Beispiele:

Nadine und die misslungene Bewerbung

Nadine, 16 Jahre, hat sich bei einer großen Versicherung um einen Ausbildungsplatz als Versicherungskauffrau beworben. Als sie vergangene Woche die Einladung zum Bewerbungsgespräch im Postkasten gefunden hatte, war die Freude riesig. Nun, als ihr der Personalchef der Versicherung gegenübersitzt, schießen Nadine tausende Fragen durch den Kopf: Bin ich passend angezogen? Habe ich mir genug über das Unternehmen durchgelesen? Werde ich etwas auf Englisch sagen müssen? Die ersten zehn Minuten des Gesprächs verlaufen soweit ganz gut, doch dann konfrontiert der Personalchef Nadine plötzlich mit ziemlich unangenehmen Fotos. Darauf zu sehen ist Nadine in offensichtlich angetrunkenem Zustand, wie sie recht spärlich bekleidet und mit einer Bierflasche in der Hand auf einer Bar-Theke tanzt. Der Personalchef erklärt, dass er nach ihrem Namen im Internet gesucht hätte und dabei auf die Bilder auf einer Fotoplattform gestoßen wäre. Er möchte wissen, ob sie so etwas in ihrer Freizeit öfter machen würde. „Die Fotos habe ich doch erst vor ein paar Tagen ins Netz gestellt", denkt sich Nadine schockiert und bringt kein Wort mehr heraus. Ihren ersehnten Ausbildungsplatz bei der Versicherung kann sie jetzt natürlich vergessen.

Stefan im Liebesrausch

Der 13-jährige Stefan hat sich total in seine Klassenkameradin Ines verliebt. In der Schule traut er sich nicht, Ines anzusprechen, aber er weiß, dass sie viel in einer bestimmten Online-Community unterwegs ist. Um seiner Angebeteten näher zu sein, registriert sich Stefan ebenfalls dort. „Vielleicht verliebt sie sich ja auch in mich, wenn sie mehr über mich weiß", denkt sich Stefan und bestückt sein Profil daher mit vielen privaten Details und Fotos. Nachdem er nun schon öfter mit Ines in der Community geschrieben hat, fasst er sich schließlich ein Herz und gesteht seine Liebe in einem Eintrag auf Ines' Profilpinnwand. Seine schmachtenden Liebesschwüre unterzeichnet er mit „Dein Kuschelbär" – denn irgendwo hat Stefan mal gelesen, dass das bei Frauen gut ankommt. Er ist sich sicher, dass das eh keiner liest, der ihn kennt, schließlich ist keiner seiner Freunde in der Community registriert. Einige Tage später geht Stefan wie gewohnt zum Fußballtraining – aber irgendwas ist heute anders als sonst: Seine Trainingskollegen begrüßen ihn mit breitem Grinsen, manche tuscheln hinter ihm und einer klopft ihm schließlich auf die Schulter mit den Worten: „Na, Kuschelbär, wie geht's uns heute?". Alle brechen in schallendes Gelächter aus. Als Stefan auf das „Schwarze Brett" des Fußballvereins schaut, wird ihm plötzlich alles klar und am liebsten würde er vor Scham im Erdboden versinken: Vor ihm prangt ein Ausdruck seines Liebesgeständnisses an Ines aus der Community!

Adina und die teure Rechnung aus China

Die 15-jährige Adina ist täglich mehrere Stunden in ihrem Lieblingschat online, dort hat sie schon viele nette Bekanntschaften gemacht. Seit einigen Wochen chattet sie mit „Michael", 17 Jahre. Die beiden haben schon so viel – auch über Privates – miteinander geplaudert, sodass Adina kein bisschen misstrauisch ist als Michael sie nach ihren Zugangsdaten für ein bestimmtes Online-Auktionshaus fragt. Er würde dort gerne etwas nachschauen, müsse dafür aber eingeloggt sein. „Freunde helfen sich doch gegenseitig", sagt Adina und gibt ihrem Chatpartner bereitwillig die Login-Daten. Das war das letzte Mal, dass Adina von Michael gehört hat – und obendrein möchte ein chinesischer Versandhandel nun 350 Euro von ihr und droht mit einer Klage. Michael hat dort mit Adinas Account mehrere Artikel über das Auktionshaus ersteigert und Adina auf der Rechnung sitzen lassen!

Tarik in Erklärungsnöten

Tarik, 13 Jahre, wird am Nachmittag von seinem Freund Paul angerufen, der ihn zum Schwimmen einladen möchte. Aber Tarik hat weder Lust auf den Badesee noch auf Paul und erzählt ihm deshalb, dass seine Oma zu Besuch wäre und er daher keine Zeit hätte. Nach dem Gespräch schwingt sich Tarik wieder vor seinen Computer und schreibt nichtsahnend in die Statusmeldung auf seinem Community-Profil: „Bin daheim und versuche das nächste Level von World of Warcraft zu knacken". Eine halbe Stunde später erhält Tarik eine beleidigte SMS seines versetzten Freundes: „Wenn du lieber WoW spielst, kannst es gleich sagen. Brauchst mich aber nicht so falsch anlügen. Hab gedacht wir sind Freunde. Paul" Tarik hatte gar nicht daran gedacht, dass Paul die Statusmeldung lesen könnte! Jetzt muss er sich ordentlich etwas zur Wiedergutmachung einfallen lassen ...

Saschas verhängnisvolle Internet-Vergangenheit

Sascha ist mittlerweile 29 Jahre alt, hat ein abgeschlossenes Betriebswirtschaftsstudium, einen verantwortungsvollen Job in einem internationalen Technologiekonzern, eine harmonische Beziehung mit Freundin Birgit und eine schicke gemeinsame Eigentumswohnung – kurz gesagt: er lebt das Leben, das er sich immer ausgemalt hat. Noch vor ein paar Jahren war das allerdings ganz anders. Sascha fehlten die Ziele im Leben, er hatte kaum Freunde und saß ständig daheim vor seinem Computer. Damals hat er ziemlich viel Blödsinn ins Internet gestellt und sich an sinnlosen Online-Diskussionen und -Aktivitäten beteiligt. „Eine verrückte Zeit", denkt Sascha heute und ist froh, dass sein Leben jetzt anders ist. Doch einige Zeit später hagelt es plötzlich Probleme, Saschas Internet-Vergangenheit scheint über ihn hereinzubrechen: Zuerst wird Sascha zu seinem Chef zitiert, der ihm irgendwelche Internetausdrucke aus einem Aktivisten-Forum vorlegt und dafür eine Erklärung verlangt. Sascha hat dort vor über sieben Jahren einen sehr kritischen Beitrag über die Machenschaften internationaler Unternehmen verfasst, in dem er auch seinen jetzigen Arbeitgeber scharf angreift. Sein Chef findet das natürlich weniger lustig ... Und als ob das nicht reichen würde, bittet ihn wenig später auch seine Freundin zu einem ernsten Gespräch. Sie hätte einen Hinweis von einer Bekannten erhalten, dass Sascha in einer Online-Singlebörse registriert und auf der Suche nach blonden, vollbusigen Damen sei. „Das war doch alles schon vor zig Jahren", zeigt sich Sascha verzweifelt über sein Schlamassel und ärgert sich grün und blau, was er da früher alles ins Internet gestellt hat und warum er es nicht wieder rechtzeitig gelöscht hat ...

2 Internet: Das Ende der Privatsphäre?

Immer öfter und selbstverständlicher informieren wir uns im Internet, kommunizieren online und kaufen im Netz ein. Die Frage „Bist du auch auf *Facebook*?“ ist dir wahrscheinlich nicht fremd. Interaktive Webplattformen wie Chats, Blogs, Diskussionsforen und Soziale Netzwerke sind aus dem Online-Alltag nicht mehr wegzudenken. Kein Wunder, denn nirgendwo sonst kann man so einfach Kontakte pflegen, sich selbst im Netz präsentieren, neue Leute kennenlernen, mit anderen Fotos und Videos austauschen und dadurch dem Internet ein „persönliches Gesicht“ geben. Doch vor allem bei der Nutzung von Communitys befindet man sich häufig in einem Zwiespalt: Die Verwendung von *Facebook, Google+ & Co.* macht nur Sinn, wenn man etwas von sich preisgibt. Umgekehrt kann allzu große Freizügigkeit unangenehme Folgen haben. Was dabei oft vergessen wird: **Das Publikum im Internet ist riesengroß und was einmal online ist, lässt sich oft nicht mehr entfernen.** Außerdem gilt: Nicht alles, was im Internet über dich existiert, muss von dir selbst dort veröffentlicht worden sein. In solchen Fällen ist es meist noch schwieriger, den eigenen „Datenschatten“ im Netz loszuwerden.

Interessant zu wissen

Pro Tag registrieren sich 250.000 Internetnutzer/innen neu in einem Sozialen Netzwerk.[3] Alleine in Europa tummeln sich rund 219 Millionen Menschen auf *Facebook*, dem weltweit größten Sozialen Netzwerk. Ein Phänomen, das natürlich auch vor Österreich nicht Halt macht: Hierzulande zählt *Facebook* 2,64 Millionen Nutzer/innen – das ist jeder dritte Österreicher bzw. Österreicherin.[4] Bei den österreichischen Jugendlichen zwischen 11 und 18 Jahren nutzen 62 % Online-Communities (hauptsächlich *Facebook*), 38 % tun dies täglich. Mehr als die Hälfte gibt dort gerne Kommentare ab, ein Drittel lädt regelmäßig Fotos hoch.[5] *Facebook*, *YouTube*, *Blogger.com* und *Twitter* zählen in Österreich zu den 15 meistbesuchten Internetseiten.[6]

[3] Quelle: Europäische Kommission: http://ec.europa.eu/information_society/activities/social_networking/facts/index_en.htm (25.11.2011).
[4] Quelle: socialbakers: http://www.socialbakers.com (25.11.2011).
[5] Quelle: Education Group. 2. Oö. Jugend-Medien-Studie 2011: http://www.bimez.at/index.php?id=5993 (25.11.2011).
[6] Quelle: Alexa.com. Top Sites in Austria: http://www.alexa.com/topsites/countries;0/AT (25.11.2011).

2.1 Neue Herausforderungen für den Datenschutz

Mit zunehmender Verbreitung von Computer und Internet ist der Schutz der Privatsphäre immer mehr in den Blickpunkt der Öffentlichkeit gerückt. Aber warum ist das eigentlich so?

- **Enormer Speicherplatz:** Durch die Entwicklung von Computern wurde es möglich, Informationen in großem Ausmaß kostengünstig zu speichern. Viele hundert Gigabyte Speicherplatz auf einem Computer zur Verfügung zu haben, war vor wenigen Jahren noch eine extrem teure Angelegenheit. Es wird also immer einfacher und billiger, große Datenmengen zu archivieren.

- **Ortsunabhängiger Zugriff:** Mit der Verbreitung des Internet konnten Menschen plötzlich auf vielfältige Informationen zugreifen, unabhängig davon, an welchem Ort die Daten tatsächlich gespeichert waren. Früher musste man sich z. B. zuerst Bücher kaufen oder in Bibliotheken ausborgen, um sich über ein Thema einen ersten Überblick verschaffen zu können. Heute genügen dafür ein paar wenige Webklicks – sei es daheim, unterweges per Handy oder in der Schule. Die deutschsprachige Ausgabe der freien Internet-Enzyklopädie *Wikipedia* enthält z. B. an die 1,3 Millionen Artikel, die englische sogar über 3,75 Millionen[7] – wo wir übrigens wieder beim enormen Speicherplatz wären.

- **Aktive Beteiligung der Nutzer/innen:** Mit dem Erfolg so genannter „Web 2.0"-Anwendungen wie Blogs, Soziale Netzwerke, Wikis, Podcasts, Foto- und Videoplattformen, Social Bookmarks und vielen mehr hat sich die Internetnutzung verändert. Das Internet ist zu einem „Mitmach-Medium" geworden. Anstatt nur passiv von Website zu Website zu surfen, werden von immer mehr Menschen aktiv nach Lust und Laune eigene Inhalte veröffentlicht.

Diese Gründe – also viel Speicherplatz, ortsunabhängiger Zugriff und die aktive Beteiligung der Nutzer/innen – spielen eine wichtige Rolle für den enormen Erfolg von Computer und Internet. Gleichzeitig, sozusagen als „Kehrseite der Medaille", ergeben sich aus der Unmenge an leicht verfügbaren Daten viele neue Herausforderungen für den Datenschutz. Das verleitet Pessimisten sogar dazu, von einem „Ende der Privatsphäre" zu sprechen oder zumindest davor zu warnen.

Selbstverständlich ist es nicht nur deine Aufgabe, dich um den Schutz deiner Privatsphäre zu kümmern. Datenschutz kann nur eine **gemeinsame Verantwortung aller Beteiligten** sein – dazu zählen neben dir vor allem auch Unternehmen (z. B. dein Internet-Provider, Website-Betreiber etc.), der Gesetzgeber (er legt fest, was erlaubt ist und was nicht) und Behörden (z. B. die Polizei).

[7] Quelle: Wikipedia: http://de.wikipedia.org/wiki/Wikipedia:%C3%9Cber_Wikipedia (25.11.2011).

2.2 Digitale Spuren im Netz

Wenn du im Internet surfst, werden an verschiedenen Stellen eine Menge Daten über dich und darüber, was du im Internet machst, gespeichert. Deshalb ist es wichtig, dass es Regeln gibt, was mit deinen Daten passieren und wer auf welche Daten zugreifen darf.

Nicht immer kann man sich aber darauf verlassen, dass diese Regeln tatsächlich eingehalten werden. Gründe dafür gibt es mehrere: von menschlichen Fehlern über kriminelle Handlungen bis hin zu dem Umstand, dass oft noch nicht im Detail klar ist, wie genau Gesetze im Internet anzuwenden sind.

Deshalb lohnt es sich, sich auch selbst aktiv um den Schutz der eigenen Privatsphäre im Internet zu kümmern!

TIPP: Was sollte ich vor der Veröffentlichung privater Daten im Web beachten?

WO, WIE und WIEVIEL du dich im Netz involvierst und präsentierst, musst du natürlich selbst für dich entscheiden. Aber vergiss nicht: Das Internet hat ein langes Gedächtnis!
Damit du einmal nicht in unangenehme Situationen kommst, stelle dir vor der Veröffentlichung privater Informationen, Fotos etc. im Web immer folgende Fragen:

- Würde ich diese Informationen oder Fotos auch meinen Eltern, meinen Lehrer/innen oder sogar einem fremden Spaziergänger im Park erzählen/zeigen?
- Könnte jemand diese Angaben gegen mich oder zu meinem Nachteil verwenden?
- Könnten mir die Inhalte zu einem späteren Zeitpunkt (z. B. in fünf Jahren) peinlich oder unangenehm sein?
- Könnte eine Veröffentlichung für eine andere Person Nachteile bringen?

Bei aller Vorsicht darf man aber natürlich nicht vergessen, dass **die Chancen und der Nutzen des Internet die Risiken bei weitem übertreffen!** Es kommt – wie überall im Leben – darauf an, was man selbst daraus macht. Entscheidend für den Schutz der Privatsphäre ist, möglichst im Blick zu behalten, welche Informationen wo und an wen weitergegeben werden. ☺

Ein Beispiel:

Nehmen wir an, so wie in Abbildung 1 dargestellt, du lädst ein Foto auf eine Online-Community. Hier ist beispielhaft beschrieben, welche Datenspuren über dich dabei entstehen können. In Kapitel 4 erfährst du dann, wie du konkret den Schutz deiner Privatsphäre verbessern kannst.

- Zunächst einmal wird auf deinem Computer im Internet-Browser (z. B. *Internet Explorer* oder *Firefox*) festgehalten, wann du dich auf welchen Websites aufgehalten hast. In so genannten „Cookies“[8] können zusätzlich Daten über dich gespeichert werden.

- Wenn du ein ungesichertes WLAN-Netzwerk zum Einstieg in das Internet verwendest, kommt noch dazu, dass jemand anderer die übertragenen Daten mitlesen oder sogar deinen Internetzugang mitverwenden könnte.

- Beim Internet-Provider – das ist jenes Unternehmen, das dir den Zugang zum Internet bereit stellt – werden ebenfalls Daten gespeichert. Zum Beispiel deine IP-Adresse[9]. Der Internet-Provider kennt also nicht nur deine Kundendaten wie Name, Adresse etc. (= „Stammdaten“). Ihm stehen prinzipiell auch Informationen zur Verfügung, wann du z. B. auf welche Websites zugegriffen hast (= „Verkehrsdaten“). Natürlich könnte der Internet-Provider auch mitlesen, welche Inhalte du überträgst (= „Inhaltsdaten“). Inhaltsdaten unterliegen aber grundsätzlich, genauso wie Verkehrsdaten, dem Kommunikationsgeheimnis.

  In der Praxis gibt es zahlreiche rechtliche und politische Diskussionen, wem (z. B. der Polizei oder den Rechteinhabern von Musikstücken oder Filmen) und unter welchen Voraussetzungen Internet-Provider Auskunft über die Internetnutzung ihrer Kund/innen geben müssen. Weitere Informationen dazu findest du auf Seite 31.

- Vom Internet-Provider aus geht dein Foto in die Weiten des Internet. Deine Daten legen einen langen Weg über zahlreiche Netzwerkcomputer zurück, bis dein Foto schließlich auf der Online-Community landet. Auf diesem Weg sind deine Daten prinzipiell ebenfalls ungeschützt. Eine Ausnahme stellen verschlüsselte Verbindungen dar. Diese erkennst du daran, wenn in der Adresszeile deines Internet-Browsers die Adresse mit „https://“ und nicht mit „http://“ beginnt. Das ist etwa bei der Eingabe einer Kreditkartennummer oder beim Online-Banking besonders zu beachten.

- Wenn du Daten über dich (wie z. B. dein Foto) in der Online-Community abgespeichert hast, hat auch der Betreiber der Community Zugriff auf alle deine Daten.

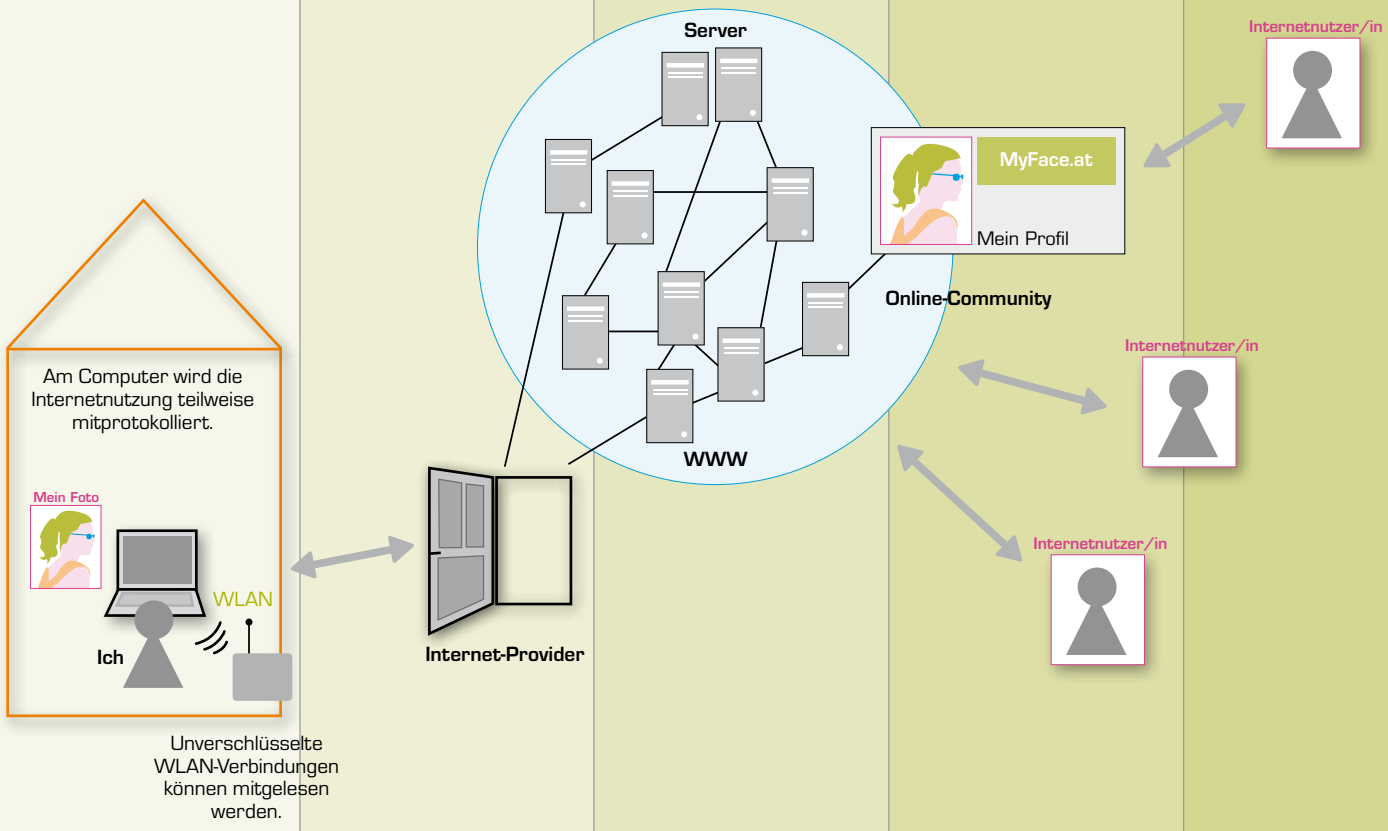
- Und natürlich können andere Internetnutzer/innen dein Foto sehen, herunterladen und beliebig weiterverwenden. Einstellungen zum Schutz der Privatsphäre direkt in der Community helfen dir, dies zu kontrollieren.

