SAFER SURFING

TIPPS & TRICKS ZUM SICHEREN UMGANG MIT DEM INTERNET

Gefördert durch die Europäische Union

Saferinternet.at
Das Internet sicher nutzen!

bmwfj
Bundesministerium für Wirtschaft, Familie und Jugend

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)

IMPRESSUM

Safer Surfing – Tipps & Tricks zum sicheren Umgang mit dem Internet

Bildmaterial bereitgestellt von SAFT
Neuauflage 2011

Medieninhaber, Herausgeber und Sitz der Redaktion:
Saferinternet.at – www.saferinternet.at, office@saferinternet.at

ÖIAT – Österreichisches Institut für
angewandte Telekommunikation
Margaretenstraße 70
1050 Wien
www.oiat.at

ISPA – Internet Service Providers Austria
Verband der österreichischen Internet-Anbieter
Währinger Straße 3/18
1090 Wien
www.ispa.at

Gefördert durch die Europäische Union (Safer Internet Programm: http://ec.europa.eu/saferinternet).

Saferinternet.at-Partner:

Gefördert durch die Europäische Union

bmwfj Bundesministerium für Wirtschaft, Familie und Jugend

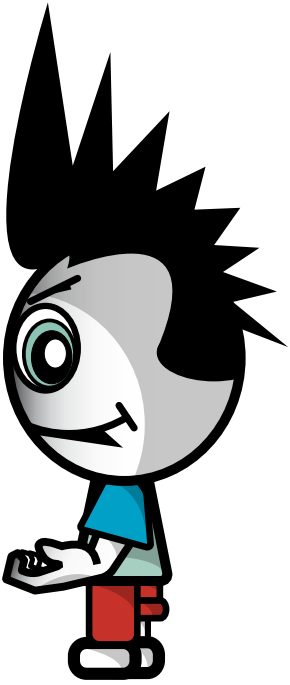
bm:uk

Microsoft

A1

ÜBER SAFERINTERNET.AT

Die Initiative Saferinternet.at unterstützt InternetnutzerInnen, besonders Kinder und Jugendliche, bei der sicheren Nutzung des Internet. Saferinternet.at ist die österreichische Informations- und Koordinierungsstelle im Safer Internet Netzwerk der EU (Insafe).



Die Initiative wird vom Österreichischen Institut für angewandte Telekommunikation (ÖIAT) in Kooperation mit dem Verband der Internet Services Providers Austria (ISPA) koordiniert und in enger Kooperation mit der öffentlichen Hand, NGOs und der Wirtschaft umgesetzt.

Die Finanzierung erfolgt durch das „Safer Internet Programm“ der EU-Kommission (GD Informationsgesellschaft & Medien), Ministerien und Sponsoren aus der Wirtschaft.

Mit dieser Broschüre möchte dir Saferinternet.at nützliche Infos und Tipps zum sicheren Umgang mit dem Internet geben und dabei helfen, unangenehme Überraschungen im Netz zu vermeiden. Mehr über Saferinternet.at und viele weitere Tipps findest du auf unserer Website: www.saferinternet.at.

Viel Spaß beim Lesen dieser Broschüre wünscht dir das Team von Saferinternet.at!

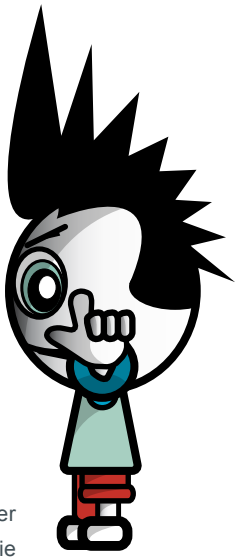
P. S.: Wenn du nach einem bestimmten Thema oder Begriff suchst, schau im Index ab Seite 70 nach, wo du in dieser Broschüre mehr Infos dazu findest. Das spart Zeit!