Bei jeder Aktivität im Internet entstehen also zahlreiche digitale Spuren, viele davon ganz unbemerkt.

[8] „Cookies“ sind kleine Dateien auf deinem Computer, die dein Surfverhalten mitprotokollieren.
[9] Die „Internet Protokoll“-Adresse ist eine eindeutige Nummer, die jedem Computer im Internet zugeordnet ist.

Abbildung 1: Datenspuren im Internet am Beispiel des Hochladens eines Fotos auf eine Online-Community

Bei jeder Aktivität im Internet hinterlässt man zahlreiche digitale Spuren, die für andere zugänglich sein können.



Computer mit Internetzugang	Internet-Provider	Internet	Online-Community	Internet-nutzer/innen
	Internet-Provider besitzen Stamm- und Verkehrsdaten über dich.	Daten werden im Internet meistens unverschlüsselt übertragen.	Website-Betreiber haben Zugriff auf die Daten, mit denen du dich registriert hast und alle Daten, die du hochgeladen hast.	Andere Internetnutzer/innen können alle deine öffentlich verfügbaren Daten einsehen und weiterverwenden.

Welche ganz alltäglichen Folgen das unüberlegte Hochladen eines Fotos ins Internet haben kann, zeigt dir der Video-Clip „Date“ unter www.watchyourweb.de.

Interessant zu wissen

Ein gutes Beispiel für das lange Gedächtnis des Internet ist die *Wayback Machine* der Plattform **www.archive.org**. Seit 1996 werden dort Millionen Online-Inhalte abgespeichert und so z. B. längst offline genommene Websites wieder abrufbar gemacht. Gib einfach mal eine beliebige URL in das Suchfeld ein und schaue, wie sich die Seite mit den Jahren verändert hat.

Das Geschäft mit den Daten

Personenbezogene Daten sind für die Wirtschaft von großer Bedeutung, weil damit gezielt mögliche Kund/innen angesprochen werden können. Es gibt auch einen eigenen Wirtschaftszweig, der sich diese Tatsache zu Nutze macht: jenen der **„Adresshändler“**. Sie sammeln (z. B. über Gewinnspiele oder Umfragen) unzählige persönliche Informationen von Konsument/innen und verkaufen diese gewinnbringend an Unternehmen weiter. Ob Alter, Ausbildung, Beruf, Reisegewohnheiten, Einkaufsverhalten, Wohnverhältnisse oder Hobbys – aus Millionen Datensätzen können sich die Unternehmen die passenden Adressen heraussuchen. Pro Datensatz lassen sich so im Durchschnitt ein bis zwei Euro verdienen!

Ist das überhaupt erlaubt?

In der EU muss eine Person grundsätzlich um Erlaubnis gefragt werden, bevor persönliche Daten für Werbezwecke über sie gesammelt und gespeichert werden dürfen. Dies ist jedoch bei weltweiten Internetangeboten nicht immer der Fall.

- Halte auf der Website Ausschau nach der so genannten **„Datenschutzerklärung“**, die auch manchmal Teil der Allgemeinen Geschäftsbedingungen (AGB) ist. Es handelt sich dabei um eine Zusammenfassung der Datenschutzbestimmungen des Anbieters. Meist kannst du diese über einen Link auf der Startseite aufrufen.

- Besonders vorsichtig solltest du bei **Angaben zur Weitergabe von Daten** sein. Nach EU-Recht musst du genau informiert werden, an wen und zu welchem Zweck deine Daten weitergegeben werden. Wenn du z. B. nur ganz allgemein aufgefordert wirst, einer Weitergabe deiner Daten „an Dritte“ zuzustimmen, musst du damit rechnen, dass deine Daten möglicherweise auch an Unbekannte weitergegeben werden.

Neben Adresshändlern nutzen aber noch viele weitere Unternehmen die Vorteile der Verknüpfung von persönlichen Daten. **Online-Shops** verwenden deine Daten, um dir z. B. beim nächsten Besuch individuell zugeschnittene Angebote machen zu können. Besonders eifrige Datensammler sind **Suchmaschinen** mit ihren zahlreichen Services (von Suchabfragen über kostenlose E-Mail-Dienste bis hin zur Online-Bilderverwaltung), die es erlauben, ihre Nutzer/innen genau zu analysieren und zu kategorisieren. Kein Wunder also, dass die großen Suchmaschinenbetreiber ihr Geld vor allem mit der möglichst zielgruppengenauen Schaltung von Werbung verdienen. Auch in den meisten Sozialen Netzwerken ist das mittlerweile so.

2.3 Fünf gute Gründe, warum der Datenschutz im Internet besonders wichtig ist

Du hast nun schon einiges darüber erfahren, warum gerade im Internet der Schutz persönlicher Daten eine große Herausforderung ist. Hier findest du zusammengefasst die fünf wichtigsten Gründe, warum du im Web mit privaten Angaben besonders vorsichtig sein solltest:

1) **Im Web ist man nicht so anonym, wie man glaubt:** Alle Inhalte, die du ins Netz stellst, sind nicht nur für deine Freund/innen zugänglich, sondern theoretisch auch für alle anderen Internetnutzer/innen auf der Welt. Auch dir unbekannte oder weniger gut gesonnene Menschen können deine privaten Informationen also unter Umständen einsehen und für böse Absichten missbrauchen. Eine leichtfertige Weitergabe persönlicher Daten kann auch Anlass für Belästigungen bis hin zu Cyber-Mobbing sein.

2) **Das Internet vergisst nicht**: Etwas, was du heute gut findest, kann dir in einigen Jahren sehr unangenehm oder peinlich sein. Einmal veröffentlichte Daten sind oft nicht mehr zu entfernen. Denke z. B. an Partyfotos, auf denen du ziemlich „hinüber" bist – sie könnten dir bei der späteren Ausbildungs- oder Jobsuche schaden.

3) **Der erste Eindruck zählt:** Communitys und andere Internetplattformen werden von Lehrer/innen, potenziellen Arbeitgeber/innen, Mitschüler/innen, Bekannten etc. genutzt, um mehr über dich zu erfahren. Glaubst du, dass sie mit Hilfe deiner Online-Angaben zu Interessen, Hobbys, Vorlieben, Freunden, Einstellungen etc. ein von dir erwünschtes Bild von deiner Person vermittelt bekommen?

4) **Nicht alles ist, wie es scheint:** Glaube nicht alles, was andere Menschen im Internet erzählen – sich als jemand anderer auszugeben bzw. etwas vorzuspielen, ist im Web besonders einfach. Informationen über andere Personen im Internet müssen nicht wahr sein.

5) **Ein Paradies für Datensammler:** Immer wieder tauchen Meldungen über Pannen auf, durch die der unerlaubte Zugriff Dritter auf Nutzer/innendaten in z. B. Sozialen Netzwerken möglich wurde. E-Mail-Adressen und andere private Daten werden für z. B. unerwünschte E-Mail-Werbung missbraucht, Fotosammlungen widerrechtlich auf Tauschbörsen zum Download angeboten oder Userprofile einfach weiterverkauft.

2.4 Der gute Ruf im Internet

Immer mehr Menschen hinterlassen ihre Spuren im Internet und prägen dadurch – ob sie wollen oder nicht – ihr „digitales Image". **Jede Spur, die wir im Internet hinterlassen, haftet an uns wie eine Tätowierung** – im Web bleibt nichts verborgen und was einmal online ist, kann nur in seltenen Fällen ganz ausradiert werden. So ergibt sich aus vielen, vielen kleinen Puzzlesteinchen ein Gesamtbild einer Person, das nicht immer vorteilhaft oder wahr sein muss, und schon gar nicht vollständig sein kann.

Interessant zu wissen

Erstaunlich viele Österreicher/innen fürchten sich davor, dass andere Menschen Informationen über sie im Internet finden könnten: Über 50 % bereitet der „digitale Fußabdruck" ein ungutes Gefühl.[10] Auf der anderen Seite hat sich in den letzten beiden Jahrzehnten ein gewisser **Hang zur Offenherzigkeit** durchgesetzt, der sich schon länger in Talkshows, Boulevardmagazinen und Reality-Formaten wie *Big Brother, Popstars* oder *Austria's Next Topmodel* widerspiegelt, und sich nun eben auch im Web zeigt.

Schon eine einfache Abfrage über eine Suchmaschine (z. B. indem man den Namen einer Person eingibt) kann heutzutage peinliche Hobbys, unvorteilhafte Fotos oder ähnlich unbequeme Tatsachen ans Licht bringen. **Zudem überschneidet sich zunehmend Privates mit Beruflichem.** Das heißt, nicht nur die eigenen Freunde oder Familienmitglieder interessieren sich für das, was du im Internet tust bzw. was es dort über dich zu finden gibt. Auch z. B. Personalabteilungen machen sich online ein Bild über ihre Bewerber/innen.

Die eigene Imagepflege im Netz wird immer wichtiger. Dazu gehört aber nicht nur Vorsicht bei der Preisgabe persönlicher Daten. Auch echte und ehrliche Angaben über einen selbst sind langfristig entscheidend für einen guten Ruf. Denn Glaubwürdigkeit spielt im Internet eine besonders wichtige Rolle.

Mach doch einmal den Test und gib deinen Namen in eine der großen Suchmaschinen ein, um deinen eigenen Ruf im Internet zu kontrollieren.

[10] Quelle: GfK Austria: http://www.gfk.at/imperia/md/content/gfkaustria/data/press/2009/2009-01-12_internetnutzung_sozfo.pdf (11.01.2010).

3 Gesetzliche Bestimmungen: Meine Rechte und Pflichten

Die wichtigsten rechtlichen Aspekte für den Datenschutz auf einen Blick:

- Der Schutz von Daten („personenbezogenen Daten") und der Schutz der Privatsphäre sind in Österreich gesetzlich geregelt.
- Andere dürfen deine Daten nur für einen mit dir vereinbarten Zweck verwenden *(so eine Vereinbarung kann z. B. nach Zustimmung der Allgemeinen Geschäftsbedingungen vorliegen)* oder wenn es per Gesetz erlaubt ist.
- Du hast das Recht, Auskunft darüber zu erhalten, welche Daten über dich gespeichert sind und kannst diese jederzeit löschen lassen, wenn die Datenverwendung nicht gesetzlich vorgeschrieben ist.
- Die Datenschutzkommission kann dir helfen, wenn andere deine Datenschutzrechte verletzt haben.
- Im Internet ist es oft schwierig, seine Rechte durchzusetzen. Deshalb solltest du dir genau überlegen, welche Daten du im Netz von dir preisgibst.

Grundrecht auf Datenschutz in Österreich (Auszug)

§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht (...)

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, d. h. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;

2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

Datenschutz spielt eine wichtige Rolle im österreichischen Recht und wird auch als **Grundrecht jedes Menschen** gesehen. Im Datenschutzgesetz ist geregelt, wer unter welchen Bedingungen welche Daten besitzen und verwenden darf. In Österreich ist der §1 des Datenschutzgesetzes auch Teil der Verfassung (siehe Kasten links), die in der Rechtsordnung über einem „normalen" Gesetz steht. Das bedeutet, dass es strengere Voraussetzungen gibt, wenn man in diese Rechte eingreifen will. Du hast ein Recht auf Datenschutz sowohl gegenüber Behörden als auch gegenüber Privatpersonen oder Unternehmen.

Außerdem ist in verschiedenen Gesetzen ein so genanntes **Brief- und Telekommunikationsgeheimnis** verankert, das für den Schutz deiner persönlichen Daten ebenfalls wichtig ist.

Die Bedeutung des Datenschutzes zeigt sich auch darin, dass in der **Europäischen Menschenrechtskonvention (EMRK)** das „Gebot der Achtung der Privatsphäre" (siehe Kasten rechts) festgeschrieben ist.

Artikel 8. EMRK – Gebot der Achtung der Privatsphäre

(1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutze der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

Interessant zu wissen

Daten dürfen grundsätzlich nur verarbeitet oder weitergegeben werden, wenn es das Gesetz erlaubt oder der/die Betroffene (= jene Person, deren Daten verwendet werden) dem zugestimmt hat. Die Daten dürfen aber immer nur so genutzt werden, wie es mit dem/der Betroffenen ausgemacht wurde.

Beispiel:
Du bestätigst im Zuge einer Bestellung in einem Online-Shop, dass dieser deine Daten für Werbezwecke an das befreundete Unternehmen X weitergeben darf. Wenn das Unternehmen X deine Daten bekommt, ist das also in Ordnung. Gibt der Online-Shop die Daten darüber hinaus aber an das Unternehmen Y weiter, ist das nicht erlaubt, da du dem ja nicht zugestimmt hast. In diesem Fall hast du z. B. das Recht, deine Daten beim Unternehmen Y löschen zu lassen.

3.1 Welche Daten sind geschützt?

Vereinfacht lässt sich sagen, dass alle Daten, die man mit einer bestimmten Person in Verbindung bringen kann (= **personenbezogene Daten**), geschützt sind.

Beispiel:

In einem Community-Profil ist neben dem vollen Namen einer Person auch deren Telefonnummer angegeben.

Hier ist die Telefonnummer, weil sie mit der Person (Namen) verknüpft ist, ein personenbezogenes Datum.

Eine wichtige Unterscheidung innerhalb der personenbezogenen Daten besteht zwischen **sensiblen** und **nicht-sensiblen Daten**.

Sensible Daten betreffen den persönlichsten Lebensbereich einer Person. Dazu gehören die ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder das Sexualleben.

Beispiel:

In einem Blog wird gepostet, dass eine bestimmte Person eine schwere Krankheit hat, ohne dass dies allgemein bekannt war.

Hier ist die Krankheit eine sensible Information, weil sie die Gesundheit, die zum „persönlichsten Lebensbereich" einer Person zählt, betrifft.

Die Verwendung von sensiblen Daten ist nur in wenigen Ausnahmefällen erlaubt – beispielsweise wenn der/die Betroffene die Daten selbst veröffentlicht hat. Natürlich darf aber z. B. ein Krankenhaus die Krankendaten seiner Patient/innen speichern oder eine politische Partei ein Mitgliedsverzeichnis führen.

Beispiel:

Jemand veröffentlicht in einem Internetforum, welche Partei er/sie wählen wird.

WICHTIG: Veröffentlicht man sensible Daten über sich selbst, dürfen diese Informationen auch ohne die eigene Zustimmung von anderen Personen verwendet und weiterverbreitet werden.

Nicht ganz so streng verhält es sich bei **nicht-sensiblen** – aber trotzdem personenbezogenen – **Daten** (z. B. Adresse, Telefonnummer, Geburtsdatum, Beruf). Diese darf man verwenden, wenn:

- es durch ein Gesetz erlaubt ist,
- der/die Betroffene zustimmt (z. B. bei der Bestellung in einem Online-Shop, wobei man natürlich die Zustimmung zurücknehmen kann) oder die Daten selbst veröffentlicht,
- lebenswichtige Interessen des/der Betroffenen dies erfordern (z. B. Handy-Ortung nach einem Bergunglück),
- überwiegende berechtigte Interessen eines Dritten vorliegen – dies wird aber streng beurteilt und ist in der Praxis teils umstritten (etwa die Frage, ob Banken die Daten z. B. zahlungsunfähiger Kund/innen gegenseitig austauschen dürfen, um sich vor Schaden zu schützen).

3.2 Welche Rechte habe ich, wenn meine Daten verwendet werden?

Im österreichischen Datenschutzgesetz ist genau geregelt, welche Rechte Betroffene (= jene Personen, deren Daten verwendet werden) haben. Diese gelten vor allem gegenüber denjenigen, die die Daten speichern (= so genannte „Datenverwender"). Hier eine kurze Vorstellung der Rechte:

- **Informationen über den Datenverwender:** Bevor du persönliche Daten von dir weitergibst, hast du das Recht, darüber informiert zu werden, **welche Daten** über dich gespeichert und **wie** diese verwendet werden (z. B. in den Allgemeinen Geschäftsbedingungen eines Online-Shops bevor du dort etwas bestellst).
- **Auskunftsrecht:** Du hast darüber hinaus auch ohne Anlassfall das Recht bei einem Datenverwender nachzufragen, **welche Daten** über dich gespeichert, **woher** diese bezogen und **an wen** sie übermittelt wurden.
- **Richtigstellung und Löschung:** Es ist natürlich auch wichtig, dass keine **falschen Daten** über dich verwendet werden. Du kannst immer verlangen, dass der Datenverwender deine Daten richtigstellt oder auch wieder löscht.
- **Widerspruch:** Dieser besteht darin, dass du dem Datenverwender **jederzeit untersagen** kannst, Daten von dir weiterzuverwenden oder weiterzugeben. Von diesem Recht gibt es allerdings Ausnahmen, etwa wenn die Verwendung gesetztlich vorgesehen ist. Es gibt also z. B. keinen Widerspruch gegen Verarbeitungen im Grundbuch oder in Polizeiakten.

Beispiel:

Eine unbekannte Firma schickt dir immer wieder Briefe oder Prospekte. Du kannst die Firma einerseits dazu auffordern, dir zu sagen, welche Daten sie von dir besitzt und woher diese stammen. Andererseits kannst du von der Firma auch verlangen, dass sie dir künftig keine Materialien mehr schickt und deine Daten unwiderruflich löscht.

Wurden Daten missbräuchlich verwendet oder veröffentlicht, hast du in der Regel einen **Anspruch auf Schadenersatz**.

TIPP: Wie nehme ich meine Rechte wahr?

Du hast das Recht, einmal im Jahr **kostenlose Auskunft** von einem Datenverwender über deine gespeicherten Daten zu erhalten. Die Aufforderung dazu schickst du am besten mittels **eingeschriebenen Briefs**. Um zu beweisen, dass du auch wirklich die Person bist, um die es geht, solltest du dem Brief eine Ausweiskopie beilegen.

Sollte das nicht erfolgreich sein und möchtest du rechtlich gegen einen Datenverwender vorgehen, gibt es zwei Möglichkeiten:

- Bei der **Datenschutzkommission** (kurz: DSK, siehe auch Seite 29) kannst du in jedem Fall dein Recht auf Auskunft durchsetzen, egal ob es sich z. B. um eine Behörde oder ein Unternehmen handelt. Darüber hinaus kannst du bei der DSK gegen eine Behörde auch eine Beschwerde einreichen. Die DSK fällt dann die Entscheidung über das Datenschutzproblem.

- Für alle anderen Ansprüche gegen Privatpersonen oder Unternehmen (Löschung, Widerspruch etc.) musst du dich direkt an ein **Gericht** wenden und Klage einbringen. Je nach Problem kann es auch sein, dass du einen Anwalt brauchst.

Probleme mit Datenverwendern außerhalb der EU

Wenn Datenverwender wie Unternehmen, Behörden etc. ihren Sitz nicht in der EU haben, hat man es **sehr schwer, seine Rechte durchzusetzen** (auch wenn man im Recht ist!).

Das Problem liegt hier einerseits in der Frage, welches Gericht zuständig ist – es könnte sein, dass man seine Ansprüche z. B. vor einem Gericht in den USA geltend machen muss. Andererseits ist die Frage, das Recht welchen Landes das Gericht anwenden muss, z. B. wenn ein Gericht in der EU ein Datenschutzproblem nach russischem Recht beurteilen muss. Das klingt zwar etwas abenteuerlich, ist aber durchaus möglich – gerade bei Internetfällen, wo der länderübergreifende Datenaustausch sehr häufig ist.

Es kann auch vorkommen, dass ein Gericht zwar eine Entscheidung fällt, diese aber nicht durchgesetzt werden kann, weil z. B. das Unternehmen in einem Staat sitzt, mit dem es keine entsprechenden internationalen Abkommen gibt. D.h. es gibt zwar ein Urteil, letztlich hat es aber keine Folgen.

Du kannst dir also vorstellen, wie schwierig es bei Datenschutzverstößen im Internet sein kann, zu seinem Recht zu kommen. Abgesehen davon sind **außerhalb der EU die Gesetze zum Schutz deiner Daten meist weniger streng**.

Sind meine Bilder auch geschützt?