INHALT

10 TIPPS: SO SURFST DU SICHER

Internet-Surfen kann doch jeder! Da ist doch wirklich nichts dabei. Damit du aber auch im Web sicher unterwegs bist und keine bösen Überraschungen erlebst, hier die wichtigsten Tipps auf einen Blick:

1. Auch im Web gibt es Regeln



Alles, was man im „richtigen“ Leben nicht tun sollte oder nicht tun darf, soll man auch im Internet bleiben lassen.

2. Schütze deine Privatsphäre

Überlege dir genau, welche Angaben du über dich im Internet machst. Veröffentliche keine Bilder oder Texte, die später einmal zu deinem Nachteil verwendet werden könnten. Wenn möglich, gib keine persönlichen Daten wie Name, Wohnadresse, Handynummer etc. im Internet bekannt. Halte Passwörter auch vor FreundInnen geheim.

3. Nicht alles ist wahr

Sei misstrauisch bei Behauptungen, die du im Netz findest. Oft ist 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. Urheberrechte beachten

Das Anbieten und Weiterverwenden (z.B. in Blogs, Profilen) von Musik, Videos, Bildern und Software ist – ohne Einwilligung der UrheberInnen – verboten. Es drohen bis zu mehrere Tausend Euro Strafe.

5. Das Recht am eigenen Bild

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.

10 TIPPS: SO SURFST DU SICHER

6. Quellenangaben nicht vergessen

Wenn du Textteile anderer AutorInnen verwendest, mach immer deutlich, dass es sich nicht um dein eigenes Werk handelt und führe die richtigen Quellenangaben an.

7. Umsonst gibt's nichts

Auch im Internet ist selten etwas wirklich kostenlos. Sei bei „Gratis"-Angeboten stets misstrauisch, besonders wenn du dich mit Namen und Adresse registrieren musst.

8. Online-Freunde niemals alleine treffen

Nimm beim ersten Treffen immer einen Erwachsenen mit, dem du vertraust.

9. Computer schützen

Verwende ein Anti-Viren-Programm und aktualisiere es regelmäßig. Aktualisiere auch laufend deine Software, am besten per automatischem Update.

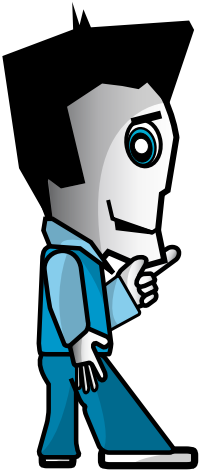
10. Wenn dir etwas komisch vorkommt, sag es!

Auf irritierende oder gar bedrohliche Nachrichten einfach nicht antworten!
Bei www.rataufdraht.at erhältst du kostenlos, anonym und rund um die Uhr telefonische Hilfe, wenn du einmal nicht mehr weiter weißt.

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

P.S.: Hänge diese Seiten doch einfach in der Nähe deines Computers auf. So hast du die „Sicherheit im Netz" immer im Blick!

DOS AND DON'TS



Eigentlich ist ja alles ganz einfach:

WAS IM REALEN LEBEN ERLAUBT IST,
IST AUCH IM INTERNET ERLAUBT,
WAS IM REALEN LEBEN VERBOTEN IST,
IST AUCH IM INTERNET VERBOTEN.

So einfach ist das. Oder doch nicht?

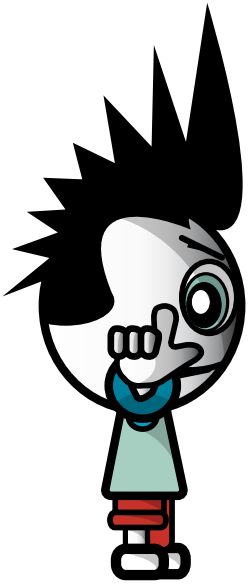
Viele Menschen glauben, dass sie im Internet anonym sind und daher die normalen gesellschaftlichen Umgangsformen für sie nicht gelten.