Es gibt im österreichischen Urheberrechtsgesetz das so genannte **„Recht am eigenen Bild“**. Fotos und/oder deren Begleittext, die die so genannten „berechtigten Interessen“ der Personen auf dem Bild verletzen, dürfen nicht veröffentlicht werden. Aufnahmen an öffentlichen Plätzen sind üblicherweise unbedenklich, wenn aber die Situation für die Abgebildeten nachteilig ist *(z. B. Oben-ohne-Foto am Strand)*, ist die Abbildung in jedem Fall schützenswert.

Im privaten Bereich sind Interessen noch viel früher beeinträchtigt, dies gilt auch für private geschlossene Veranstaltungen *(z. B. Partys bei dir oder bei Freund/innen)*. **Veröffentlichte Fotos dürfen die Abgebildeten nicht „bloßstellen“ oder „herabsetzen“**, dies kann bei Bildern von wilden Partys aber schnell der Fall sein. Es reicht allerdings nicht, wenn sich der/die Abgebildete auf einem Foto einfach nur hässlich findet – eine Bloßstellung muss objektiv nachvollziehbar sein *(z. B. heruntergelassene Hose im Vollrausch)* und die abgebildete Person muss erkennbar sein *(z. B. ein Foto vom Hinterkopf reicht in der Regel nicht aus)*.

Entdeckst du ein für dich nachteiliges Foto im Internet, so hast du also in der Regel das Recht auf Löschung dieses Fotos. Dasselbe gilt übrigens auch für Videos.

Ein Gerücht ist allerdings, dass es keinen Schutz des Einzelnen gäbe, wenn mehrere Personen auf einem Foto abgebildet sind – das ist natürlich falsch. Selbst wenn jemand in einer Menschenmenge nachteilig abgebildet wurde und erkennbar ist, kann er/sie sein/ihr „Recht am eigenen Bild“ geltend machen.

Darüber hinaus sind **auch Bilddaten personenbezogene Daten**, also gilt auch für diese das Datenschutzgesetz!

Welche Daten muss ich im Internet bekannt geben?

Das Datenschutzgesetz regelt, welche deiner Daten unter welchen Bedingungen geschützt sind. Es gibt aber gerade auch im Internet viele Situationen, **wo du Daten über dich angeben musst**:

- Für **Websites** (auch private!) gibt es eine so genannte **„Impressumspflicht“**; das bedeutet, dass der/die Betreiber/in der Website seinen/ihren Namen und Wohnort (nicht die genaue Adresse) auf der Seite veröffentlichen muss.
- **Angabe persönlicher Daten im Internet:** Wenn man sich im Internet für verschiedene Dienste anmelden möchte, muss man dabei auch immer wieder Daten zur eigenen Person angeben (Name, Geburtsdatum, Adresse etc.). Viele Internetnutzer/innen geben dabei absichtlich **falsche Daten** an. Hier ist aber Vorsicht geboten: Wenn man falsche Daten angibt, um sich eine (kostenpflichtige) Leistung zu erschleichen, kann dies als **Betrug** gewertet werden!

Beispiel:

Du meldest dich unter falschem Namen, Adresse und Geburtsdatum bei einer kostenpflichtigen Spiele-Website an, damit du keine Rechnung bekommen kannst. Das ist natürlich strafbar.

Etwas anders ist die rechtliche Situation bei vermeintlichen „Gratis"-Angeboten von Internet-Abzockern. Wenn dir der Eindruck vermittelt wird, dass ein Angebot kostenlos ist, kann dir auch kein Betrug vorgeworfen werden. Mehr Informationen zu solchen „Gratis"-Angeboten findest du auf www.ombudsmann.at (Menüpunkt „Häufige Fragen").

Gibt es die Möglichkeit, gegen nachteilige Aussagen über mich vorzugehen?

Wenn es darum geht, deinen Ruf im Internet zu schützen, finden sich im österreichischen Strafrecht folgende relevante Bestimmungen: die „Üble Nachrede", die „Beleidigung" und die „Verleumdung".

- Eine **Beleidigung** liegt vor, wenn jemand vor mindestens zwei zusätzlichen Personen beschimpft oder verspottet wird *(z. B. „saublöd", „bescheuert")*. Das gilt z. B. auch, wenn eine Person unter Angabe ihres echten Namens auf einer Website, in Chats, Foren, Communitys etc. angegriffen wird. Oder sogar, wenn die beleidigte Person regelmäßig unter dem gleichen Nickname auftritt und diesen dann aufgrund des geschädigten Rufs nicht mehr verwenden kann. Wenn Beleidigungen in bestimmten Kreisen oder Situationen allerdings üblich sind („millieubedingte Unmutsäußerungen"), wird das nicht so streng beurteilt. Ein typisches Beispiel: der Fußballplatz.

- **Üble Nachrede** ist der Vorwurf einer verächtlichen Eigenschaft oder Gesinnung, eines unehrenhaften Verhaltens *(z. B. „Lügner", „Betrüger")* oder eines Verhaltens gegen die guten Sitten in der Öffentlichkeit. Um sich strafbar zu machen, reicht schon die Anwesenheit einer dritten Person. Eine wahre Behauptung ist nicht strafbar, allerdings muss der Behauptende vor Gericht die Wahrheit beweisen können.

- Eine **Verleumdung** liegt vor, wenn man jemandem die Begehung einer Straftat vorwirft, obwohl man weiß, dass der Vorwurf nicht stimmt. Durch den Vorwurf muss der/die Betroffene der Gefahr einer behördlichen Verfolgung (durch Polizei oder Staatsanwaltschaft) ausgesetzt sein *(z. B. „Der Karli hat gestern vom Schulbuffet gestohlen.")*.

Bei Problemen mit nachteiligen Aussagen, die sich nicht so leicht lösen lassen, hilft dir der Internet Ombudsmann (**www.ombudsmann.at**) kostenlos weiter!

3.3 Wichtige Institutionen für den Datenschutz

Die Datenschutzkommission

Die österreichische Datenschutzkommission (DSK), **www.dsk.gv.at** , ist eine Kontrollstelle für alle Fragen und Probleme rund um den Datenschutz. Die DSK hat verschiedene Möglichkeiten, Datenschutzverstöße zu sanktionieren: von Empfehlungen, über eine Überprüfung der Verwendung und verbindlichen Entscheidungen bis hin zu einer Strafanzeige bei den Strafbehörden.

Mit welchen Problemen kann man sich an die DSK wenden?

Hat man ein Datenschutzproblem mit einer staatlichen Behörde, ist die DSK für das Verfahren und die Entscheidung zuständig. In diesem Fall kann man direkt bei der DSK eine Beschwerde einreichen. *Ein Beispiel dazu: Ein Polizist erzählt herum, welche Straftaten eine Person begangen hat.*

Wenn der Datenverwender statt einer Behörde eine Privatperson oder ein Unternehmen ist, muss man grundsätzlich seine Ansprüche vor einem Gericht durchsetzen. Aber auch hier kann man sich an die DSK wenden, die bei Rechtsverletzungen eine Empfehlung aussprechen kann. Diese ist zwar nicht verbindlich, hat aber durch den Status der DSK eine große praktische Bedeutung.

Was ist das Datenverarbeitungsregister (DVR)?

Oft sieht man bei z. B. Online-Shops im Impressum eine so genannte **„DVR-Nummer“**. Dies bedeutet, dass sich die Unternehmen **bei der DSK registrieren** mussten, um die Daten z. B. ihrer Kunden/Kundinnen zu speichern. In einigen Fällen sieht das Gesetz nämlich vor, dass ein Anbieter genau sagen muss, **welche Daten** er **von wem** und **zu welchem Zweck** verwenden und speichern will, und dies auch überprüfen lassen muss. Nicht melden muss man z. B. Datenanwendungen wie ein privates Telefonbuch am Computer sowie Kunden- oder Personaldatenbanken eines Unternehmens.

Der Datenschutzrat

Der Datenschutzrat ist ein im Bundeskanzleramt eingerichteter Beirat, der den Bund und die Länder in datenschutzrechtlichen Fragen berät. Darüber hinaus gibt der Rat auch Stellungnahmen zu Gesetzesentwürfen ab.

Der Europäische Datenschutzbeauftragte

Der Europäische Datenschutzbeauftragte überwacht die Institutionen und Organe der Europäischen Union bei ihrer Verwendung von personenbezogenen Daten. Er kann eine Datenverarbeitung verbieten, den/die Verantwortliche/n ermahnen oder verwarnen und auch Daten löschen lassen. Man kann den Datenschutzbeauftragten auch kontaktieren, wenn man sich von einer EU-Institution in seinen Datenschutzrechten verletzt fühlt.

Die Artikel 29 Datenschutzgruppe

Die Artikel 29 Datenschutzgruppe, die aus Datenschutz-Expert/innen aller EU-Mitgliedsstaaten besteht, ist ein unabhängiges Gremium, das die Europäische Kommission in Datenschutzfragen berät. Diese gibt auch Empfehlungen zum Datenschutz ab und fördert die einheitliche Anwendung der Datenschutzgrundsätze.

Diese Einrichtung befasst sich auch mit den Datenschutzrechten von Kindern. Im „Arbeitspapier 1/2008 zum Schutz der personenbezogenen Daten von Kindern“[11] finden sich auch Empfehlungen zum Datenschutz in Schulen.

[11] Quelle: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp147_de.pdf (25.11.2011).

3.4 Welche Rechte und Möglichkeiten haben Dritte, Daten zu erhalten?

Immer wieder gibt es die Frage, welche Daten die Polizei oder Unternehmen von Datenverwendern (z. B. Internet-Provider, Online-Shop, Website-Betreiber) über eine Person herausfordern dürfen.

Grundsätzlich sind Unternehmen ihren Kund/innen **zur Geheimhaltung persönlicher Daten verpflichtet**, es gibt jedoch Ausnahmen.

Fallbeispiel: Filesharing

Es ist ein viel diskutiertes Problem: Jemand lädt sich über eine **Online-Tauschbörse** urheberrechtlich geschützte Filme oder Musik herunter. Was viele Nutzer/innen aber nicht wissen: Wenn man diese Dateien herunterlädt, bietet man sie in der Regel automatisch auch wieder anderen Personen zum Download an. Urheberrechtlich ist **das Anbieten dieser Dateien** klar verboten. Deswegen versuchen die Urheber/innen (und ihre Rechtsvertreter/innen) jene Personen zu finden, die urheberrechtlich geschütztes Material im Internet verbreiten.

Bei vielen Filesharing-Programmen ist allerdings nur die IP-Adresse[12] der Nutzer/innen angegeben. Die Urheber/innen haben also vorerst keine Informationen, wer hinter einer bestimmten IP-Adresse steht und die Dateien angeboten hat. Hier stehen sich einerseits die Urheber/innen, die die Personen finden wollen, die ihre Rechte verletzt haben, und die Internet-Provider, die ihren Kund/innen zum Schutz der Daten verpflichtet sind, gegenüber. **In der Praxis müssen die österreichischen Provider diese Daten derzeit nicht herausgeben** (Stand: Oktober 2011).
Man darf die derzeitige Situation aber nicht als „Freibrief" missverstehen. Das unerlaubte Anbieten urheberrechtlich geschützter Werke ist und bleibt eine Straftat. Aufgrund großer wirtschaftlicher Interessen handelt es sich aber hierbei um ein heiß umkämpftes Thema, weshalb es in Zukunft sicher noch viele Änderungen geben wird.

Interessant zu wissen

Welche Daten darf der Provider überhaupt speichern?

Ein Internet-Provider darf Daten, wie z. B. welche/r Nutzer/in zu welchem Zeitpunkt eine bestimmte IP-Adresse verwendet hat, nur so lange speichern, wie dies zur Verrechnung notwendig ist (d. h. bis die Einspruchsfrist für die Rechnung abgelaufen ist).

Es gibt aber in der EU eine Vorgabe für die Pflicht zur Speicherung solcher Daten – die so genannte **„Vorratsdatenspeicherung"**: Es wurde eine EU-Richtlinie beschlossen, in der steht, dass z. B. der Internet-Provider genau die oben genannten Daten – wer wann welche IP-Adresse hatte – zu Strafverfolgungszwecken speichern muss. Die Umsetzung der Richtlinie tritt in Österreich am 1. April 2012 in Kraft. Kritiker der Vorratsdatenspeicherung wenden ein, dass damit u. a. erstmals umfassend das Internetnutzungsverhalten der Bevölkerung gespeichert werden soll. Diese ohne konkreten Verdacht – „auf Vorrat" – erfassten Daten könnten leicht missbraucht werden und sind ein Schritt zu einer übermäßigen Überwachung, so die Befürchtungen. Befürworter erhoffen sich Vorteile für die Verbrechensbekämpfung.

[12] Die Internet-Protokoll-Adresse ist eine eindeutige Nummer, die jedem Computer im Internet zugeordnet ist und damit die Identifikation eines benutzten Computers ermöglicht.

Fallbeispiel: Intime Daten auf Websites

Beispiel:

Jemand postet auf seiner Website intime Details über dich. Du kannst den Internet-Provider, bei dem die Website gespeichert ist, kontaktieren, um eine Herausgabe von Name und Adresse zu verlangen, damit du gegen diese Person rechtliche Schritte unternehmen kannst. Der Betreiber ist auch verpflichtet, illegale Inhalte zu entfernen oder den Zugang zu sperren, sobald er von diesen Kenntnis hat.

Hier geht es vor allem um das Problem, wie man unbekannte Personen, die Daten im Internet veröffentlicht haben, erreichen kann. Es ist meist schwer, im Netz die Identität von Personen herauszufinden. Leichter ist es, den **Betreiber der Website** (z. B. Forums- oder Community-Betreiber) oder den **Provider**, der die Website hostet, zu kontaktieren. Im E-Commerce Gesetz[13] gibt es eine Regelung, in der Provider Namen und Adresse ihrer Nutzer/innen an Dritte herausgeben müssen, wenn diese glaubhaft behaupten, dass ein illegales Verhalten vorliegt.

Herausgabe von Daten an Gerichte und Polizei

Unabhängig von Ansprüchen von Privatpersonen oder Unternehmen auf die Herausgabe von Daten, haben Gerichte und Polizei **weitreichendere Rechte**.

Noch bevor es zu einem Prozess kommt, darf die **Polizei** in ihrer Ermittlung[14] auch von z. B. Internet-Providern Daten wie IP-Adresse, Postanschrift, Name usw. erheben. Dies muss zur Abwehr der konkreten Gefahrensituation allerdings unbedingt notwendig sein und es muss sich um einen so genannten „gefährlichen Angriff" (z. B. Terrorismus) oder um eine Gefahr für Leib und Leben (z. B. Lawinenunglück, Selbstmordankündigung) handeln.

Beispiel:

Eine Terroristengruppe plant in einem Internetforum einen Bombenanschlag in einer U-Bahn-Station. In diesem Fall darf die Polizei z. B. beim Internet-Provider oder Foren-Betreiber die Herausgabe aller relevanten Daten über die Beteiligten verlangen, um diese auffinden und vor der Tat stellen zu können.

In einem Verfahren vor **Gericht** kann dieses grundsätzlich alle Daten ausforschen, die für eine Lösung des Streitfalles notwendig sind. Sobald also eine Strafanzeige vorliegt oder ein Prozess stattfindet, kann der/die Richter/in die Ausforschung dieser Daten beantragen.

[13] § 18 E-Commerce Gesetz
[14] § 53 Sicherheitspolizeigesetz

4. Tipps: So schütze ich meine Privatsphäre

Welche unangenehmen Auswirkungen der leichtfertige Umgang mit privaten Informationen haben kann, hast du schon in den vorangegangenen Kapiteln erfahren. Dabei macht es keinen Unterschied, ob du nur gelegentlich etwas im Internet nachschaust oder Dauernutzer/in bist – wer heute im Internet unterwegs ist, muss sich auch mit dem Schutz der Privatsphäre beschäftigen. In diesem Kapitel erhältst du viele nützliche Tipps, wie du Risiken vermeidest und auf der sicheren Seite bist.

4.1 Mein Profil im Internet

Soziale Netzwerke, Communitys, Foren

Communitys und Foren leben davon, dass ihre Nutzer/innen möglichst viel Persönliches von sich preisgeben. Neben der totalen „Online-Freizügigkeit" gibt es aber auch die Möglichkeit, Soziale Netzwerke wie *Facebook* zu nutzen, ohne gleich sein komplettes Leben öffentlich machen zu müssen. Es lohnt sich, einige Spielregeln zum Schutz der Privatsphäre einzuhalten.

BEVOR DU EIN PROFIL ANLEGST, solltest du folgende Punkte beachten:

- **Such dir das richtige Netzwerk:** Die verschiedenen Communitys richten sich an verschiedene Zielgruppen, etwa an Kinder, Schüler/innen, Student/innen oder Berufstätige. Es gibt auch Netzwerke speziell für Mädchen (z. B. **www.mona-net.at, www.lizzynet.de**). Die Wahl des richtigen Netzwerks erleichtert dir nicht nur die Suche nach Leuten mit ähnlichen Interessen, sie dient auch deinem Schutz. Daher solltest du immer das für dich passende Netzwerk wählen.
  (Quelle: klicksafe.de)

- **Gib nicht zu viel von dir preis:** Das Internet hat ein langes Gedächtnis. Inhalte, die einmal online sind, können oft nur schwer kontrolliert und gelöscht werden. Überlege daher genau, was du von dir selbst erzählen willst! Veröffentliche keine Fotos, Videos oder Texte, die dir oder anderen peinlich sein könnten. Sei sparsam mit der Angabe persönlicher Daten (voller Name, Adresse, Wohnort, Telefonnummer etc.), die es Fremden ermöglichen, dich auch außerhalb des Internet aufzuspüren oder zu belästigen.

- **Verwende sichere Passwörter:** Verhindere, dass andere Zugriff auf dein Profil haben und in deinem Namen Einträge veröffentlichen. Halte Passwörter auch vor Freunden und Freundinnen geheim. Sicher sind Passwörter, die nur schwer zu erraten sind. Mehr dazu findest du im Kapitel 4.4 *Sicherer Umgang mit Passwörtern und Codes* ab Seite 47.

- **Wähle unterschiedliche Nutzer/innennamen und Passwörter:** Bist du in mehreren Communitys aktiv, ist es natürlich verlockend, immer die gleichen Zugangsdaten zu verwenden. Für den Fall aber, dass dein Passwort missbräuchlich verwendet wird, kann der Schaden dann viel größer ausfallen. Außerdem kann man bei unterschiedlichen Nutzer/innennamen nicht so schnell herausfinden, wo du noch überall registriert bist, und keine (falschen) Schlüsse ziehen.

- **Lies die Nutzungsbedingungen:** Wenn du dich für ein Netzwerk entschieden hast, lies dir die Nutzungsbedingungen genau durch. Dort erfährst du, welche Rechte du an den/die Website-Betreiber/in abtrittst und welche Rechte bzw. Pflichten du als Nutzer/in hast.

Passe **NACH DER ANMELDUNG** gleich die **Einstellungen zur Privatsphäre** an deine Bedürfnisse an:

- **Wer darf was sehen?** In deinem Profil kannst du festlegen, wer welche Angaben lesen darf. Empfehlenswert ist beispielsweise die Einstellung, dass dein Profil und deine Fotoalben nur für „Freunde" zugänglich sind. Aber vergiss nicht: Viele Leute, mit denen du im Internet „befreundet" bist, kennst du eigentlich kaum. Deswegen überlege dir lieber genau, welche Inhalte und Fotos du in deinem Profil veröffentlichst.

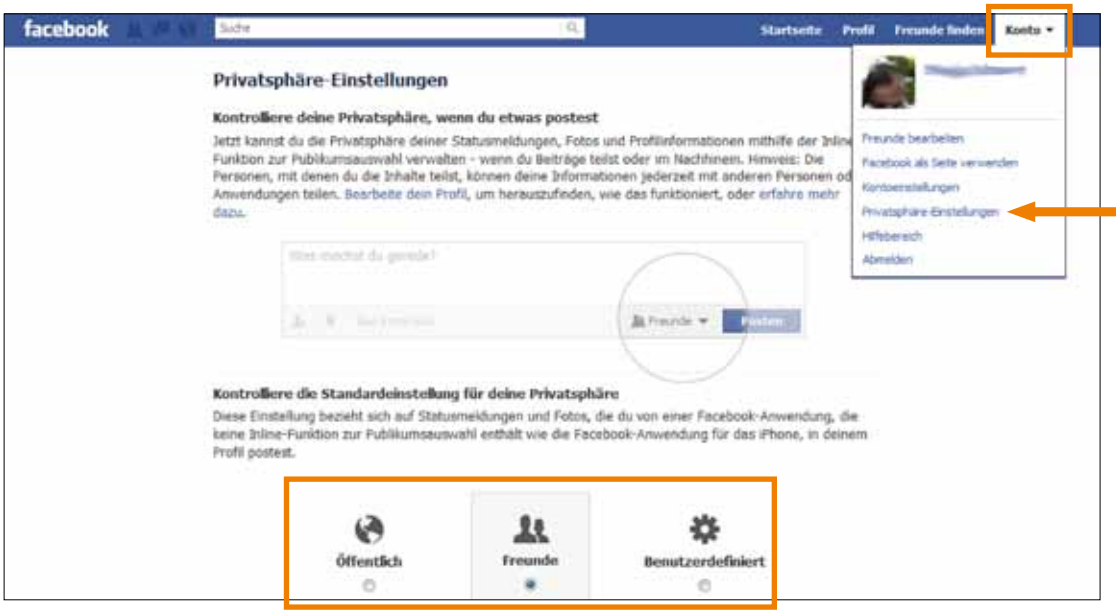


Abbildung 2: Allgemeine Datenschutzeinstellungen bei *Facebook* (Quelle: www.facebook.com)

Was aber meist alle sehen können, sind dein Name und dein Profilfoto. Deinen Nachnamen musst du auf einigen Plattformen nicht ganz ausschreiben – wenn es die Nutzungsbedingungen erlauben, wähle am besten überhaupt einen Fantasienamen (Nickname). Bei deinem Profilfoto solltest du darauf achten, dass es ok für dich ist, wenn es auch Nutzer/innen sehen, die du nicht kennst.

- **Wie werde ich gefunden?** Eine weitere wichtige Einstellungsmöglichkeit ist, welche Angaben aus deinem Profil für die Suche freigegeben sind. Dabei wird meistens unterschieden zwischen der Suche in Communitys selbst und der Suche mit Hilfe externer Suchmaschinen wie *Google, Bing, 123people.at* oder *yasni.de*. Überlege, ob es notwendig ist, dass jede/r ganz einfach herausfinden kann, wo du registriert bist. Bei vielen Anbietern kannst du externen Suchmaschinen den Zugriff auf dein Profil gänzlich verweigern.

Auf der Website www.saferinternet.at/leitfaden erfährst du in einfachen Leitfäden, wie du deine Privatsphäre in einzelnen Sozialen Netzwerken (z. B. *Facebook*) besser schützen kannst. Da sich die Privatsphäre-Einstellungen immer wieder ändern, solltest du sie zumindest monatlich überprüfen.

Auch **WÄHREND DER NUTZUNG** solltest du ein Auge auf deine Privatsphäre haben:

- **Sichtbarkeit einzelner Inhalte einschränken:** Manche Communitys erlauben dir individuelle Einstellungen für einzelne Beiträge wie etwa Postings, Fotos oder Videos. Du kannst festlegen, ob einzelne Inhalte öffentlich oder nur für „Freunde" sichtbar sind – gerade bei Fotos und Videos sind das wichtige Einstellungen! Über das Anlegen spezieller „Freundeslisten" (z. B. Enge Freunde, Familie, Schule, Arbeit, Fußballverein ...) kannst du die Sichtbarkeit deiner geteilten Inhalte noch zielgerichteter steuern.

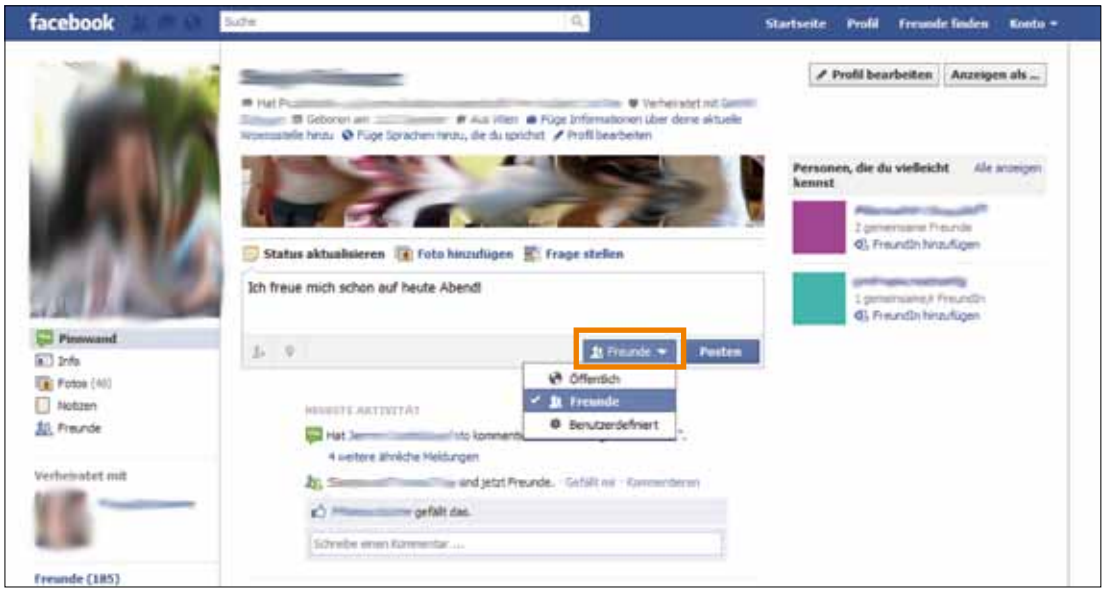


Abbildung 3: Sichtbarkeit für Statusmeldungen, Fotos und Profilinformationen auf *Facebook* einschränken (Quelle: www.facebook.com)

- **Nur bekannte Personen als „Freunde" akzeptieren:** Viele glauben, je mehr „Freunde" sie verlinkt hätten, desto beliebter wären sie. Aber in manchen Fällen ist der Schaden größer als der Nutzen – was spricht also dafür, nur bekannte Personen als „Freunde" zu akzeptieren?

  - Leute, die du tatsächlich kennst, wissen bereits etwas über dich. Sie sind nicht ausschließlich auf Angaben aus dem Netz angewiesen, um sich ein Bild über dich zu machen, und beurteilen dich nicht nur danach.
  - Bei bekannten Personen lässt sich besser einschätzen, welche Informationen du ihnen anvertrauen kannst und welche nicht.
  - Immer wieder werden in Communitys Schadprogramme (Viren, Trojaner etc.) verbreitet. Dies passiert häufig über Personen aus der „Freundesliste", die man nicht kennt.

Wenn Fremde dich einladen, dich als „Freund" zu verlinken, nimm diese Person genau unter die Lupe, bevor du die Einladung annimmst!

- **Keine peinlichen Fotos veröffentlichen**, auch nicht für „Freunde". Denn aus „Freunden" können später einmal „Feinde" werden. Nicht selten werden Fotos, die zu Zeiten enger Freundschaft ausgetauscht wurden, später für Cyber-Mobbing missbraucht. „Witzige" Bilder, intime Aufnahmen etc. können leicht auch gegen einen selbst verwendet werden. Ist ein Foto für den Abgebildeten/die Abgebildete „bloßstellend", gilt allerdings das „Recht am eigenen Bild" (siehe Seite 28).

TIPP: Belästigungen

Sollten dich andere Nutzer/innen in einer Community belästigen, so kannst du sie in der Regel über das eigene Profil oder deine Einstellungsseite **blockieren/ignorieren**. Blockierte/ignorierte Nutzer/innen können nicht mehr auf dein Profil zugreifen und dir auch keine Nachrichten mehr schicken. Falls die unerwünschte Kontaktaufnahme trotzdem nicht aufhört, kontaktiere den/die Website-Betreiber/in. In der Regel findest du dazu einen Link (z. B. „Person melden") direkt auf der Profilseite der entsprechenden Person.

- **Privates nicht über die „Pinnwand" austauschen:** Einen Geburtstagsgruß hinterlassen oder etwas Lustiges an die Pinnwand eines „Freundes" schreiben ist eine nette Sache, aber persönliche Dinge solltest du lieber über private Nachrichten austauschen (sonst geht es dir vielleicht einmal so wie Stefan in unserem Beispiel auf Seite 12). Ein Treffen über eine Pinnwand auszumachen, kann z. B. zu ungebetenen Überraschungsgästen führen.

- **Vorsicht bei externen Anwendungen:** Viele Plattformen bieten externe Programme von Drittanbietern an, mit denen du z. B. Geburtstagsgrußkarten versenden, Tests ausfüllen, an Gewinnspielen teilnehmen oder Spiele spielen kannst. Die Nutzung ist meist kostenlos, dafür erlauben die Website-Betreiber den Drittanbietern Zugriff auf die Daten deines Profils sowie auf die Daten aller „Freunde". Wenn einer deiner „Freunde" eine solche Anwendung ausführt, kann sie folglich auch auf deine Daten zugreifen. In den „Privatsphäre-Einstellungen" kannst du meist den Zugriff dieser Programme auf private Daten verbieten! Bedenke: Je mehr Anwendungen du verwendest, desto mehr Dritte können deine Daten für eigene Zwecke weiter verarbeiten, Überprüfe und lösche daher überflüssige Anwendungen regelmäßig aus deinem Profil!

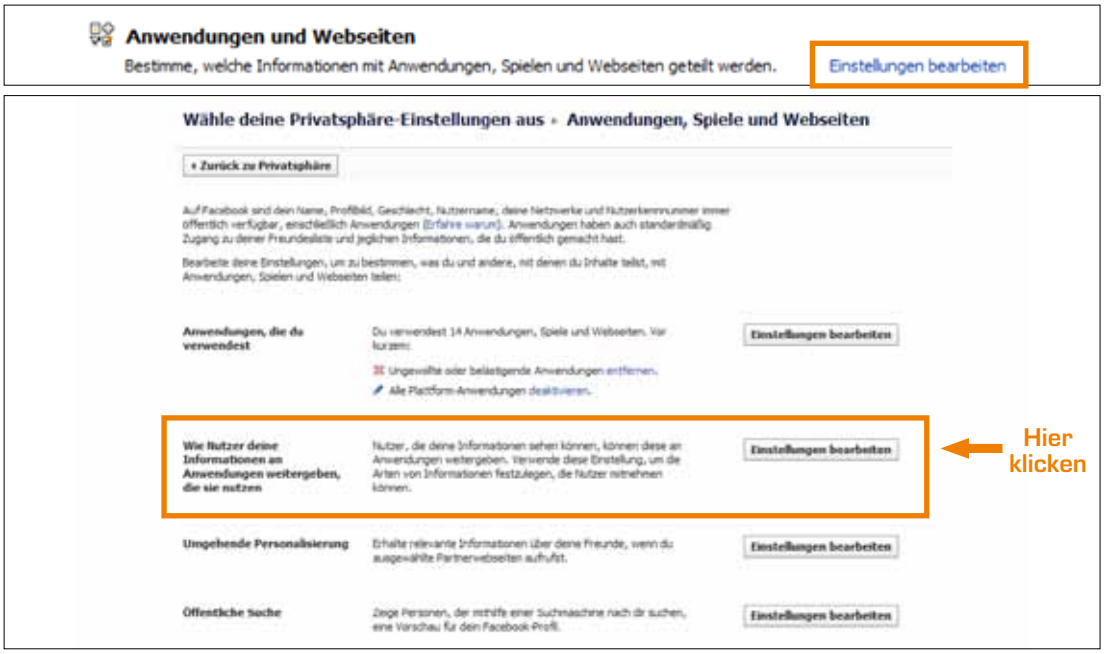


Abbildung 4: Datenschutz-Einstellungen für externe Anwendungen bei *Facebook* (Quelle: www.facebook.com)

- **„Gruppen"-Mitgliedschaften überdenken:** In Communitys gibt es viele unterhaltsame und interessante Gruppen, aber auch viele, bei denen man sich fragen sollte, was sie über einen aussagen, wenn man Mitglied ist. Das betrifft z. B. Gruppen, in denen ein hoher Alkoholkonsum oder Gewalt idealisiert wird. Gerade Menschen, die dich nicht persönlich kennen, können sich anhand deiner Gruppen-Mitgliedschaften ein ganz anderes Bild von dir machen, als du es vielleicht möchtest.

- **Sag nicht jedem, wo du bist:** In den meisten Sozialen Netzwerken ist es inzwischen möglich, geteilte Inhalte mit Ortsangaben zu verknüpfen. Wenn du z. B. ein aktuelles Foto via Handy hochlädst, wird den anderen Nutzer/innen angezeigt, an welchem Ort du das Foto aufgenommen hast. Damit weiß jeder, wo du gerade bist! In manchen Fällen mag das sinnvoll sein, aber Fremde müssen das wirklich nicht wissen. Schalte diese Funktion daher am besten nur für „Freunde" frei.

- **Markierungen im Griff behalten:** Bestimme, was passiert, wenn Freunde dich oder deine Inhalte markieren, d. h. wenn Kommentare, Fotos oder Orte direkt mit deinem Profil (und damit auch mit deinem Namen) verknüpft werden. Ohne entsprechende Privatsphäre-Einstellungen können dich fremde Nutzer/innen auf Fotos erkennen, Beiträge von dir lesen oder sehen, wo du dich gerade aufhältst. In vielen Communitys kannst du Markierungen, die Freunde von dir machen, auch bearbeiten und löschen. Deaktiviere auch Markierungsvorschläge für Fotos, die durch eine automatische Gesichtserkennung zustande kommen.

WENN DU NICHT MEHR AKTIV BIST auf einer Plattform, **lösche oder deaktiviere dein Profil**. Denn nicht mehr aktualisierte Angaben können leicht einen falschen Eindruck von deiner Person vermitteln. Dieser Löschvorgang wird einem von den Betreiber/innen nicht immer leicht gemacht – die Löschfunktion ist oft schwer auffindbar und der Weg bis zur erfolgreichen Abmeldung erfordert mehrere Schritte – aber es lohnt sich in jedem Fall!

Wenn du dein Profil unwiderruflich löscht, ist es theoretisch möglich, dass sich jemand anderer unter deinem Namen neu registriert und für schlechten Ruf sorgt. Um deinen Namen zu schützen, kannst du dein Profil nur mit den allernötigsten Informationen ausgestattet bestehen lassen.

Chats, Instant Messenger

Die wichtigsten Tipps, wie du Probleme in Chats oder über Instant Messenger vermeidest:

- **Such dir einen Chat, in dem du dich wohlfühlst:** Am besten chattet es sich mit Leuten, die in deinem Alter sind und dieselben Interessen haben. Oder du chattest dort, wo die meisten deiner Freunde sind. Frag deine Eltern oder Geschwister, ob sie dir bei der Wahl des richtigen Chats helfen. In seriösen Chats achten „Moderatoren" darauf, dass alle freundlich miteinander umgehen und helfen dir, wenn du dich nicht zurechtfindest oder andere Nutzer/innen gemein zu dir sind. Beziehungsweise gehen sie auch gegen dich vor, wenn du gemein zu anderen bist.

- **Verrate nie persönliche Daten,** über die du im „echten" Leben ganz einfach aufgespürt werden kannst, wie etwa deinen Nachnamen, deine Adresse oder deine Telefonnummer, und gestalte auch deine Nicknames so.

TIPP: Was ist ein guter „Nickname" (Spitzname)?

Gechattet wird in der Regel nicht unter richtigem Namen, sondern unter einem frei wählbaren Spitznamen („Nickname"). Der Nickname sollte reine Fantasie sein (z. B. Namen aus Lieblingsbüchern, Lieblingsfilmen oder ein lustiges Wort) und nichts Privates über dich verraten – also nicht deinen richtigen Namen, dein Alter, dein Geschlecht, und schon gar nicht deine Wohnadresse oder auf welche Schule du gehst.

- **Sei freundlich, aber wachsam:** Verhalte dich genauso freundlich wie im richtigen Leben, aber bleibe immer auch ein bisschen misstrauisch. Glaube nicht alles, was andere Menschen in Chats erzählen – etwas vorzuspielen ist dort besonders einfach. Am anderen Ende sitzt vielleicht jemand, der dich aushorchen und belästigen will. Gib daher nicht zu viel Persönliches preis und behalte Fotos lieber bei dir!

- **Triff dich nie alleine mit Leuten aus dem Chat:** Man kann nie wissen, wer tatsächlich auf dich wartet. Wenn du dich unbedingt treffen willst, nimm einen Erwachsenen mit, dem du vertraust!

- **Wird dir das Chatten unangenehm,** beende einfach die Unterhaltung und bitte eine/n Moderator/in um Hilfe. Nutze die „Ignorieren"-Einstellung, damit der/die Nutzer/in dich nicht weiter belästigen kann.

TIPP: Nützliche Sicherheitseinstellungen für Instant Messenger

- **Profilangaben möglichst anonym halten:** Gib im Profil keine persönlichen Daten wie Name, Adresse oder Telefonnummer preis und wähle einen Nickname, der keine Rückschlüsse auf dein „echtes" Leben zulässt. Nutze in deinem Profil am besten eine eigens dafür eingerichtete E-Mail-Adresse, die ebenfalls nichts Privates über dich verrät.

- **Automatisches Ablehnen von Nachrichten fremder Nutzer/innen:** Du erhältst dann nur mehr Nachrichten von Personen, die in deiner Kontaktliste stehen. Das ist die beste Möglichkeit, dich vor Belästigungen oder auch vor Viren oder Spam zu schützen. Leute, die du nicht kennst, solltest du grundsätzlich nicht in deine Kontaktliste aufnehmen – wozu auch?

- **Unerwünschte Personen auf die „Ignorier"-Liste setzen:** Wenn du dich von jemandem bedrängt fühlst, setze ihn/sie auf die „Ignorier"Liste – der/die Nutzer/in kann dich dann nicht mehr kontaktieren.

- **Öffentliche Statusanzeige ausschalten:** Oft wird nicht nur im Messenger selbst, sondern auch in öffentlichen Profilen im Internet dein Online-Status angezeigt. Somit können nicht nur Leute aus deiner Kontaktliste, sondern jede/r beliebige Internetnutzer/in sehen, ob du gerade online bist.

- **Anzeigebild überlegt aussuchen:** Dein Profilfoto wird allen Nutzer/innen im Nachrichtenfenster angezeigt. Überlege dir daher gut, welches Foto du einstellst – du solltest darauf zumindest nicht so gut erkennbar und auf jeden Fall nicht zu freizügig abgebildet sein.

- **Aufnahme in Kontaktlisten kontrollieren:** Du weißt, wen du in deiner Kontaktliste hast, aber weißt du auch, wer dich aller hinzugefügt („geadded") hat? Damit du darüber Kontrolle hast, aktiviere die Einstellung, dass du immer erst deine Erlaubnis erteilen musst, bevor dich andere Nutzer/innen in ihre Kontaktlisten aufnehmen.

- **Dateitransfer, Webcam und Telefonieren ausschalten:** Meistens lassen sich diese Zusatzfunktionen nicht komplett abstellen. Zumindest kannst du aber regulieren, dass z. B. nur deine Kontakte derartige Anfragen stellen dürfen und du vor Start der Anwendung zustimmen musst.

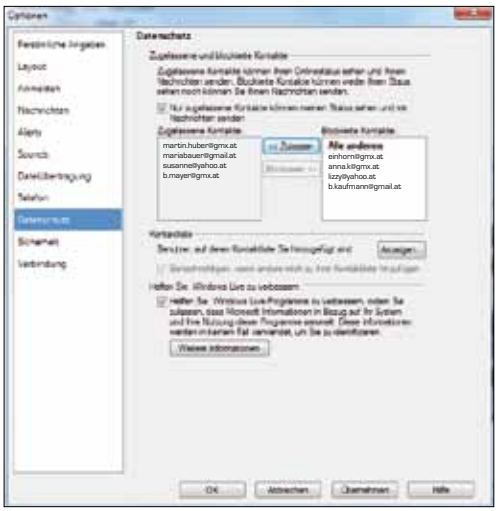


Abbildung 5: Privatsphäre-Einstellungen bei *Windows Live Messenger* (Quelle: http://messenger.live.de)

Websites, Blogs

Auch als Betreiber/in bzw. Autor/in einer Website/eines Blogs solltest du dich vor Veröffentlichung von Inhalten immer fragen:

- Was gebe ich mit dem gerade Geschriebenen/Veröffentlichten von mir preis?
- Wie einfach mache ich es anderen, auf meine „echte" Identität rückzuschließen?
- Könnten mir oder anderen die veröffentlichen Inhalte irgendwann einmal schaden?

4.2 Mein Ruf im Internet

Nun hast du schon ganz schön viel darüber erfahren, wie du deinem Image – sowohl in der „virtuellen" als auch in der „realen" Welt – mit nur ein paar unüberlegten Angaben im Internet schaden kannst. Aber was ist eigentlich, wenn andere Schlechtes oder Unerwünschtes über dich im Web verbreiten? Hier erfährst du, was du in diesem Fall tun kannst:

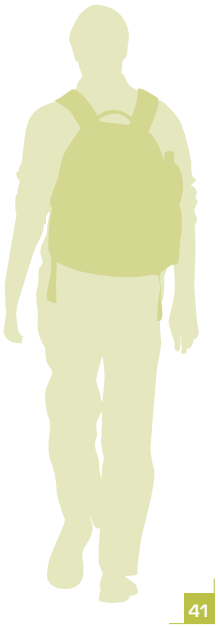
Wie finde ich heraus, was über mich im Internet steht?

Das geht eigentlich ganz einfach – du brauchst dafür nur einmal deinen eigenen Namen in eine Internet-Suchmaschine einzugeben. Um ein exakteres Suchergebnis zu bekommen, setze einfach deinen Vornamen und Nachnamen in Anführungszeichen („Maria Meier"). Die Anführungszeichen verbinden die beiden Wörter zu einer fixen Wortgruppe.