Abgesehen davon, dass es eigentlich egal sein sollte, ob man erwischt werden kann oder nicht: Wie ist das eigentlich mit der Anonymität? **BIN ICH IM INTERNET ANONYM?** Die kurze Antwort darauf lautet **„NEIN!"**, die längere ist etwas komplizierter:

WERDEN WIR KONKRETER:
Würdest du deine/n LehrerIn oder deine/n ChefIn von Angesicht zu Angesicht beschimpfen? Würdest du in ein Geschäft gehen und die Ware ohne zu bezahlen mitnehmen? Würdest du dich mit deiner CD-Sammlung und einem CD-Brenner auf die Straße setzen und alle vorbeikommenden Leute einladen, eine Kopie davon zu machen? NEIN? Siehst du, und dasselbe gilt für das Internet.

DOS AND DON'TS

ANONYMITÄT



Alle Computer, die mit dem Internet verbunden sind, haben eine eindeutige Adresse, über die sie identifiziert werden können, die so genannte **„IP-ADRESSE“**. Das ist ein Zahlencode, der einem Rechner entweder fix zugeordnet ist (wie z.B. bei vielen Kabelgesellschaften) oder vom Provider dynamisch vergeben wird.

Wann immer ein/e UserIn im Internet etwas macht (z.B. Chatten, eine E-Mail schreiben, eine Website besuchen), wird die IP-Adresse des jeweiligen Rechners in einem Logfile gespeichert bzw. zusätzlich auch noch im „Header“ der E-Mail verewigt.

MAN HINTERLÄSST ALSO SPUREN, WENN MAN SICH IM INTERNET BEWEGT. Diese Spuren sind nicht immer sofort einer bestimmten Person zuzuordnen, sie können aber – wenn z.B. die Polizei eine Anzeige erhält – miteinander verknüpft werden und führen dann zur Identität des/der entsprechenden UserIn.

Auch andere BenutzerInnen desselben Computers können sich manchmal ansehen, welche Websites ihre VorgängerInnen besucht oder welche Programme sie aufgerufen haben.

Mit etwas technischem Sachverstand lässt sich sehr viel über andere herausfinden. Natürlich gibt es Tools, um sich gegen diese Art von Schnüffelei zu wehren. Diese setzen aber meist sehr viel technisches Wissen voraus und geben trotzdem keine 100%ige Sicherheit. Wenn jemandem genügend Daten (Logfiles, Nicknames, Passwörter etc.) zur Verfügung stehen, kann er/sie meist auch den schlauesten Internet-UserInnen das Handwerk legen. Denn irgendwann macht jeder einen Fehler.

DOS AND DON'TS

COMMUNITY-GUIDELINES / NETIQUETTE

Für viele UserInnen sind Communitys, Foren, Chats, Messenger etc. wichtige Kommunikationsmittel und Zeitvertreib. Hier kann man sich einbringen, Infos, Fotos und Videos austauschen, neue Leute kennenlernen, andere Identitäten annehmen und seinen Hobbys nachgehen. Dabei gibt es einige wenige Grundregeln, die so genannte „Netiquette", die du beim Kommunizieren einhalten solltest:

Regel Nummer eins:

ERST LESEN, DANN SCHREIBEN

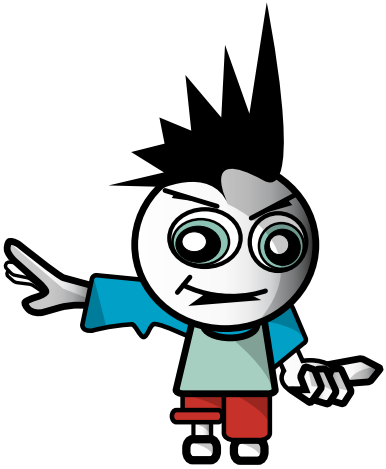
Es ist wie im richtigen Leben: Wenn du in einem fremden Land ein Lokal betrittst, solltest du halbwegs im Bilde sein, wie die Gebräuche dieses Landes im Allgemeinen und die Regeln des Lokales im Speziellen sind. In einem islamischen Land wirst du dich anders verhalten als an einem karibischen Strand, in einem Drei-Hauben-Restaurant anders als in einer Bar.

Genauso ist es auch im Netz: Schon länger bestehende Communitys haben oft eigene Benimm-Regeln erarbeitet (meist kann man diese auf den zugehörigen Websites nachlesen), und wenn man sich als Neuling nicht an diese hält, gilt man im besten Fall als unhöflich, im schlechteren als dämlich. Jedenfalls ist der Einstieg gründlich daneben gegangen. Deshalb schadet es nicht, sich ein wenig einzulesen, bevor man sich selbst zu Wort meldet. Alteingesessene UserInnen wollen nicht ständig dieselben Fragen beantworten, deshalb haben Communitys oft so genannte FAQs („Frequently Asked Questions", eine Zusammenstellung häufig gestellter Fragen) online. Und denk dran: Auf blöde Fragen bekommt man auch blöde Antworten!

DOS AND DON'TS

Regel Nummer zwei:

NIE MIT WUT IM BAUCH SCHREIBEN



Die Tatsache, dass sich die teilnehmenden Personen in Online-Communitys nicht sehen können, verführt leicht zu einer etwas gröberen Ausdrucksweise als bei der Kommunikation von Angesicht zu Angesicht. Denk immer daran, dass am anderen Ende der Leitung ein richtiger Mensch sitzt und eine einmal gesendete Message nicht mehr zurückgeholt werden kann. Gib dir selbst ein paar Stunden oder einen Tag Zeit bis der erste Ärger verraucht ist und du wieder klar denken kannst. Dann schreib deine E-Mail, dein Posting oder deine Chat-Nachricht, aber bleibe sachlich in deiner Kritik, beleidige niemanden und stehe zu deiner Meinung. Dann hast du nichts zu bereuen und auch nichts zu befürchten. Und: **;-)**.

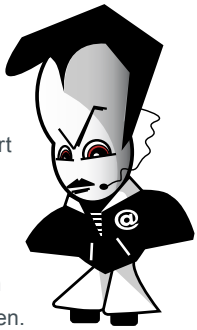
Regel Nummer drei:

ANDERE LESEN MIT

In Web bist du alles andere als anonym. Wenn du in Communitys, Foren und Chats etwas postest, geh immer davon aus, dass alle deine FreundInnnen, LehrerInnen, Eltern und eine Menge anderer Leute mitlesen können. Nur wenn du diese Regel beachtest, brauchst du nie ein schlechtes Gewissen zu haben. Falls du darauf hoffst, dass alles irgendwann einmal gelöscht wird: Online-Postings bleiben oft über Jahre im Netz gespeichert und können von Suchmaschinen ganz leicht gefunden werden.

DOS AND DON'TS

WAS IST IM NETZ VERBOTEN?



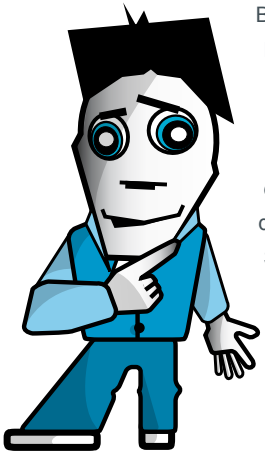
Wie schon gesagt, im Großen und Ganzen ist es wie im wirklichen Leben: was dort verboten ist, ist auch im Internet verboten.

AB WELCHEM ALTER KANN ICH MICH STRAFBAR MACHEN?

Du sagst „Ich bin eh erst 14, mir kann nix passieren". Ist das richtig? Ab deinem 14. Geburtstag kannst du für strafbare Handlungen verantwortlich gemacht werden. Bis zu deinem 18. Geburtstag gilt allerdings das Jugendstrafrecht, das geringere Strafausmaße vorsieht.

Das heißt aber nicht, dass man unter 14 Jahren tun und lassen kann, was man will! Es können die Eltern zur Verantwortung gezogen werden, wenn sie ihre Aufsichtspflicht verletzt haben.