Mittlerweile gibt es auch zahlreiche **Personensuchmaschinen** (z. B. *123people.at, yasni.de*), die verschiedenste Spuren einer Person im Netz miteinander verknüpfen. Zu einem gesuchten Namen werden auf einer Seite alle verfügbaren Suchergebnisse – Websites, Community-Profile, Zeitungsartikel, Fotos, Videos, Forenbeiträge, Blogpostings, E-Mail-Adressen, Telefonnummern, Dokumente u.v.m. – aufgelistet.

Genau genommen sind diese Personensuchmaschinen eigentlich nur „Namenssuchmaschinen". Denn der Name ist das einzige Merkmal, wonach gesucht werden kann. Die meisten Menschen sind mit ihrem Namen online allerdings nicht alleine unterwegs. Die im Internet verfügbaren Daten zu einem Namen können daher nicht immer nur einer bestimmten Person zugeordnet werden. Das führt im Netz immer wieder zu Verwechslungen mit **„digitalen Doppelgängern"** (z. B. *der Vorsitzende eines Vegetarier-Vereins hat einen Namensvetter im Internet, der eine Fleischerei betreibt).*

Viele Personensuchmaschinen erlauben es, das eigene Profil anzupassen und unerwünschte Einträge zu entfernen (meist kostenlos). Dafür musst du dich allerdings bei der jeweiligen Personensuchmaschine registrieren und Daten über dich bekannt geben. Daneben gibt es professionelle Services, die dabei helfen, digitale Identitäten zu pflegen, indem sie störende oder veraltete Daten von einer Online-Quelle löschen (kostenpflichtig – je nach Aufwand von 20 bis zu mehreren hundert Euro).



Was kann ich machen, wenn ich Unerwünschtes von mir im Netz finde?

Gesetzlich hast du ein **Recht auf Wahrung der Privatsphäre**, d. h. jemand anderer darf ohne deine Zustimmung keine privaten oder vertraulichen Informationen von dir im Internet veröffentlichen oder verwerten. Entdeckst du z. B. ein für dich **nachteiliges Foto oder Video** im Netz, so hast du ein Recht auf Löschung dieses Fotos/Videos, da hier das **„Recht am eigenen Bild"** gilt (siehe Kapitel 3 *Gesetzliche Bestimmungen: Meine Rechte und Pflichten,* Seite 28).

Bei einer Rechtsverletzung gehst du am besten so vor:

1) Speichere dir zum Beweis der Rechtsverletzung einen Screenshot der Website, wo die betreffende Aufnahme hochgeladen wurde.

2) Kontaktiere schriftlich die Person oder das Unternehmen, das dein Foto/Video veröffentlicht hat, und/oder den Website-Betreiber und bitte um Entfernung. Dabei ist allerdings wichtig, dass du eine Frist setzt (z. B. drei Wochen), bis zu der das Foto/Video entfernt sein sollte. Nutze dazu z. B. das Muster einer Unterlassungsaufforderung auf Seite 43. In den meisten Sozialen Netzwerken findest du bei jedem Bild den Link „Foto melden".

3) Sollte das nichts nützen, kannst du in gravierenden Fällen mit einer Unterlassungsklage und Schadenersatzforderungen drohen und deine Rechte vor einem Gericht geltend machen. Lasse dich vorher beim Internet Ombudsmann dazu beraten (**www.ombudsmann.at**).

Interessant zu wissen

Suchmaschineneinträge

Viele Suchmaschinen erstellen automatisch eine Kopie jeder erfassten Internetseite in einem Zwischenspeicher („Cache"). Anhand dieser Kopie können Webinhalte auch abgerufen werden, wenn die Originalseite nicht mehr verfügbar ist oder die Inhalte längst von der Seite gelöscht wurden. Erst wenn die Suchmaschine die Seite das nächste Mal „besucht", werden die Änderungen in den Suchergebnissen übernommen. Das heißt, dass unerwünschte Inhalte wie Texte, Fotos, Videos, Dokumente, Postings etc. trotz Löschung noch einige Zeit im Internet aufgerufen werden können oder zumindest als „Vorschau" in den Trefferlisten der Suchmaschinen bestehen bleiben.

TIPP:

Bei großen Suchmaschinen wie *Google* oder *Bing* hat man die Möglichkeit, über ein spezielles Tool zum Entfernen von Websites die Löschung der Informationen aus der Web- bzw. Bildsuche zu beantragen. Bei *Google* muss man sich hierfür ein eigenes *Google*-Konto einrichten, bei *Bing* geht das auch ohne Anmeldung.

Aber Achtung: Eine Garantie, dass unerwünschte Inhalte nicht irgendwo im Netz wieder auftauchen, hast du nicht. Das Internet vergisst nicht so schnell: Trotz Löschung an der ursprünglichen Stelle bleiben Texte, Fotos, Videos etc. oft noch jahrelang anderswo gespeichert und können von anderen Nutzer/innen weiterverbreitet werden!

Muster einer Unterlassungsaufforderung

EINSCHREIBEN Datum

Name/Firma
Adresse

Eigener Name
Eigene Adresse

Unterlassungsaufforderung

Sehr geehrte/r Herr/Frau XY,
Sehr geehrte Damen und Herren,

auf Ihrer Website/Ihrem Blog haben Sie ein Foto/ein Video/eine vertrauliche Aufzeichnung von mir veröffentlicht. Dies erfolgte ohne meine Zustimmung. Ich fordere Sie daher auf, dieses Foto/dieses Video/diese vertrauliche Aufzeichnung und alle davon existierenden Kopien zu löschen und eine weitere Verwendung oder Veröffentlichung bei sonstiger gerichtlicher Einforderung meiner Ansprüche zu unterlassen. Dies geschieht gemäß § 78 UrhG, § 7 MedienG, § 1 und § 27 DSG sowie jedem anderen tauglichen Rechtsgrund.

Für die vollständige Entfernung des Fotos/des Videos/der vertraulichen Aufzeichnung haben Sie 21 Tage ab Datum dieser Erklärung Zeit. Verstreicht diese Frist ungenutzt, werden diese Aufforderung sowie alle Unterlagen und Screenshots an meinen Anwalt weitergeleitet.

Mit freundlichen Grüßen,

Unterschrift

Eigener Name

Trend: „Sexting“

Sich einmal wie Paris Hilton nackt vor der Kamera räkeln oder wie David Beckham in knappen Shorts posieren – immer mehr Jugendliche machen von sich selbst oder anderen erotische Fotos bzw. Nacktaufnahmen und versenden diese per Handy an Freund/innen und Bekannte. Oft landen die Bilder auch im Internet, z. B. in Sozialen Netzwerken und werden von dort an ein großes Publikum verbreitet. „Sexting“ – zusammengesetzt aus „Sex“ und „Texting“ – heißt dieser zweifelhafte Trend. Das Problem: Oft werden die anzüglichen Bilder vorerst „nur“ zwischen Pärchen oder besten Freund/innen verschickt, z. B. als eine Art Liebes- oder Freundschaftsbeweis oder zum Flirten. Wenn die Beziehungen oder Freundschaften aber in die Brüche gehen, landen einige der Fotos aus Rache öffentlich im Web oder werden zur Erpressung verwendet.

ACHTUNG: Wenn es sich bei den Fotos um pornografische Darstellungen von unter 14-Jährigen handelt, fällt das unter **„Kinderpornografie“**. Neben dem Herstellen, Verbreiten, Überlassen und Vorführen solcher Aufnahmen, reichen bereits auch das wissentliche Betrachten oder bloßer Besitz, um sich strafbar zu machen! Als Kinderpornografie gilt übrigens auch die Darstellung sexueller Handlungen an Personen unter 18 Jahren oder von Personen unter 18 Jahren an sich selbst, an anderen oder an Tieren. Es kann bereits eine Abbildung reichen, wo die Genitalien oder der Schambereich abgebildet sind, wenn diese der sexuellen Erregung des Betrachters dient.

Aber Halt! Natürlich ist es nicht strafbar, wenn du mit deinem Freund oder deiner Freundin Fotos zum eigenen Gebrauch anfertigst. Das Gesetz sieht die Straflosigkeit vor, wenn der/die Abgebildete über 14 Jahre alt ist und diese freiwillig an einen Freund/eine Freundin zu dessen/deren eigenen Gebrauch schickt. Der Gesetzgeber will sich nicht in euer privates Leben einmischen. Aber: Die Weitergabe der Bilder an Dritte ist nicht nur unfair, sondern auch strafbar! Das gilt übrigens auch, wenn du dich an deinem Ex-Freund/deiner Ex-Freundin rächen willst und dessen/deren Bilder ungefragt weiterschickst.

Deshalb: Verschicke am besten weder erotische Fotos von dir, noch von anderen! Von den möglichen rechtlichen Folgen ganz abgesehen, möchtest du wirklich, dass dich vielleicht mal deine Verwandten, dein zukünftiger Chef oder – noch schlimmer – deine eigenen Kinder in eindeutiger Pose im Internet finden?

4.3 Über andere im Netz berichten

Peinliche oder sonst irgendwie unerwünschte Inhalte über sich selbst im Internet zu finden, kann ganz schön unangenehm sein, oder? Vor allem, weil einmal ins Web gestellte Dinge von dort nicht mehr so leicht verschwinden. **Genau wie du selbst, hat aber auch jeder andere ein Recht auf Datenschutz und Privatsphäre!**

Bevor du private Informationen oder Fotos von Freund/innen oder anderen Personen veröffentlichst, überlege dir, ob sie etwas dagegen haben könnten. Frag sicherheitshalber vor dem Veröffentlichen nach!

DO's and DONT's

Würdest du deine/n Lehrer/in oder deine/n Chef/in von Angesicht zu Angesicht beschimpfen? Würdest du vor deiner besten Freundin/deinem besten Freund über deren/dessen neue Frisur lästern? Würdest du Fotos von der letzten Party in der Klasse aufhängen? NEIN? Siehst du, und dasselbe gilt für das Internet!

Über andere Menschen hinter deren Rücken im Netz herzuziehen, Lügen zu verbreiten oder sich lustig zu machen ist nicht nur ziemlich feig, sondern kann unter Umständen auch **strafbar** sein:

- Angelegenheiten, die offensichtlich **privater Natur** sind, etwa Familienleben, Intimleben oder auch vertraulich Mitgeteiltes darfst du im Internet nicht ausplaudern. Bringt eine Person jedoch selbst Privates an die Öffentlichkeit, darfst du dazu etwas sagen.

- Auch wenn Meinungen und Kommentare erlaubt sind, dürfen sie die betroffene Person **nicht beleidigen, beschimpfen, bloßstellen, verletzen, kränken oder kreditschädigend sein.** Auch nicht erlaubt sind Ver- und Beurteilungen, etwa im Sinne eines Vorwurfs einer strafrechtlich relevanten Handlung *(„der Maxi klaut im Supermarkt", „die Sabine schummelt sich durch jede Prüfung").*

- Verboten sind selbstverständlich die **Verbreitung von Lügen** oder eine **verzerrte Darstellung einer Sache**. Das würde auch zutreffen, wenn wichtige Teile eines Sachverhalts weggelassen werden oder wenn alte Tatsachen so dargestellt werden, als ob sie heute noch genauso gelten.

- Ein besonderer Schutz gilt für **Bilder**, auf denen der Betroffene erkannt werden kann (siehe Kasten auf Seite 46).

TIPP: Darf ich selbst gemachte Fotos/Videos von anderen Personen online stellen?

Du machst auf einer Party zu fortgeschrittener Stunde Fotos von verschiedenen betrunkenen Besucher/innen und stellst sie anschließend gleich ins Internet. Im nüchternen Zustand ist diesen Personen die Veröffentlichung der Bilder allerdings gar nicht recht. Sie drohen dir mit einer Klage – und das dürfen sie auch. Bei der Veröffentlichung von Bildern anderer Personen ist immer das **„Recht am eigenen Bild"** zu beachten: Fotos/Videos und/oder deren Begleittext, die die so genannten „berechtigten Interessen" der Personen auf dem Bild verletzen, dürfen nicht veröffentlicht werden (siehe Kapitel 3 *„Gesetzliche Bestimmungen: Meine Rechte und Pflichten"*, Seite 28). Als Entscheidungshilfe, ob die „berechtigten Interessen" der abgebildeten Person verletzt sind, kann dir die Frage helfen: Würde ich eine solche Aufnahme auch von mir selbst im Netz finden wollen? Bedenke das auch, wenn du andere Personen auf einem Foto markieren („taggen") möchtest – nicht jedem ist das immer recht. Frag daher zur Sicherheit vorher bei der/dem Betroffenen nach!

Spezialfall: Lehrer/innen im Internet schlechtmachen

Immer öfter tauchen im Internet **bloßstellende Fotos oder Videos aus dem Schulunterricht** auf, die Lehrer/innen in peinlichen Situationen zeigen. Als Filmemacher/innen entpuppen sich in den meisten Fällen die eigenen Schüler/innen. Vielerorts im Web sind auch derbe **Beschimpfungen, Beleidigungen und Lästereien** zu lesen, oder es werden **Fake-Profile** in Chats und Communitys angelegt, um Lehrer/innen mit anzüglichen Bemerkungen und rufschädigenden Äußerungen in ein schlechtes Licht zu rücken. Die betroffenen Personen erfahren oft erst viel später, dass sie von ihren Schüler/innen einem potenziell weltweiten Publikum zur Belustigung ausgesetzt wurden.

Lehrer/innen „anonym" im Internet zu mobben, hat mit Schülerscherzen oder Spaß nichts mehr zu tun. Denn die meisten Schüler/innen vergessen schlichtweg, dass Lehrer/innen durch solche Vorkommnisse **psychisch extrem belastet** werden können.

Was die **rechtliche Seite** betrifft, gelten für „nachteilige Darstellungen" von Lehrer/innen im Internet dieselben Regelungen wie zuvor auf Seite 45 beschrieben. Wenn z. B. Videos oder Fotos so aufgenommen oder zusammengeschnitten werden, dass eine Lehrkraft damit lächerlich gemacht wird, ist die Veröffentlichung gesetzlich verboten.

TIPP: Lehrer/innen-Benotung

Internet-Plattformen wie *spickmich.de*, wo Schüler/innen Lehrer/innen der eigenen Schule nach bestimmten Kategorien benoten können, werden immer wieder diskutiert. Viele Lehrer/innen und Schulen sehen sich an den Internet-Pranger gestellt. Natürlich ist es nicht verboten, deine Meinung zu sagen, achte aber darauf, dass du sachlich bleibst und niemanden beleidigst! Informationen aus dem z. B. Privat- oder Intimleben einer Lehrerin/eines Lehrers haben auf solchen Portalen nichts zu suchen. Man sollte nicht nur Kritik austeilen, sondern auch mal die positiven Eigenschaften von Lehrer/innen angeben.

4.4 Sicherer Umgang mit Passwörtern und Codes

Deine Passwörter und Codes sind besonders schützenswert. Wenn sie in falsche Hände geraten, besteht Missbrauchsgefahr – das kann vom Plündern des Bankkontos über das Einkaufen in fremdem Namen bis hin zu verfälschten Community-Profilen reichen. Wie unangenehm das sein kann, zeigt dir folgendes Beispiel:

Sabine und die verunstalteten Profile

Die 13-jährige Sabine teilt mit ihrer besten Freundin Karin einfach alles. Karin kennt Sabines peinlichste Fotos, ihr Tagebuch, ihre Liebesbriefe an Marc und sogar ihre Zugangsdaten für diverse Online-Communitys. „Meine beste Freundin kann ruhig alles von mir wissen, ist ja nichts Schlimmes dabei", denkt sich Sabine. Doch dann gibt es zwischen den beiden Mädchen einen großen Streit – es geht natürlich um einen Typen. Karin kündigt Sabine die Freundschaft auf und schmiedet Pläne, wie sie der „blöden Kuh" so richtig eines auswischen kann. Sie loggt sich mit Sabines Zugangsdaten in verschiedene Online-Communitys ein und füllt die Profile ihrer ehemals besten Freundin mit lauter Unwahrheiten – als „Draufgabe" zitiert sie auch noch peinliche Stellen aus Sabines Tagebuch und stellt ein total furchtbares Erstkommunionsfoto online, das ihr Sabine einmal geschickt hatte. Damit sich Sabine so richtig ärgert und die neuen Profilinhalte nicht gleich wieder löschen kann, ändert Karin auch noch Sabines Passwort. Als Sabine die verunstalteten Profile entdeckt, fällt sie aus allen Wolken – hätte sie doch bloß nicht ihre Geheimnisse weitergegeben!

Ein Passwort ist wie eine Zahnbürste – und die würdest du auch nicht weitergeben, oder? Halte deine Passwörter daher geheim (auch z. B. vor der besten Freundin/dem besten Freund) und wähle sie so, dass andere sie nicht knacken können.

Wie sieht ein sicheres Passwort aus?

- Verwende Passwörter, die aus einer Kombination aus mindestens acht Buchstaben (variiere mit Groß- und Kleinschreibung), Zahlen und Sonderzeichen (z. B. ! ? % ^ & * @ # $ [ ] [ ] \ ; : / < > ~) bestehen. Ob dein Passwort sicher genug ist, kannst du mit dem Microsoft-Kennwortprüfer testen: **www.microsoft.com/de-de/security/pc-security/password-checker.aspx**.
- Verzichte auf einfache Wörter oder Namen (wie z. B. den deines Haustieres), die einfach zu knacken sind. Auch einfache Zahlenkombinationen wie „123456" oder „123123" sind nicht sehr sicher.
- Wähle Zeichenfolgen, die du dir merkst, die andere aber nicht erraten können.
- Benutze verschiedene Passwörter für verschiedene Anwendungen.
- Und schließlich: Gib dein Passwort stets unbeobachtet von Dritten ein!

Gute Tipps für den Umgang mit Passwörtern geben auch Bit & Byte im Video „Passwortschutz": www.youtube.com/saferinternetat.

Ein TIPP zum Merken von Passwörtern:

Hilf dir mit Eselsbrücken, z. B. für das Passwort „IbegFvFM4!“:
„Ich bin ein großer Fan von FM4!“.

Oder: „JMgS&i2MiK“: „Jeden Monat gehen Sofie & ich 2 Mal ins Kino“.

Wenn du dir deine Passwörter nicht merken kannst, solltest du **beim Aufschreiben Folgendes beachten:**

- Passwort nicht als Passwort bezeichnen.
- Nicht zusammen mit ergänzenden Zugangsdaten hinterlegen.
- Keinesfalls direkt am Computer oder Handy aufbewahren.
- Verschlüssle dein Passwort zusätzlich, z. B. durch Buchstaben-, Silben- oder Zahlendreher (schreibe z. B. statt „13“ „31“).

Wenn du glaubst, dass jemand anderer dein Passwort herausgefunden hat, solltest du es sofort ändern! Ändere deine Passwörter am besten überhaupt regelmäßig.

Was ist „Phishing“ und was kann ich dagegen tun?

Unter „Phishing“ versteht man eine besondere Form des Online-Betrugs. Dabei versuchen Betrüger/innen **mittels gefälschter Websites und E-Mails an die Passwörter ahnungsloser Internetnutzer/innen** für Online-Bankkonten, Auktions-Plattformen, Online-Shops oder Ähnliches zu kommen. Die Benutzer/innen erhalten meist eine täuschend echte E-Mail, in der sie aufgefordert werden, auf einen Link zu klicken und sich unter irgendeinem Vorwand in den Account einzuloggen, z. B. um dort die Nutzerdaten zu aktualisieren. Die Website, auf die der Link verweist, ist aber ebenfalls gefälscht, auch wenn sie auf den ersten Blick wie das Original aussieht. Wenn du dich dort versuchst einzuloggen, teilst du den Betrügern deine Accountdaten mit. Innerhalb kürzester Zeit ist dann beispielsweise dein Bankkonto leergeräumt.

Nachdem die Fälschungen oft täuschend echt sind, solltest du besonders vorsichtig mit der Weitergabe deiner Accountdaten umgehen. Einige aktuelle Browser haben mittlerweile von Haus aus Phishing-Filter eingebaut, die dich vor unsicheren Websites warnen.

Die wichtigste Regel ist:
Banken, Online-Shops, Auktionshäuser etc. fragen sensible Daten ihrer Kund/innen NIEMALS via E-Mail ab – ignoriere solche Nachrichten daher! Wenn du dir nicht sicher bist, ob eine E-Mail echt ist oder nicht, frag am besten telefonisch bei der Hotline der jeweiligen Bank, des Online-Shops etc. nach.

4.5 Computer- und Internetzugang schützen

Auf deinem Computer hast du viele private Daten gespeichert. Hier findest du Schritt für Schritt erklärt, wie du deinen Computer- und Internetzugang schützen kannst.

Schritt eins: So sicherst du deinen Computer

Ohne ausreichenden Schutz nach außen ist dein Computer vergleichbar mit einem „offenen Buch". Technisch versierte Internetnutzer/innen können darin ungestört „lesen", deine Dokumente durchstöbern, beliebig Daten löschen, Viren einschleusen etc.

Wenn du folgende vier Punkte beachtest, ist dein Computer in jedem Fall gut geschützt:

1. Anwendungsprogramme und Betriebssysteme weisen immer wieder Sicherheitslücken auf, die erst mit der Zeit ausfindig gemacht werden. Deshalb ist es wichtig, dass du hier die automatischen **Software-Updates** aktivierst und regelmäßig durchführst.

2. Zusätzlichen Schutz bietet eine so genannte **Firewall**. Firewalls verhindern gefährliche Zugriffe aus dem Internet auf deinen Computer. Moderne Betriebssysteme haben von Haus aus eine Firewall eingebaut, die möglicherweise aber noch aktiviert werden muss.

3. Verwende ein **Anti-Viren-Programm**. Ein solches Programm schützt deinen Computer aber nur, wenn du es regelmäßig (mindestens einmal pro Tag) aktualisierst. Alle Virenschutzprogramme bieten eine automatische Aktualisierung an, die du unbedingt nutzen solltest. Dabei werden die neuesten Informationen über bekannte Schadprogramme vom Server des Anti-Viren-Programm-Herstellers heruntergeladen.

4. Eine besondere Art von Schadprogrammen, die zum Beispiel unbemerkt persönliche Daten auf dem eigenen Computer erfassen und über das Internet weiterleiten, wird als „Spyware" bezeichnet. Nicht jede Anti-Viren-Software bietet auch einen Schutz gegen Spyware. Deshalb empfiehlt es sich, ergänzend **Anti-Spyware-Programme** zu verwenden.

Es gibt auch kostenlose Versionen dieser Schutzprogramme. Infos dazu findest du auf der Saferinternet.at-Website: **www.saferinternet.at**.

Sichere deine USB-Sticks! Spezielle Software verschlüsselt den Inhalt von Datensticks, die danach nur noch per Passwort benutzbar sind. Einige USB-Sticks bringen diese Möglichkeit beim Kauf schon mit.

Ein gut geschützter Computer sieht zum Beispiel so aus:

Abbildung 6: Sicherheitscenter von *Windows Vista*

Schritt zwei: So verschlüsselst du deine WLAN-Verbindung

Drahtlose Funknetzwerke („Wireless Local Area Networks", kurz WLAN) werden auch für zuhause, in Schulen, in Cafés und auf Unis immer beliebter. Die Zahl der öffentlich eingerichteten WLAN-Zugänge, der so genannten „Hotspots", nimmt ebenfalls zu. Kein Wunder, kabellos im Internet surfen zu können ist ja auch sehr praktisch, aber trotzdem (oder gerade deswegen) muss man auf ein paar Dinge aufpassen: **Unverschlüsselt über ein WLAN-Netzwerk übertragene Daten sind nämlich grundsätzlich von jeder Person in der Reichweite deines Funknetzwerks lesbar** – fast so, als wenn du eine private E-Mail an eine Freundin ausgedruckt für alle, die vorbeikommen, an deine Wohnungstür hängen würdest. Außerdem können Dritte über ein ungeschütztes WLAN-Netz auf deine Kosten im Internet surfen und z. B. illegale Inhalte herunterladen – die rechtlichen Konsequenzen musst dann aber du tragen!

Um das alles zu verhindern, kannst du deine WLAN-Verbindung mit wenigen Handgriffen schützen. Dazu musst du den Datentransfer über eine „WPA- bzw. WPA2-Verschlüsselung" absichern. Außerdem solltest du für jeden Computer, den dein Funknetzwerk erkennen soll, die so genannte „MAC (Media Access Control) -Adresse" am WLAN-Router festlegen. Wie du das genau machst, steht im Handbuch deines Routers beschrieben, zu finden unter den Stichworten „MAC-Adresse" und „WPA-Verschlüsselung". Wenn du Hilfe brauchst, wende dich an jemanden mit Computererfahrung!

TIPP: Auf was muss ich aufpassen, wenn ich öffentliche Computer benutze?

Sind öffentliche Computer in der Schule, Internetcafés, Bibliotheken und Bahnhöfen sicher? Das hängt ganz davon ab, wie du sie verwendest! Beachte folgende Tipps, um deine persönlichen Daten zu schützen:

1. **Speichere nie deine Login-Daten:** Hast du dich auf einer bestimmten Website (z. B. zum Checken deiner E-Mails oder deines Community-Profils) eingeloggt, melde dich auch stets wieder mit Klick auf „Logout" o. ä. ab. Es reicht nicht, einfach das Browserfenster zu schließen oder eine andere Internetadresse einzugeben. Deaktiviere in jedem Fall auch automatische Anmeldefunktionen (z. B. bei Instant Messengern).

2. **Lasse den Computer während deiner Nutzung niemals unbeaufsichtigt:** Wenn du fertig bist, melde dich bei allen Websites und Programmen ab und schließe alle Fenster, die vertrauliche Daten enthalten könnten.

3. **Beseitige deine Spuren:** Die meisten Browser merken sich automatisch deine Passwörter und jede Website, die du besucht hast, selbst nachdem du sie geschlossen und dich abgemeldet hast. Klicke beispielsweise im *Internet Explorer* auf „Extras" und anschließend „Internetoptionen >> Allgemein" und lösche dort den gesamten Browserverlauf. Bei *Firefox* findest du diese Möglichkeit unter „Extras >> Einstellungen >> Datenschutz".

4. **Besser noch, erzeuge keine Spuren:** Moderne Browser, wie z. B. *Internet Explorer 8* oder *Firefox 8.0.1*, können in den so genannten „In Private Browsing"-Modus geschalten werden. So werden erst gar keine Informationen (z. B. Cookies, temporäre Internetdateien, Verlauf) auf dem Computer gesammelt. Um diese Funktion zu aktivieren, klicke bei *Internet Explorer* auf „Sicherheit >> InPrivate-Browsen", bei *Firefox* auf „Extras >> Privaten Modus starten".

5. **Lasse niemanden zuschauen:** Achte bei der Nutzung eines öffentlichen Computers immer darauf, dass dir niemand Fremdes über die Schulter schaut und dabei vertrauliche Daten ausspionieren könnte.

6. **Sei generell sparsam mit der Eingabe von persönlichen Daten**, denn so bist du in jedem Fall auf der sicheren Seite – auch vor Gelegenheitshackern, die eventuell nach dir denselben öffentlichen Computer benutzen könnten. Bank- oder Kreditkartendaten oder ähnlich vertrauliche Informationen solltest du am besten NIE auf einem öffentlichen Computer eingeben.

7. **Vorsicht bei drahtlosen Netzwerken:** Wenn du dich mit deinem Laptop in ein öffentliches WLAN-Netz einwählst, surfe am besten über ein Betriebssystem-Nutzerkonto mit eingeschränkten Zugriffsrechten, deaktiviere die Datei- und Verzeichnisfreigaben für Netzwerke und gib Daten ausschließlich über SSL-verschlüsselte Websites (erkennbar an „https://" und einem Schloss-Symbol entweder neben der Adressleiste oder am unteren Bildschirmrand) ein – denn viele öffentliche Verbindungen sind nicht geschützt! Sorge dafür, dass deine Anti-Viren-Software und Firewall auf dem neuesten Stand sind.

Schritt drei: Cookies, Cache & Co. – So beseitigst du deine Internetspuren am Computer

Auch dein eigener Computer protokolliert einiges mit, was du im Internet machst (z. B. besuchte Websites, eingegebene Zugangsdaten etc.), um dir bei einem erneuten Aufruf einer Website Zeit zu sparen. Was als eigentlich praktisches Hilfsmittel gedacht ist, erlaubt anderen Nutzer/innen deines Computers – etwa Familienmitgliedern oder Mitschüler/innen – deine Surfgewohnheiten nachzuvollziehen. Hier erfährst du, wie du deine Internet-Spuren ausradierst:

Cookies

Cookies (engl. „Kekse") sind kleine Dateien auf deinem Computer, die sich beim Besuch bestimmter Websites (z. B. Online-Shops, Communitys etc.) „merken" z. B. welche Registrierungsdaten eingegeben wurden, was du bestellt hast, wie lange du dort gesurft hast oder welche Unterseiten genau angeschaut wurden. Besuchst du später nochmal diese Website, „weiß" der Server dank der Cookies, dass du schon einmal dort warst und füllt alle deine persönlichen Daten automatisch ein. Das ist für dich natürlich praktisch, aber denk dran, dass dadurch auch andere Computer-Nutzer/innen ganz leicht an deine Passwörter, Codes etc. kommen können! Außerdem werden Cookies manchmal auch dazu missbraucht, dich mit nerviger Werbung zu belästigen.

Im Browser *(Internet Explorer:* „Extras >> Internetoptionen >> Datenschutz", *Firefox:* „Extras >> Einstellungen >> Datenschutz") lässt sich einstellen, dass Cookies entweder komplett verhindert, nur für die aktuelle Sitzung zugelassen oder auch generell zugelassen und nur Cookies von bestimmten Sites gesperrt werden. Solltest du auf eine Website angewiesen sein, die ohne Cookies nicht korrekt funktioniert, kannst du eine „Sondererlaubnis" erteilen. Ebenso kannst du dort alle bisher gespeicherten Cookies von deinem Computer löschen.

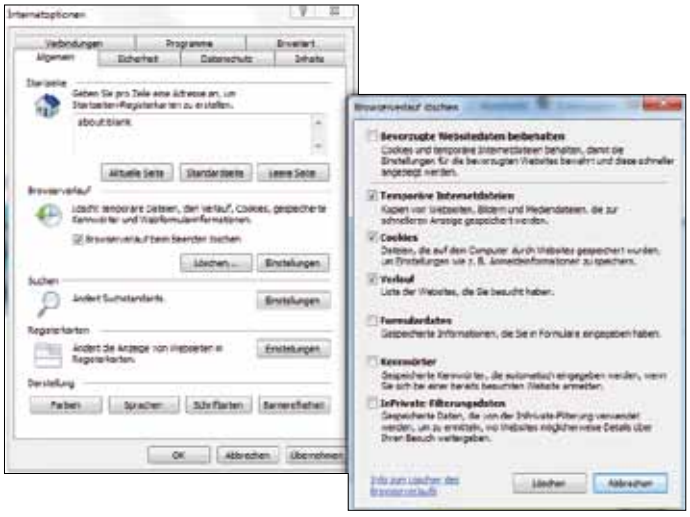


Abbildung 7: Cookies, Verlauf und temporäre Dateien im *Internet Explorer* löschen

TIPP: Internet-Surfen ohne Spuren

Moderne Webbrowser, wie z. B. *Internet Explorer 8* oder *Firefox 8.0.1*, können mit nur einem Klick in den so genannten „In Private Browsing"-Modus geschalten werden. So werden erst gar keine Informationen (z. B. Cookies, temporäre Internetdateien, Verlauf) auf dem Computer gesammelt. Um diese Funktion zu aktivieren, klicke bei *Internet Explorer* auf „Sicherheit >> InPrivate-Browsen", bei *Firefox* auf „Extras >> Privaten Modus starten".

Cache und Verlauf

Neben einer Liste der zuletzt besuchten Websites („Verlauf") werden auch Teile dieser besuchten Sites („temporäre Internetdateien") auf der Festplatte im so genannten „Cache" gespeichert, um sie bei einem neuerlichen Aufruf schneller anzeigen zu können. Im Browser *(Internet Explorer:* „Extras >> Internetoptionen >> Allgemein", *Firefox:* „Extras >> Einstellungen >> Datenschutz") lässt sich einstellen, dass abgerufene Sites gar nicht erst im Cache gespeichert werden, keine Verlaufsliste erstellt wird oder beides nach jeder abgeschlossenen Sitzung wieder verschwindet. In jedem Fall solltest du die automatisch gespeicherten Browserinformationen in regelmäßigen Abständen entfernen, damit keine anderen Computernutzer/innen nachverfolgen können, was du im Internet gemacht hast.

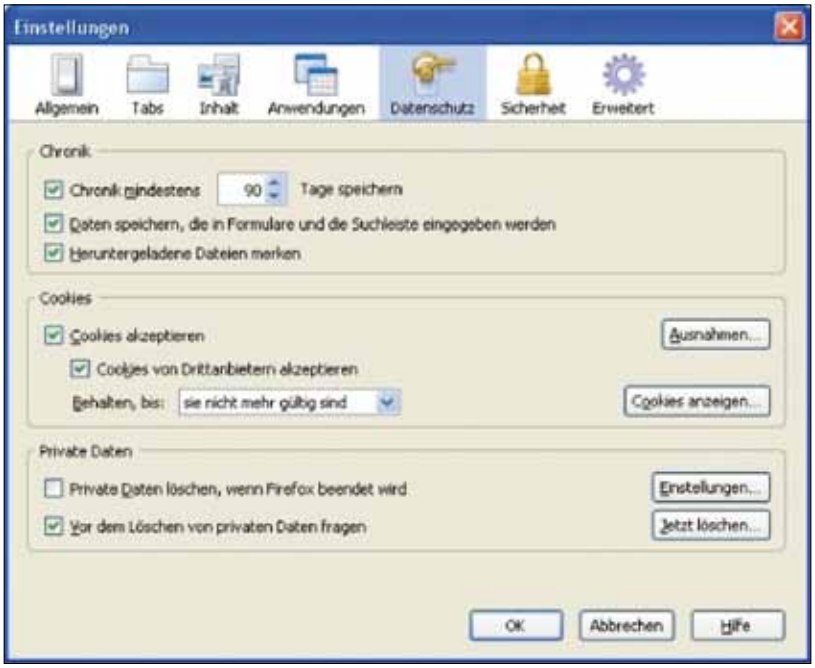


Abbildung 8: Cookies, Verlauf und temporäre Dateien bei *Firefox* löschen

Anonymisierungssoftware

Wer möchte, dass die eigene IP-Adresse und damit der Computerstandort verschleiert werden, kann auch anonym im Internet surfen. Dafür gibt es – kostenlose – Anonymisierungsprogramme (z. B. **www.torporject.org**), die die Internetverbindung deines Computers über einen Anonymisierungsserver lenken.

TIPP: Festplatte löschen

Beim Löschen von Dateien werden in der Regel nur die Einträge im Inhaltsverzeichnis der Festplatte gelöscht. Die Daten selbst bleiben so lange bestehen, bis sie überschrieben werden. Eine Wiederherstellung ist mit verschiedenen Tools ganz einfach möglich. Selbst das Formatieren der Festplatte löscht Dateien nicht endgültig. Bevor du deine Festplatte daher weitergibst oder entsorgst, solltest du einen so genannten „Datenshredder" verwenden (z. B. das Gratis-Programm „Eraser").

TIPP: Handy löschen

Willst du dein Handy verkaufen, verschenken oder entsorgen, solltest du daran denken, dass sich meist sensible und persönliche Daten darauf befinden. Ob gespeicherte SMS, E-Mails, Fotos, Kontakte oder Zugangsdaten zu Sozialen Netzwerken – all das soll natürlich keinem Dritten in die Hände fallen. Über die einfache Löschfunktion werden Daten nicht tatsächlich vom Handy entfernt, es wird lediglich der belegte Speicherplatz freigegeben. Solange keine neuen Daten darüber installiert werden, sind die alten Daten also noch vorhanden. Um auf Nummer sicher zu gehen, erkundige dich bei deinem Mobilfunkbetreiber über die Rücksetzfunktion deines Geräts. Generell sollten Daten immer auf Micro-SD-Karten gespeichert werden anstatt im internen Handyspeicher. Denn diese lassen sich mit Hilfe des Computers einfach und gründlich löschen (z. B. mit dem Gratis-Programm „Eraser").

5. Weiterführende Links

Allgemeine Informationen

Saferinternet.at – die österreichische Informations- und Koordinierungsstelle für die sichere Internetnutzung unterstützt mit praktischen Infos und konkreten Tipps, Broschüren- und Veranstaltungsservice sowie Beratung: **www.saferinternet.at**

Saferinternet.at-Leitfäden mit einfachen Schritt-für-Schritt-Anleitungen zu den Privatsphäre-Einstellungen in einzelnen Sozialen Netzwerken (z. B. *Facebook*, *Szene1.at*, *flickr* u. v. m.):
www.saferinternet.at/leitfaden

Handywissen.at – das Partnerprojekt von Saferinternet.at gibt auf der Website und in Broschüren Tipps und konkrete Hilfestellungen für die sichere und verantwortungsvolle Nutzung des Handys:
www.handywissen.at

Die **ARGE DATEN** – Österreichische Gesellschaft für Datenschutz setzt laufend Initiativen zum Schutz der Privatsphäre: **www.argedaten.at**

Watch Your Web – Online-Initiative der Fachstelle für internationale Jugendarbeit der Bundesrepublik Deutschland (IJAB) mit jugendgerecht aufbereiteten Infos, Tipps, Videoclips, Tutorials etc. zum Privatsphärenschutz im Netz: **www.watchyourweb.org**

filmABC – Institut für angewandte Medienbildung und Filmvermittlung. In der Rubrik „Unterrichtsmaterialien" finden sich Themenhefte wie z. B. Heft 32 „The Social Network"; als Ausgangspunkt für Diskussionen zu Sozialen Netzwerken, Datenschutz und Cyber-Mobbing wird der Film „The Social Network" (USA 2010) herangezogen: **www.filmabc.at**

Behörden

Österreichische Datenschutzkommission (DSK) – Informationen über die Arbeit der DSK, Rechtsquellen, Berichte und Materialien: **www.dsk.gv.at**

Technische Informationen

Das **„Safety & Security Center"** von Microsoft liefert Tipps, Tricks und Werkzeuge für optimale Sicherheitseinstellungen des Computers und zum Schutz persönlicher Daten:
www.microsoft.com/de-de/security/default.aspx

Rechtliche Grundlagen

Website von **Richter Dr. Franz Schmidbauer** mit Antworten auf viele rechtliche Fragen rund um Internet und Handy: **www.internet4jurists.at**

Rechtsinformation des Bundes mit Gesetzestexten und gerichtlicher Entscheidungssammlung:
www.ris.bka.gv.at

Notizen

6. Übungen

Die folgenden Übungen beinhalten **Anregungen, wie Lehrende ihren Unterricht zum Thema „Schutz der Privatsphäre im Internet" gestalten können**. Technische Hilfsmittel und Computerräume sind für die meisten Übungen nicht notwendig. Übungen, die einen Computer voraussetzen, sind mit einem Computer-Symbol am rechten oberen Seitenrand gekennzeichnet.

Unter **www.saferinternet.at/broschuerenservice** finden Sie diese Materialien kostenlos zum Downloaden bzw. Nachbestellen.

Übung 1: „Private Daten – Öffentliche Daten. Wo ist meine Grenze?"

Ziele

- Private Daten von öffentlichen Daten unterscheiden lernen
- Die Weitergabe von persönlichen Daten reflektieren

Ablauf

Phase 1

Die Schüler/innen erhalten eine kurze Einführung, was „personenbezogene Daten" sind (siehe Kapitel 3 ab Seite 23). Anschließend füllen die Schüler/innen in 2er- oder 3er-Gruppen das Arbeitsblatt auf Seite 58 aus. Gemeinsam sollen sie darüber nachdenken und diskutieren, welche der auf dem Arbeitsblatt angegebenen Daten ganz privat sein sollten und welche man vielleicht weitergeben darf.

Phase 2

Die Schüler/innen stellen ihre Ergebnisse in der Klasse vor und fertigen an der Tafel eine gemeinsame Liste an. Fälle, über die Uneinigkeit herrscht, sollen vor dem Aufschreiben diskutiert werden. Abschließend wird gemeinsam nochmals das Ergebnis reflektiert und auch die Frage besprochen, wo eigentlich die Grenze zwischen privaten und öffentlichen Daten sein sollte.

(Übung und Arbeitsblatt bereitgestellt von klicksafe.de)

Arbeitsblatt zu Übung 1: „Private Daten – Öffentliche Daten. Wo ist meine Grenze?“

Du hast gerade gelernt, was „personenbezogene Daten“ sind. Sicherlich hast du schon einmal deine persönlichen Daten angeben müssen, z. B. bei der Anmeldung in einer Online-Community. Überlege und diskutiere mit deinen Klassenkamerad/innen, welche davon ganz privat sein sollten und welche man vielleicht weitergeben darf. Wo also ist die Grenze deiner persönlichen Daten zwischen privat und öffentlich? Du wirst merken, dass das gar nicht so einfach zu beantworten ist und manchmal auch gar nicht eindeutig zu sagen ist.