PORNOGRAFIE IM INTERNET

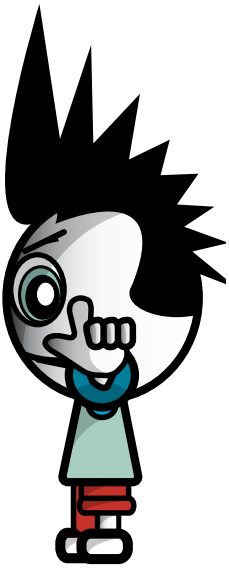


Bei vielen Seiten mit pornografischem Inhalt finden sich auf der Startseite Hinweise, dass diese nur von Personen über 18 Jahre besucht werden dürfen. Manchmal muss man auch auf Formulierungen wie „über 18" klicken. Beides soll vor allem der eigenen Absicherung der SeitenbetreiberInnen dienen, sich nicht selbst strafbar zu machen. Wenn du unter 18 bist und trotzdem eine solche Seite besuchst, hat das für dich keine rechtlichen Folgen. Anders ist es, wenn sich auf einer solchen Seite illegale Bilder befinden, in erster Linie Kinderpornografie. Hier ist seit dem 1.6.2009 neben dem Besitz auch die wissentliche Betrachtung strafbar. Besitz liegt dann vor, wenn eine solche Darstellung auf dem eigenen Computer gespeichert wird. In der Regel werden die Inhalte einer Website schon beim bloßen Ansehen vorübergehend auf der Festplatte gespeichert! Bereits das kann als Besitz eines Bildes gelten! Eine wissentliche Betrachtung kann z.B. dann angenommen werden, wenn eine Website mit eindeutigem Material wiederholt besucht wird.

DOS AND DON'TS

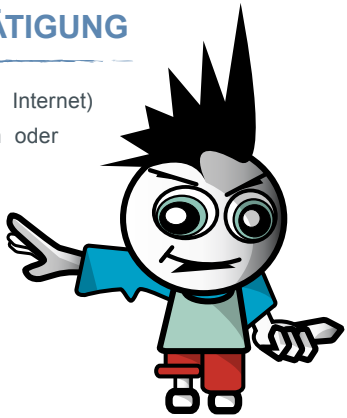
Als **KINDERPORNOGRAFIE** gilt vor allem die Darstellung sexueller Handlungen an Personen unter 18 oder von Personen unter 18 an sich selbst, an anderen oder an Tieren. Es kann bereits eine Abbildung reichen, wo die Genitalien oder der Schambereich abgebildet sind, wenn diese der sexuellen Erregung des Betrachters dient. Pornografische Darstellungen mit Kindern unter 14 sind immer strafbar. Bei Betrachten oder bloßem Besitz von Kinderpornografie gilt ein Strafrahmen von bis zu einem Jahr, handelt es sich um Aufnahmen Unmündiger (unter 14), beträgt der Strafrahmen zwei Jahre Gefängnis (für Erwachsene). Diese Strafe kann sich auf bis zu drei Jahre erhöhen, wenn man Kinderpornografie herstellt oder auch nur anderen zugänglich macht. Jemand, der sich z.B. ein Kinderporno-Video über eine Tauschbörse herunterlädt und dieses Video anderen zum Download bereitstellt, fällt unter den höheren Strafsatz. Wenn du auf Kinderpornografie im Internet aufmerksam wirst, kannst du dich anonym an www.stopline.at (eine Meldestelle der Internet-Provider) wenden.

ABER HALT, natürlich ist es nicht strafbar, wenn du mit deinem Freund oder deiner Freundin Fotos zum eigenen Gebrauch anfertigst. Das Gesetz sieht in diesem Fall die Straflosigkeit vor, wenn der/die Abgebildete über 14 Jahre alt ist und diese Fotos mit seiner/ihrer Zustimmung hergestellt werden. Der Gesetzgeber will sich nicht in euer privates Leben einmischen. Aber: Die Weitergabe der Bilder an Dritte ist nicht nur unfair, sondern kann beispielsweise auch sogar strafbar sein, wenn diese Bilder eine pornografische Darstellung Minderjähriger beinhalten. Das gilt übrigens auch, wenn du dich an deinem Ex-Freund/deiner Ex-Freundin rächen willst und dessen/deren Bilder ungefragt weiterschickst.