Arbeitsauftrag:

1. **Bitte lies dir diese Liste personenbezogener Daten genau durch:**

   Mein Alter / Meine Adresse / Die Uhrzeit, wann meine Eltern aus dem Haus sind / Meine Schuhgröße / Meine Schule, Ausbildungsplatz etc. / Krankheiten, unter denen ich leide / Meine Telefonnummer / Meine Hobbys / Mein Gewicht / Welche Pickelcreme ich benutze / Die Anzahl meiner Pickel im Gesicht / Mein Lieblingsessen / Meine Mathematik-Note vom letzten Zeugnis / Meine Lieblings-Fernsehserie / Der Vorname meines besten Freundes / Die Farbe meiner Unterwäsche / Meine Lieblingsband / Mein heimlicher Schwarm, in den ich verliebt bin / Meine Religionszugehörigkeit / Ein Foto von mir in der Badewanne / Meine E-Mail-Adresse / Ein Foto, auf dem nur mein Gesicht zu sehen ist (Porträtfoto) / Die Höhe meines Taschengeldes / Der Name meines Haustiers / Mein Spitzname in der Klasse / Mein Geburtstag

2. **Trage nun in dieser Tabelle die Daten mit einem Stichwort ein:**

Auf jeden Fall privat	Nur für Freunde	Nicht eindeutig	Kann immer öffentlich sein

3. **Stellt eure Ergebnisse in der Klasse vor und fertigt eine gemeinsame Liste an der Tafel an.** Besprecht die unterschiedlichen Meinungen bei Fällen, wo ihr euch uneinig seid.

4. **Diskutiert danach das Ergebnis und auch die Frage, wo eigentlich die Grenze zwischen privaten und öffentlichen Daten sein sollte.**

(Übung und Arbeitsblatt bereitgestellt von klicksafe.de)

Übung 2: „Ich im Netz“

Ziele

- Die Bedeutung des Schutzes der Privatsphäre im Internet erkennen
- Unerwünschte Online-Inhalte über sich selbst vermeiden lernen
- Ein Gespür dafür bekommen, wie schnell und einfach personenbezogene Informationen im Internet beschaffbar sind

Ablauf

Phase 1

Die Schüler/innen sitzen einzeln oder zu zweit an einem Computer mit Internetzugang und erhalten folgenden Arbeitsauftrag:

- Du hast dich bei einer Firma um einen ausgeschriebenen Praktikumsplatz beworben und schlüpfst nun in die Rolle des verantwortlichen Personalchefs. Um die Angaben in der Bewerbung zu überprüfen bzw. um mehr über die Kandidatin/den Kandidaten zu erfahren, suchst du im Internet nach entsprechenden Informationen.
- Dazu gibst du deinen Vor- und Zunamen (1) bei einer Suchmaschine, (2) bei einer Personensuchmaschine (z. B. **123people.at, yasni.de**) und (3) bei den von dir am häufigsten genutzten Online-Communitys ein.
- Die Ergebnisse deiner Suche notierst du stichwortartig mit. Berücksichtige dabei auch Einträge von Personen, die zwar nichts mit dir zu tun haben, aber genauso wie du heißen.

Phase 2

Die Schüler/innen reflektieren miteinander, ob und wie einfach es war, bestimmte Informationen herauszubekommen, und welche Folgen die gefundenen Inhalte auf die Bewerbung haben könnten. Dabei können sich die Schüler/innen in z. B. 3er- oder 4er-Gruppen aufteilen:

- Welcher Eindruck wird dem Personalchef von mir vermittelt, welches Bild entsteht von mir?
- Was könnten Gründe dafür sein, das Praktikum nicht zu bekommen bzw. nicht zu einem Vorstellungsgespräch eingeladen zu werden?
- Habe ich etwas erfahren/entdeckt, wo mir vorher gar nicht bewusst war, dass es online ist?
- Wie kann ich vermeiden, dass unerwünschte Inhalte von mir im Netz landen?
- Was kann ich zur möglichen Schadensbegrenzung tun?

Variante

Wenn ein gutes Vertrauensverhältnis zwischen Schüler/innen und Lehrer/in besteht, können die Schüler/innen auf dieselbe Art und Weise auch nach ihrem/ihrer Lehrer/in im Internet suchen.

Anmerkung: In der Regel lässt sich ohnehin nicht verhindern, dass die Schüler/innen im Internet nach ihren Lehrer/innen suchen. Im Zuge dieser Übung tun sie es zumindest mit der Lehrkraft gemeinsam. Um unangenehme Situationen zu vermeiden, sollten Lehrer/innen vorab selbst im Web nach sich suchen.

Idee für Hausaufgaben

z. B. für den Deutsch- oder Englisch-Unterricht, ab der 8. Schulstufe

„Mein digitaler Fußabdruck im Internet – Welchen Einfluss könnten persönliche Inhalte im Web auf (m)eine Stellenbewerbung haben?“ Schreibe einen Aufsatz zum Thema!

Arbeitsblatt zu Übung 2: „Ich im Netz“

Arbeitsauftrag

- Du hast dich bei einer Firma um einen ausgeschriebenen Praktikumsplatz beworben und schlüpfst nun in die Rolle des verantwortlichen Personalchefs. Um die Angaben in der Bewerbung zu überprüfen bzw. um mehr über die Kandidatin/den Kandidaten zu erfahren, suchst du im Internet nach entsprechenden Informationen.
- Dazu gibst du deinen Vor- und Zunamen (1) bei einer Suchmaschine, (2) bei einer Personensuchmaschine (z. B. **123people.at, yasni.de**) und (3) bei den von dir am häufigsten genutzten Online-Communitys ein.
- Die Ergebnisse deiner Suche notierst du stichwortartig mit. Berücksichtige dabei auch Einträge von Personen, die zwar nichts mit dir zu tun haben, aber genauso wie du heißen.

Notiere hier deine Ergebnisse (Stichworte):

Diskutiere anschließend folgende Fragen mit deinen Mitschüler/innen:

- Welcher Eindruck wird dem Personalchef von mir vermittelt, welches Bild entsteht von mir?
- Was könnten Gründe dafür sein, das Praktikum nicht zu bekommen bzw. nicht zu einem Vorstellungsgespräch eingeladen zu werden?
- Habe ich etwas erfahren/entdeckt, wo mir vorher gar nicht bewusst war, dass es online ist?
- Wie kann ich vermeiden, dass unerwünschte Inhalte von mir im Netz landen?
- Was kann ich zur möglichen Schadensbegrenzung tun?

Übung 3: „Mein Profil in meiner Online-Community“

Ziele

→ Den sicheren Umgang mit persönlichen Daten erlernen
→ Die eigene Profilgestaltung in einer Online-Community reflektieren
→ Sich selbst im Internet schützen lernen

Ablauf

Phase 1

Die Schüler/innen arbeiten einzeln oder in Gruppen. Ausgehend von folgenden Leitfragen analysieren sie das Arbeitsblatt auf Seite 63/64.

Frage 1
„Nadine Brüller“ und „Markus Metal“ haben ihr Community-Profil gestaltet. Sie möchten viele neue Freund/innen kennenlernen, mit denen sie auf Partys bzw. Konzerten Spaß haben können. Wird ihnen dieses Ziel gelingen? Welchen Eindruck vermitteln die Profile, was für Menschen könnten deiner Meinung nach hinter „Nadine Brüller“ und „Markus Metal“ stecken? Welche Personen vermutest du, werden auf das jeweilige Profil ansprechen und „Nadine Brüller“ bzw. „Markus Metal“ kontaktieren?

Frage 2
Welche Daten/Aussagen im Profil von „Nadine Brüller“ bzw. „Markus Metal“ hätte sie/er besser nicht bekannt gegeben und warum?

Phase 2

Die Schüler/innen bringen nun ihre Überlegungen in die ganze Klasse ein. Dabei können folgende Fragen besprochen werden:

- Welche (ungewollten) Images können durch einzelne Online-Angaben entstehen?
- Welche Folgen könnten sich daraus für das „virtuelle“ und das „reale“ Leben ergeben?
- Wie könnten diese Überlegungen die Gestaltung des eigenen Community-Profils beeinflussen?

Ergänzend kann mit der Klasse der Videofilm „Date“ der Initiative www.watchyourweb.de angesehen werden, der die Risiken des Veröffentlichens von persönlichen Informationen und Bildern im Internet behandelt.

Lösungsinformation zu Übung 3

Persönliche Daten geheim halten: Gib keine persönlichen Daten bekannt, die es Fremden ermöglichen, dich auch im „echten" Leben aufzuspüren oder dich zu belästigen. Im Arbeitsblatt sind das v. a. die Telefonnummer, die Wohnadresse und die Angaben zu Schule und Klasse.

Veröffentliche keine Bilder oder Texte, die dir oder anderen später einmal peinlich sein oder zu deinem Nachteil verwendet werden könnten. Im Arbeitsblatt sind die Profilfotos und verschiedene Aussagen in den weiteren Profilangaben problematisch.

Zusätzlich ist zu beachten:

Zugriff auf das eigene Profil begrenzen: Nutze die Einstellungsoptionen deiner Community für mehr „Privatsphäre", indem du z. B. den Zugriff auf deine Freunde beschränkst.

Achte auf deine „Freunde": Wenn Fremde dich einladen, dich als „Freund" zu verlinken, nimm diese Person genau unter die Lupe, bevor du die Einladung annimmst.

Idee für Hausaufgaben

z. B. für den Deutsch- oder Englisch-Unterricht, ab der 7./8. Schulstufe

Oft heißt es: „Wer nichts angestellt hat, hat auch nichts zu verbergen". Diese Aussage veranlasst viele Menschen dazu, sehr freizügig mit ihren persönlichen Daten umzugehen, unter anderem auch im Internet. Haben sie damit recht? Schreibe einen Aufsatz!

Arbeitsblatt zu Übung 3:
„Mein Profil in meiner Online-Community“

Arbeitsauftrag

Analysiere ausgehend von folgenden Fragen die dargestellten Profile von „Nadine Brüller“ und „Markus Metal“ in einer Online-Community:

Frage 1
„Nadine Brüller“ und „Markus Metal“ haben ihr Community-Profil gestaltet. Sie möchten viele neue Freund/innen kennenlernen, mit denen sie auf Partys bzw. Konzerten Spaß haben können. Wird ihnen dieses Ziel gelingen? Welchen Eindruck vermitteln die Profile, was für Menschen könnten deiner Meinung nach hinter „Nadine Brüller“ und „Markus Metal“ stecken? Welche Personen vermutest du, werden auf das jeweilige Profil ansprechen und „Nadine Brüller“ bzw. „Markus Metal“ kontaktieren?

Frage 2
Welche Daten/Aussagen im Profil von „Nadine Brüller“ bzw. „Markus Metal“ hätte sie/er besser nicht bekannt gegeben und warum?

Hallo bei MyFace.at Suche

Pinnwand

Freunde (702)

 Chantal

 Sabrina

 Dune

 Ice

 Sven

 Kopfweh3.0

 Grinseboy

 King Kong

Nadine Brüller

Als FreundIn hinzufügen

Aus Saabstein Geboren am 13. April

Allgemeines

Über Nadine	Craaaaaaaaazy girl, partysüchtig, meistens zu laut, grad mal Single, gehe in die 4. Klasse der Rentreichschule, also die 1er HAK in Saabstein – wir sind die Bestn! Wenn wem mal faad ist: 0600-29397 – das wär ure supsi! Mein Motto: Ich hasse schlechte Laune, also, keep smiling und keep drinking :-)
Beziehungsstatus	Single
Geschlechtt	Weiblich
Telefon	0600-29397

Kunst und Unterhaltung

Musik	Lady Gaga, Katy Perry, Rihanna
Bücher	Ich les nix!
Filme	Twilight, Rocky, Kung Fu Panda
Fernsehen	Rosamunde Pilcher, Barbara Karlich, iCarly

Aktivitäten und Interessen

Aktivitäten	Party ohne Ende
Interessen	Romantik, Sommer, Sonne, Vodka Feige, Bacardi

Hallo bei MyFace.at

Suche

Markus Metal

+ Als FreundIn hinzufügen

Aus Graz Geboren am 6. Juni

Pinnwand

Freunde (666)


Nadine


Headache


Dune


Ice


Sven


LisaXXX


Martin


King Kong

Allgemeines

Über Markus	ohne Metal geht original goar nix, und ohne saufen auch nix *fg*, ich find Gewalt voi geil und hasse Krocha, black is best, bin immer auf den Metal Konzerten im Raabenhof – ihr erkennt mich am schwarzen Ledermantel mit Totenkopf :-]]] Komm vorbei wenn du mal endharten Metal hören willst, ich hab auch Zeug aus Amerika und so: Sebastianstraße 12/5 in Graz
Beziehungsstatus	Es ist kompliziert
Geschlecht	Männlich
E-Mail	boese@hotmail.com

Kunst und Unterhaltung

Musik	Slipknot, Machine Head, Marylin Manson
Filme	Triple xXx, Scream
Fernsehen	Alarm für Cobra 11, 24
Spiele	WoW

Sport

Lieblingssportarten	American Football
Lieblingssportler	Tom Brady, Chris Johnson

Aktivitäten und Interessen

Interessen	Metal, Ego Shooter, Guitar Hero, Lack & Leder, Winter, Schmerzen

Übung 4: „Was sage oder zeige ich im Web?“

Ziele

- Verständnis für die Bedeutung des Schutzes der Privatsphäre bekommen
- Die eigene Preisgabe von persönlichen Daten reflektieren
- Sensibel werden für mögliche Auswirkungen des eigenen Handelns auf andere

Ablauf

Diese Übung ist für eine kleinere Klasse oder Teilgruppe gedacht, um einen möglichst intensiven Austausch zu ermöglichen.

Phase 1

Ein langes, breites Kreppband, über dessen gesamte Länge ein Zahlenstrahl von 1-10 reicht, wird am Boden aufgeklebt.

Nun werden den Schüler/innen Aussagen (siehe Arbeitsblatt auf Seite 67-69) vorgelesen, zu denen Stellung genommen werden soll. Je nachdem wie die Schüler/innen die jeweils genannte Handlung bewerten, sollen sie sich entlang des Zahlenstrahls positionieren. Die Zahl 1 bedeutet „Ich stimme zu“ bzw. „Das ist richtig“, die Zahl 10 „Ich stimme nicht zu“ bzw. „Das ist falsch“.

Die Schüler/innen werden aufgefordert, sich in die jeweilige Situation hineinzuversetzen, auch wenn sie diese noch nicht selbst erlebt haben.

Nach dem Erklingen eines vorher vereinbarten Signals ist kein Wechseln mehr möglich. Nun geht es darum, die gewählten Positionen zu begründen und mit den Klassenkolleg/innen zu diskutieren. Die häufigsten Pro- und Kontra-Argumente schreibt der/die Lehrer/in zur Visualisierung an die Tafel. Im Zuge der Diskussion kann auch auf mögliche rechtliche Konsequenzen für bestimmte Handlungen hingewiesen werden (siehe dazu Kapitel 3 ab Seite 23).

Phase 2

Zur Vertiefung tragen die Schüler/innen die besprochenen Inhalte auf dem Arbeitsblatt in der Zeile „Meine Meinung dazu“ ein. Damit soll der eigene Umgang mit persönlichen Daten im Internet sowie mit persönlichen Daten anderer Personen reflektiert werden.

Idee für Hausaufgaben

z. B. für den Deutsch- oder Ethik-Unterricht, ab der 11. Schulstufe

„Warum und in welchen Situationen ist es mitunter besser, persönliche Informationen wie meine politische oder religiöse Einstellung, meine sexuellen Vorlieben, Daten meine Gesundheit betreffend etc. für mich zu behalten?“ Schreibe einen Aufsatz zum Thema!

Befrage dazu auch weitere Personen (z. B. Eltern, Geschwister, Großeltern, Nachbarn) und baue die Antworten in deinen Text ein.

Variante für Volksschulklassen

Anstatt des Kreppbands werden am Boden drei große Papierkreise in den Farben rot – orange – grün (Ampelfarben) aufgeklebt.

Nun werden den Schüler/innen Aussagen (siehe Arbeitsblatt auf Seite 70/71) vorgelesen, zu denen Stellung genommen werden soll. Je nachdem wie die Schüler/innen die jeweils genannte Handlung bewerten, sollen sie sich bei den Ampelfarben positionieren. Rot bedeutet „Ich stimme nicht zu" bzw. „Das ist falsch", Orange „Ich bin mir nicht sicher", Grün „Ich stimme zu" bzw. „Das ist richtig".

Nach dem Erklingen eines vorher vereinbarten Signals ist kein Wechseln mehr möglich. Nun geht es darum, die gewählten Positionen zu begründen und mit den Klassenkolleg/innen zu diskutieren. Die Kernaussagen schreibt die Lehrerin/der Lehrer zur Visualisierung an die Tafel.

Zur Vertiefung tragen die Schüler/innen die Diskussionsergebnisse auf dem Arbeitsblatt in der Zeile „Das haben wir dazu besprochen" ein. Kreuzen Sie mit Ihren Schüler/innen gemeinsam unbedingt auch die Felder „darf ich machen" bzw. „darf ich nicht machen" an!

Arbeitsblatt zu Übung 4:
„Was sage oder zeige ich im Web?“

Aussagen zur Weitergabe von persönlichen Daten im Internet

1. Ich bin oft in Online-Communitys, -Foren und -Chats unterwegs, um neue Leute kennenzulernen. Da gebe ich auch schon mal meine Telefonnummer weiter oder erzähle, in welche Schule ich gehe.

   Meine Meinung dazu:

   _____

   _____

   _____

2. Ich gehe mit Freunden zum Schwimmen. Es gelingen mir ein paar echt witzige Schnappschüsse. Damit alle etwas davon haben, stelle ich die Fotos gleich ins Internet und schicke den Link weiter.

   Meine Meinung dazu:

   _____

   _____

   _____

3. Ich habe schon öfter Nacktbilder bzw. erotische Aufnahmen von Gleichaltrigen per Handy oder E-Mail geschickt bekommen. Ich verstehe nicht, wie man sowas machen kann.

   Meine Meinung dazu:

   _____

   _____

   _____

4. Ab und zu poste ich etwas über meine Lehrer/innen in einer Online-Community oder einem Lehrer/innen-Benotungsportal. Ich finde, da ist nichts dabei.

   Meine Meinung dazu:

   _____

   _____

   _____

5. Wenn ich schlecht gelaunt bin, kann es schon einmal vorkommen, dass ich meinem Frust bei einem Internet-Chat durch unfreundliche oder beleidigende Bemerkungen freien Lauf lasse.

   Meine Meinung dazu:

   _____

   _____

   _____

6. Ich messenge oft mit jemandem, den ich noch nie im „echten" Leben getroffen habe. Wir haben uns immer sehr gut unterhalten und jetzt will er, dass ich ihm Fotos von mir schicke. Ich denke, es ist normal, dass er mich näher kennenlernen will.

   Meine Meinung dazu:

   _____

   _____

   _____

7. Ein Freund hat mir von einem neuen, lässigen Chat erzählt. Damit ich mitmachen kann, muss ich meinen Vor- und Nachnamen als Nickname angeben. Aber ich möchte eigentlich nicht, dass alle wissen, wer ich bin.

   Meine Meinung dazu:

   _____

   _____

   _____

8. Ich habe eine E-Mail von einem Online-Auktionshaus erhalten. Darin steht, dass mein persönliches Konto von Hackern angegriffen wurde. Ich klicke den angegebenen Link in der E-Mail an und gebe auf der Seite wie gewünscht meine Zugangsdaten ein, da ansonsten mein Konto aus Sicherheitsgründen gesperrt werden würde.

   Meine Meinung dazu:

   _____

   _____

   _____

9. Ich bin auf vielen Internet-Plattformen wie Chats, Online-Shops, Online-Communitys, Foren, Tauschbörsen etc. registriert. Um mir die Sache zu vereinfachen, benutze ich immer den gleichen Nutzernamen und das gleiche Passwort.

   Meine Meinung dazu:

   _____

   _____

   _____

10. Ich kenne jemanden, der in seinem Community-Profil ein Foto eines Klassenkollegen anstatt seines eigenen verwendet. In dem Profil steht ziemlich viel unsinniges Zeug. Ich finde das eigentlich sehr witzig.

    Meine Meinung dazu:

    _____

    _____

    _____

11. In meiner Online-Community schaue ich ganz genau darauf, wen ich in meine „Freundesliste“ aufnehme – ich muss die Leute zumindest persönlich kennen.

    Meine Meinung dazu:

12. Ich habe eine Website gefunden, wo man ein supertolles neues Handy gewinnen kann, wenn man sexy Strandfotos von sich selbst einschickt. Da mache ich natürlich mit!

    Meine Meinung dazu:

13. Ein Freund hat ein ziemlich peinliches Video von mir von der letzten Party ins Netz gestellt. Mir passt gar nicht, dass das online ist. Aber da kann ich eh nichts machen.