DOS AND DON'TS

NATIONALSOZIALISTISCHE WIEDERBETÄTIGUNG



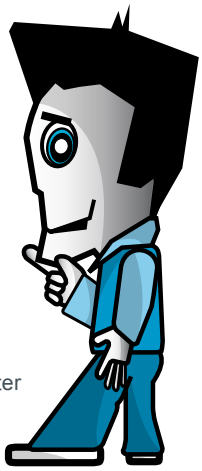
Es ist strafbar, in einem Medium (dazu gehört auch das Internet) nationalsozialistische Verbrechen zu leugnen, zu verharmlosen oder gutzuheißen („Auschwitz-Lüge"). Der Strafrahmen beträgt bis zu zehn Jahren Haft. Noch empfindlichere Strafen gibt es für die Gründung von nationalsozialistischen Verbindungen, das Anwerben von Mitgliedern für eine solche Verbindung oder auch für die bloße Beteiligung daran. Diese Handlungen sind alle auch im Internet möglich.

ILLEGALE FOREN UND CHATS

In Foren und Chats wird keineswegs nur über harmlose Themen diskutiert. Statt von Modellbau ist von Bombenbasteln und Drogen zum Selbermachen (z.B. Anbau von Cannabispflanzen) die Rede, es gibt Foren zum Adressaustausch von Kinderpornoseiten oder zur Verabredung zum Selbstmord. Das Verfolgen der Diskussion in solchen Foren ist noch nicht strafbar. Dies kann aber bei „konstruktiven" Beiträgen sehr wohl der Fall sein. Adressen von Kinderpornoseiten zu posten ist als Zugänglichmachen von Kinderpornografie strafbar (Strafrahmen drei Jahre). Auch das Veröffentlichen einer Anleitung zur Herstellung von Drogen kann als Beihilfe zur Erzeugung strafbar sein. Weiters ist die Mitwirkung bei Selbstmord in Österreich strafbar, z.B. jemanden durch Bestärkung zum Selbstmord zu verleiten. Allerdings müsste eine sehr starke psychologische Beeinflussung vorliegen, die über das Internet schwer möglich ist. Der bloße Satz „Bring dich ruhig um, is eh net schad um dich" wird jedenfalls nicht ausreichend sein (ist aber trotzdem nicht nett).

DOS AND DON'TS

HACKING

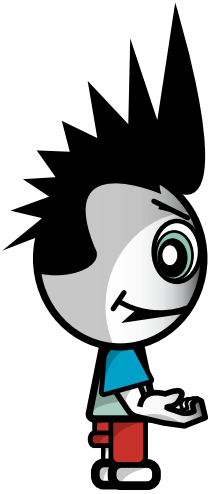


Beim Hacking handelt es sich um unerlaubtes Eindringen in ein fremdes Computersystem. Dies ist allerdings nur dann strafbar, wenn Sicherheitsvorkehrungen des Systems verletzt bzw. überwunden werden und der/die TäterIn sich zusätzlich einen Vermögensvorteil verschafft oder den/die BetreiberIn des Systems schädigen will (z.B. durch Auskundschaften von Betriebsgeheimnissen, Löschen der Festplatte). Auch die schwere Störung der Funktionsfähigkeit eines fremden Computersystems ist strafbar, genauso wie das Umgehen von Zugangsbeschränkungen oder technischen Sperren. Eine Freiheitsstrafe bis zu zwei Jahren ist möglich.

Das Verwenden von Hacking-Tools oder Computerviren ist als so genannter „Missbrauch von Computerprogrammen" seit 2003 im österreichischen Strafrecht genannt. Das Abfangen von Daten, die über Computernetzwerke übermittelt werden und nicht für dich bestimmt sind, ist ebenfalls verboten. Sowohl im Strafgesetzbuch als auch im Telekommunikationsgesetz gibt es weitere Strafbestimmungen, die es verbieten, fremde E-Mails zu lesen oder sonstige fremde Daten anzusehen oder weiterzugeben. Denk dran: Du würdest doch auch im realen Leben nicht einfach die Briefe deiner Nachbarin öffnen oder den Schulrucksack deines besten Freundes durchwühlen!

DOS AND DON'TS

WELCHE MÖGLICHKEITEN GIBT ES, MICH IN COMMUNITYS, CHATS & CO. STRAFBAR ZU MACHEN?



BELEIDIGUNG

Eine Beleidigung liegt vor, wenn du eine andere Person öffentlich oder vor mehreren Leuten (mindestens zwei zusätzliche Personen) beschimpfst oder verspottest (z.B. „saublöd", „bescheuert"). Greifst du eine andere Person unter Angabe ihres echten Namens auf der eigenen Website, in Chats, Foren oder Communitys an, kannst du dich leicht strafbar machen. Der Strafrahmen beträgt bis zu drei Monate, meist gibt es Geldstrafen. Handelt es sich um Foren und Chats, die nur den Zweck haben, sich gegenseitig wüst zu beschimpfen, gilt wohl der Grundsatz „Teilnahme auf eigene Gefahr".

Selbst wenn es sich um anonyme Beteiligte in einem Chatroom handelt, kann eine Beleidigung vorliegen, z.B. wenn die beleidigte Person regelmäßig unter dem gleichen Nickname auftritt und auf Grund des Imageverlustes diesen Nickname nicht mehr verwenden kann.

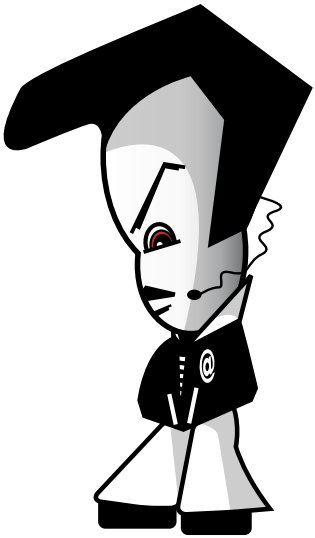
DOS AND DON'TS

ÜBLE NACHREDE

Üble Nachrede ist der Vorwurf einer verächtlichen Eigenschaft oder Gesinnung oder eines unehrenhaften Verhaltens (z.B. „Faschist", „Rechtsextremist") oder eines Verhaltens gegen die guten Sitten in der Öffentlichkeit. Für das Kriterium „Öffentlichkeit" reicht schon die Anwesenheit einer einzigen weiteren bzw. dritten Person. Eine wahre Behauptung ist nicht strafbar, allerdings muss der Behauptende die Wahrheit beweisen. Straffrei ist auch das Zitat einer fremden Äußerung, solange man sich nicht mit dem Inhalt identifiziert („In der Zeitung habe ich gelesen, dass ..."). Die Strafe kann bis zu sechs Monate betragen. Werden die Behauptungen jedoch einer breiten Öffentlichkeit zugänglich gemacht, was bei übler Nachrede im Internet meist der Fall ist, gilt ein Strafrahmen bis zu einem Jahr.

VERLEUMDUNG

Eine Verleumdung liegt vor, wenn man jemandem die Begehung einer Straftat vorwirft, obwohl man weiß, dass der Vorwurf nicht zutrifft. Der Vorwurf muss aber so konkret sein, dass der/die Betroffene eine behördliche Verfolgung (durch Polizei oder Staatsanwaltschaft) zu erwarten hat (z.B. „Der Karli hat gestern bei der Gumpendorfer Straße mit Heroin gedealt"). Die Strafe kann je nach Schwere der vorgeworfenen Straftat entweder bis zu einem Jahr oder bis zu fünf Jahren betragen.



E-MAIL,SPAM & PHISHING

Die E-Mail war eine der ersten Anwendungen im Internet und ist bis heute auch eine der Wichtigsten. Hier eine kurze Übersicht, worauf man aufpassen sollte:

1. VERSCHICKEN VON E-MAILS

In den Anfangstagen des Internet wurden Neulinge oft darauf hingewiesen, vor dem Versenden von E-Mails oder dem Mitdiskutieren in Newsgroups erst die „Netiquette“ zu lesen. In dieser Sammlung von Benimmregeln stand unter anderem noch zu lesen, dass man keine Umlaute verwenden soll, da diese nicht auf allen Computern darstellbar wären. So streng sind die Regeln heute zum Glück nicht mehr, trotzdem kannst du dir und anderen das Leben erleichtern: **ATTACHMENTS** (Dateianhänge) sollte man nur mitschicken, wenn diese unbedingt notwendig sind. Größere Anhänge sollte man nur verschicken, wenn der/die EmpfängerIn vorgewarnt wurde. Es ist ganz schlechter Stil, eine leere E-Mail zu versenden und den Text einfach in eine angehängte Word-Datei zu packen.