    Meine Meinung dazu:

Arbeitsblatt zu Übung 4: „Was sage oder zeige ich im Web?“, für Volksschulklassen

Aussagen zur Weitergabe von persönlichen Daten im Internet

1. Meinen Chat-Freunden verrate ich meinen richtigen Namen.
   ☐ darf ich machen ☐ darf ich nicht machen

   Das haben wir dazu besprochen:

   _____
   _____
   _____

2. Im Internet verrate ich meine Adresse und meine Telefonnummer.
   ☐ darf ich machen ☐ darf ich nicht machen

   Das haben wir dazu besprochen:

   _____
   _____
   _____

3. Meinen Chat-Freunden erzähle ich, wie meine Lieblingsband heißt.
   ☐ darf ich machen ☐ darf ich nicht machen

   Das haben wir dazu besprochen:

   _____
   _____
   _____

4. Ich schicke meinen Internet-Freunden Fotos von mir.
   ☐ darf ich machen ☐ darf ich nicht machen

   Das haben wir dazu besprochen:

   _____
   _____
   _____

5. Mit meinen Chat-Freunden würde ich mich nur in Begleitung meiner Eltern treffen.
   ☐ darf ich machen ☐ darf ich nicht machen

   Das haben wir dazu besprochen:

   _____
   _____
   _____

6. Im Internet erzähle ich, in welche Schule ich gehe.
   ☐ darf ich machen ☐ darf ich nicht machen

   Das haben wir dazu besprochen:

   _____

   _____

   _____

7. Wenn mein Freund/meine Freundin eine Chat-Bekanntschaft treffen möchte, begleite ich sie.
   ☐ darf ich machen ☐ darf ich nicht machen

   Das haben wir dazu besprochen:

   _____

   _____

   _____

8. Wenn mich im Internet jemand belästigt, erzähle ich das meinen Eltern.
   ☐ darf ich machen ☐ darf ich nicht machen

   Das haben wir dazu besprochen:

   _____

   _____

   _____

9. Ich finde, es ist nichts dabei, selbst gemachte Fotos von Freund/innen oder Mitschüler/innen ins Internet zu stellen.
   ☐ darf ich machen ☐ darf ich nicht machen

   Das haben wir dazu besprochen:

   _____

   _____

   _____

10. Wenn ich mich in der Schule geärgert habe, kommt es schon einmal vor, dass ich im Chat über meine Lehrer/innen schimpfe.
    ☐ darf ich machen ☐ darf ich nicht machen

    Das haben wir dazu besprochen:

    _____

    _____

    _____

Übung 5: „Meine Eltern und das Internet“

Ziele

→ Eigenes Wissen den Eltern vermitteln
→ Sich selbst als kompetent erleben

Ablauf

Phase 1

Jede/r Schüler/in bereitet eine 20-minütige Einführung/Präsentation für ihre/seine Eltern vor, wie man mit persönlichen Daten im Internet umgeht. Dabei werden Interessen, Wissensstand und Computerkenntnisse der Eltern berücksichtigt. Es kann auch darauf eingegangen werden, was die Eltern selbst in ihrer Jugend so alles gemacht haben und welche Folgen es gehabt hätte, wenn „Beweise“ dazu im Internet verfügbar gewesen wären.

Schüler/innen mit Eltern, deren Interessen und Vorwissen ähnlich sind, können diese Vorbereitung auch in Gruppen machen.

Während dieser Vorbereitungsphase sollen die Schüler/innen die Möglichkeit haben, Feedback für ihr Konzept von dem/der Lehrer/in bzw. den Klassenkolleg/innen einzuholen, z. B. indem sie Inhalte auf einer Lernplattform posten, in Kleingruppen diskutieren oder Einzelgespräche mit dem/der Lehrer/in führen.

Phase 2

Jede/r Schüler/in hat dann zwei Wochen Zeit, die Einführung/Präsentation für die Eltern durchzuführen. Diese kann beispielsweise auch im Rahmen eines Elternabends im EDV-Saal der Schule erfolgen.

Phase 3

Die Schüler/innen reflektieren miteinander, wie es war, die eigenen Eltern zu unterrichten.

- Wann war ich überrascht? Was habe ich so erwartet?
- Was haben meine Eltern verstanden? Mit welchen Inhalten hatten sie Schwierigkeiten?
- Welche generellen Ansichten vertreten meine Eltern, was den Umgang mit persönlichen Daten im Internet betrifft? Wie sehr deckt sich das mit meiner Meinung?

Ein/e Schüler/in moderiert die Diskussion in der Klasse, ein/e Schüler/in filmt, ein/e Schüler/in schreibt mit, ein/e Schüler/in stellt die Ergebnisse anschließend als Powerpoint-Präsentation auf die Schulwebsite, damit auch andere von den Ergebnissen profitieren können (Achtung: Urheberrechte und Datenschutz beachten!) etc.

Übung 6: „Schutz in Communitys“

Ziele

→ Konkrete Handlungsmöglichkeiten, wie man die eigene Privatsphäre in Communitys schützen kann, erlernen und anwenden

Ablauf

Phase 1

Die Schüler/innen gehen in Kleingruppen (4–5 Personen) zusammen. Jede Gruppe wählt eine Online-Community aus, auf der viel kommuniziert wird (z. B. Facebook, MySpace, Szene1.at, Google+ ...). Idealerweise sind die Schüler/innen (bzw. eine Person der Gruppe) dort bereits selbst aktiv. Nach Möglichkeit untersucht jede Gruppe eine unterschiedliche Online-Community. Als Einstieg könnte auch eine Community gemeinsam mit allen Schüler/innen besprochen werden. Folgende Fragen sollen bearbeitet werden:

- Wie kann ich mein Profil einstellen, damit meine persönlichen Daten möglichst gut geschützt sind?
- Was kann ich gegen ein peinliches Bild unternehmen, das ein/e andere/r Nutzer/in von mir online gestellt hat?
- Wie kann ich lästige Nutzer/innen ignorieren bzw. melden?
- Was steht in den Nutzungsbedingungen zum Schutz der Privatsphäre?
- Wie seriös erscheint mir der Umgang mit meinen Daten bei dieser Community?
- Wer sind die Nutzer/innen der Community, lassen sich bestimmte Richtungen erkennen (Alter, Schreibstil, Interessen etc.)?
- Wie lösche ich mein Profil aus der Community?

Phase 2

Jede Gruppe erstellt nun für die untersuchte Plattform eine Präsentation der bearbeiteten Fragen, z. B. in Form eines Plakats.

Phase 3

Jede Gruppe präsentiert in der Klasse ihre Ergebnisse. Abschließend findet eine Feedbackrunde statt:

- Waren die Tipps der Mitschüler/innen hilfreich?
- Warum ist es überhaupt wichtig, so etwas zu wissen?
- Wann und warum könnte es schwer fallen die Tipps einzuhalten?
- Welche Schwachstellen sind bei welchen Communitys aufgetaucht? Wo ist Vorsicht geboten?

Variante

Die Ergebnisse können auch allen anderen Schüler/innen und Eltern (z. B. im Rahmen einer Ausstellung in der Aula, in einem Artikel in der Schüler/innenzeitung, einem Beitrag auf der Schulwebsite oder einem Handyfilm) präsentiert werden.

Arbeitsblatt zu Übung 6: „Schutz in Communitys“

Arbeitsauftrag

Untersucht in der Gruppe eine von euch gewählte Online-Community (_____) und beantwortet dazu folgende Fragen:

- Wie kann ich mein Profil einstellen, damit meine persönlichen Daten möglichst gut geschützt sind?

- Was kann ich gegen ein peinliches Bild unternehmen, das ein/e andere/r Nutzer/in von mir online gestellt hat?

- Wie kann ich lästige Nutzer/innen ignorieren bzw. melden?

- Was steht in den Nutzungsbedingungen zum Schutz der Privatsphäre?

- Wie seriös erscheint mir der Umgang mit meinen Daten bei dieser Community?

- Wer sind die Nutzer/innen der Community, lassen sich bestimmte Richtungen erkennen (Alter, Schreibstil, Interessen etc.)?

- Wie lösche ich mein Profil aus der Community?

Übung 7: „Mein Fake-Profil“

Ziele

→ Eine Idee davon bekommen, wie einzelne Angaben von sich selbst auf andere wirken können
→ Angaben, die negative Folgen haben könnten, vermeiden lernen
→ Erkennen, wie schnell im Internet falsche Identitäten und Eindrücke entstehen können

Diese Übung eignet sich auch gut für eine Supplierstunde.

Ablauf

Phase 1

Jede/r Schüler/in erhält den Arbeitsauftrag, für sich selbst ein „falsches“ Community-Profil zu erstellen. Dazu wird das Arbeitsblatt auf Seite 76 mit beliebig erfundenen und durchaus auch überzogenen Inhalten und Bildern bestückt. Als Name wird ein Fantasiename gewählt. Wichtig für die weitere Übung ist, dass die Schüler/innen ihre Profile vorerst untereinander geheim halten.

Phase 2

Die fertig erstellten Fake-Profile werden einmal in der Mitte gefaltet und in eine Box geworfen. Anschließend zieht jede/r Schüler/in nach der Reihe ein Blatt aus der Box und stellt das gezogene Profil der Klasse vor. Danach wird das Arbeitsblatt auf einer Pinnwand aufgehängt.

Phase 3

Die Schüler/innen werden dazu angeregt, über die einzelnen Profile zu diskutieren:

- Welche Angaben sind ok? Was sollte man besser nicht veröffentlichen?
- Was für ein Mensch könnte wohl hinter diesem Profil stecken? Wie könnte sein/ihr Charakter sein?
- Welche Folgen könnten bestimmte persönliche Informationen jetzt und in einigen Jahren auf das „reale“ Leben haben?

Abschließend raten die Schüler/innen, wer das jeweilige Profil erstellt haben könnte.
Im Zuge dieser Diskussion soll auch gemeinsam reflektiert werden, was man als Betroffene/r unternehmen kann, wenn andere über einen selbst ein Fake-Profil anlegen.

Variante

Anstatt auf Papier können die Fake-Profile von den Schüler/innen auch als Word- oder Powerpoint-Datei erstellt werden. Zur Vorstellung der einzelnen Profile werden diese dann über Laptop und Beamer an die Wand projiziert.

Anmerkung

Diese Übung dient dazu, in spielerischem Umgang zu reflektieren, welche Angaben über die eigene Person in einem Community-Profil (oder auch anderswo im Internet) negative Folgen haben könnten. Oft kommen Inhalte, die man selbst gut findet, bei anderen ganz anders an als gedacht und können (ungewollt) ein falsches Bild von der eigenen Person vermitteln. U. a. könnten solche Inhalte auch Ausgang für Cyber-Mobbing-Aktivitäten sein. Aus diesem Grund empfiehlt es sich auch nicht, echte Community-Profile der Schüler/innen für Übungen im Unterricht heranzuziehen.

Mehr Informationen zum Thema „Cyber-Mobbing“ finden sich online unter **www.saferinternet.at/themen/cyber-mobbing** oder im Unterrichtsmaterial „Aktiv gegen Cyber-Mobbing“ unter **www.saferinternet.at/broschuerenservice**.

Arbeitsblatt zu Übung 7: „Mein Fake-Profil“

Hallo bei MyFace.at

Suche

Profilfoto

NAME

+ Als FreundIn hinzufügen

Aus _____ Geboren am _____

Pinnwand

Freunde (___)

_____

_____

 Dune

 Ice

_____

 Basti

 LisaLollipop

 King Kong

Allgemeines

Über mich _____

_____

_____

_____

Beziehungsstatus _____

Geschlecht _____

E-Mail _____

Kunst und Unterhaltung

Musik _____

Filme _____

Fernsehen _____

Spiele _____

Sport

Lieblingssportarten _____

Aktivitäten und Interessen

Interessen _____

_____

Exercise 8: World Café: "Talking about online threats"

Objectives

→ Reflect on your habits of posting personal data
→ Raising awareness of potential risks and dangers that can arise online

Procedure

This exercise is targeted towards English classes and should be done in two back-to-back classes.

Phase 1

The class is split up into 8 groups. Each group is assigned to a table. The tables are spread out all over the classroom and covered with white paper. On each table permanent markers are provided. Each group appoints one person as a spokesperson. This person will remain the spokesperson throughout the whole process.

Each table has one of the following issues assigned to it:

- Inappropriate usage of pictures online
- Identity theft (fake profile)
- Computer viruses
- Phishing (see also page 48)
- Sexting (see also page 44)
- Stolen or misused passwords
- Spam E-mail
- Cyber-Bullying

Each group is given 10 minutes to reflect on these topics and brainstrom relevant ideas on the flip chart:

- What could the term mean?
- Examples
- Have you ever experienced it yourself? Have you heard stories?
- How should one react, if it happens?
- How could it be prevented?

After 10 minutes, the group moves on to a different topic, while the spokesperson explains the groups rationale to the next group. The spokesperson tries to facilitate the discussion.
Due to time restrictions, not all of the topics can be discussed. Students have to choose the topics most relevant for them. Groups can also be split up after every change.

Phase 2

After five rounds, each spokesperson recounts the results, followed by a group discussion. Summarizing the discussion will be assigned as homework.

Übung 9: „Wer bin ich?“, für Volksschulklassen

Ziele

→ Eine andere Person im Internet erkennen können
→ Sicherheit im Umgang mit Online-Identitäten erwerben

Diese Übung ist speziell für 3./4.-Volksschulklassen gedacht.

Ablauf

Phase 1

Die Schüler/innen registrieren sich anonym mit einem Fantasienamen in einem geschützten Online-Chat oder -Forum. Ein entsprechender Bereich kann z. B. über Lernplattformen wie **edumoodle.at** eingerichtet werden. Nun haben die Schüler/innen einen bestimmten Zeitraum zur Verfügung (z. B. eine Unterrichtseinheit), um mit ihren Klassenkolleg/innen zu kommunizieren und dabei herauszufinden, wer sich hinter dem jeweiligen Nickname verbirgt.

Den Schüler/innen sollte während dieser Phase möglichst viel Freiraum gelassen werden, da sonst kein realitätsnahes Szenario entsteht, das für den weiteren Verlauf und Lerneffekt dieser Übung aber notwendig ist. D.h. die Schüler/innen sollten schreiben können, was sie wollen; sie dürfen nach Belieben Fotos, Links etc. verwenden; sie können in der Klasse herumgehen, um die Identitäten der anderen zu überprüfen („Lass mal schauen, ob du der xy bist!“) etc.

Phase 2

Am Ende der vereinbarten Zeit erfolgt die Auflösung: Wer ist wer?

Phase 3

Im Anschluss wird gemeinsam reflektiert:

- Woran erkenne ich, wer die andere Person ist?
- Wie kann ich andere besonders gut in die Irre führen? Wie wurde ich besonders gut in die Irre geführt?
- Was kann ich tun, wenn jemand anderer ein Foto von mir verwendet und ich das nicht möchte?
- Wie kann ich bei Fremden im Internet erkennen, wer das eigentlich ist?
- Was sollte ich von mir auf gar keinen Fall im Internet bekannt geben?

Anmerkung

Diese Übung dient dazu, in spielerischem Umgang zu reflektieren, welche Angaben über die eigene Person in einem Community-Profil (oder auch anderswo im Internet) negative Folgen haben könnten. Oft kommen Inhalte, die man selbst gut findet, bei anderen ganz anders an als gedacht und können (ungewollt) ein falsches Bild von der eigenen Person vermitteln. U. a. könnten solche Inhalte auch Ausgang für Cyber-Mobbing-Aktivitäten sein.

Diese Übung kann sehr schnell zu einer Eigendynamik führen, die auf die Lehrerin/den Lehrer durchaus negativ oder befremdlich wirken kann. Vergessen Sie nicht, dass das die Alltagsrealität der Kinder ist – zuhause würden sie sich nicht anders bzw. vielleicht sogar „schlimmer“ verhalten! Deshalb ist es wichtig, mit Kindern so früh wie möglich bestehende Internet-Risiken zu thematisieren.

(Übung bereitgestellt von Chris Wegmayr)

10 Tipps zum Schutz der Privatsphäre im Internet

1. **Nicht zu viel von sich preisgeben**
   Veröffentliche keine Fotos, Videos oder Texte, die später einmal zu deinem Nachteil verwendet werden oder dir peinlich sein könnten. Einmal veröffentlichte Daten sind oft nicht mehr zu entfernen.

2. **Persönliche Daten geheim halten**
   Wohnadresse, Telefonnummer, Passwörter etc. gehen Fremde nichts an. Wenn möglich, verwende einen anonymen Nickname anstelle deines richtigen Namens.

3. **Nicht alles glauben**
   Sei misstrauisch bei Behauptungen, die du im Netz findest. Oft ist es nicht klar, woher die Infos stammen und man weiß nie, ob jemand wirklich der ist, der er oder sie vorgibt zu sein. Überprüfe Infos daher besser mehrfach!

4. **Das Recht am eigenen Bild beachten**
   Die Verbreitung von Fotos oder Videos, die andere Personen nachteilig darstellen, ist meist nicht erlaubt. Frag zur Sicherheit die Abgebildeten vorher, ob sie mit einer Veröffentlichung einverstanden sind.

5. **Community-Profil nach außen schützen**
   Nutze die Einstellungsoptionen deiner Community für mehr „Privatsphäre", z. B. indem du den Zugriff auf dein Profil und die von dir eingestellten Inhalte auf „Freunde" beschränkst.

6. **Unerwünschte Nutzer/innen blockieren**
   Wenn du dich in einer Community oder per Messenger von jemandem belästigt fühlst, setze ihn/sie auf die „Ignorier"-Liste – der/die Nutzer/in kann dich dann nicht mehr kontaktieren.

7. **Sichere Passwörter verwenden**
   Sichere Passwörter bestehen aus einer Kombination aus mindestens acht Buchstaben, Zahlen und Sonderzeichen. Wähle stets verschiedene Passwörter für verschiedene Anwendungen und ändere diese regelmäßig. Halte Passwörter auch vor Freund/innen geheim.

8. **Computer schützen**
   Verwende ein Anti-Viren-Programm und aktualisiere es regelmäßig. Aktualisiere auch laufend deine Software, am besten per automatischem Update, installiere eine Firewall und verschlüssle deine WLAN-Verbindung.

9. **Vorsicht bei der Nutzung öffentlicher Computer**
   Hast du dich auf einer bestimmten Website (z. B. zum Checken deiner E-Mails oder deines Community-Profils) eingeloggt, melde dich auch stets wieder mit Klick auf „Logout" o. ä. ab. Lasse dir bei der Eingabe persönlicher Daten nicht von Fremden über die Schulter schauen!

10. **Wenn dir etwas komisch vorkommt, sag es!**
    Wenn du einmal kein gutes Gefühl beim Surfen hast, dann sprich darüber mit Erwachsenen, denen du vertraust. Auf irritierende oder gar bedrohliche Nachrichten einfach nicht antworten!

Weitere Tipps zur sicheren Internetnutzung findest du auf www.saferinternet.at.

Impressum

Unterrichtsmaterialien
Schutz der Privatsphäre im Internet

3. Auflage 2011

Medieninhaber, Herausgeber und Sitz der Redaktion:
Saferinternet.at/Österreichisches Institut für angewandte Telekommunikation
Margaretenstraße 70, 1050 Wien

Redaktion: DI[in] Barbara Amann-Hechenberger, DI[in] Barbara Buchegger, Mag. Piotr Luckos, Mag.[a] Katharina Maimer, Mag.[a] Sonja Schwarz

Design, Satz:
veni vidi confici® | Atelier für visuelle Kommunikation

Herstellung:
Gutenberg Druck GmbH, Johannes Gutenberg Straße 5, 2700 Wr. Neustadt

Rückfragen und Nachbestellungen:
Saferinternet.at/Österreichisches Institut für angewandte Telekommunikation
Margaretenstraße 70, 1050 Wien
Website: **www.saferinternet.at**
E-Mail: office@saferinternet.at
Telefon: (01) 595 21 12-0

Gefördert durch:
Bundesministerium für Unterricht, Kunst und Kultur – efit21: **www.efit21.at**
Österreichische Datenschutzkommission
Microsoft Österreich
Europäische Union – Safer Internet Programm: **http://ec.europa.eu/saferinternet**

Microsoft

Bist du dir sicher – mit uns Dreien?

Und wie! Mit uns beiden auf den ersten Blick, mit meinem PC auf den ersten Klick.
Dank der Programme von Microsoft. Die sind einfach, aktuell, schnell und automatisch sicher, vom Start weg. Klar gehört meine Software gepflegt – wie meine Beziehung auch.
Das ist aber einfach und geht sehr schnell. Wie?

Mit regelmäßigen Aktualisierungen bin ich auf dem sichersten Stand – und damit voll entspannt. Für noch mehr Sicherheit: Zuerst Augen auf, dann erst E-Mail auf. Egal ob beim Surfen oder Mailen, beim Shoppen oder Banken:
Mit den Programmen von Microsoft bin ich mir ganz sicher.

Hilf auch Du Deinem PC sicherer zu sein.
Mit nur drei einfachen Schritten schützt Du ihn vor den Gefahren des Internets.
www.microsoft.com/austria/PC-Schutz

Microsoft Infoservice
E-Mail: austria@microsoft.com
✆ 08000 123-345 (gebührenfrei)

Partner von Saferinternet.at:

bm:uk

bmwfj
Bundesministerium für Wirtschaft, Familie und Jugend

BUNDESKANZLERAMT ÖSTERREICH

Microsoft

A1