HTML-MAILS (Nachrichten mit Bildern, Farben, verschiedenen Schriftstilen etc.) können zwar von den meisten E-Mail-Programmen dargestellt werden, sind aber viel größer als reine Text-E-Mails. Außerdem ist die Darstellung in den verschiedenen Programmen durchaus unterschiedlich. Als Faustregel gilt: Nur dann HTML-Mails versenden, wenn es notwendig und passend ist (z.B. bei einer schön gestalteten Einladung), ansonsten ist normaler Text ausreichend. Niemand braucht zum Verstehen der Nachricht „Ich komme heute etwas später“ einen Blümchenhintergrund – solche E-Mails wirken eher peinlich.

Die Einstellungen **„WICHTIG“** oder **„DRINGEND“** sollte man nur verwenden, wenn der Inhalt auch entsprechend ist. Leute, die diese Optionen routinemäßig anklicken, sagen damit mehr über sich selbst aus als über ihre E-Mails...

E-Mails an viele verschiedene EmpfängerInnen sollten als **BCC** (Blind Carbon Copy) verschickt werden. Diese Einstellung bewirkt, dass die EmpfängerInnen untereinander nicht sehen, wer die E-Mail noch bekommen hat. Dadurch wird die Vertraulichkeit der E-Mail-Adressen gewahrt.

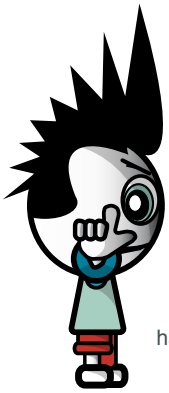
E-MAIL,SPAM & PHISHING

2. WAS TUN MIT SPAM?

In deiner Mailbox findest du täglich eine größere Anzahl an E-Mails, die dir diverse Produkte – von Finanzdienstleistungen bis Potenzmittel – anbieten. Du brauchst aber keinen Kredit und schon gar nicht Viagra, im Übrigen nervt dich das dauernde Löschen dieser E-Mails. Was kannst du tun?

Eine Zusendung von Werbemails an Private ist ohne vorherige Einwilligung des Adressaten nicht erlaubt, ebenso Zusendungen an mehr als 50 Personen, deren Einwilligung nicht vorliegt.

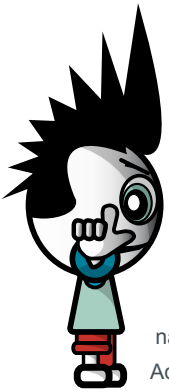
Erlaubt wäre eine Zusendung von Werbemails in folgendem Fall: Du hast deine E-Mail-Adresse bei einer Bestellung dem Online-Shop oder Versandhandel bekannt gegeben und hast der Zusendung von Werbemails zugestimmt (z.B. durch Ankreuzen eines Kästchens mit dem Text „Ich stimme der Zusendung von E-Mails zu“). In den Werbemails darf das Unternehmen aber nur eigene Produkte bewerben und muss dir Gelegenheit geben, weitere Werbemails abzulehnen. Erhältst du unerlaubte Werbemails, könntest du gegen den Absender Anzeige beim Fernmeldebüro erstatten. Der Absender muss dann Strafe bezahlen. Bei Zusendung von Werbemails aus dem Ausland ist das allerdings nicht möglich.



Generell ist davon abzuraten, eine E-Mail mit einer Ablehnungserklärung („remove me“) zurückzusenden. **Oft bekommt man nur noch mehr Spam, wenn man auf Spam reagiert!** Die Spam-Versender wissen dann nämlich, dass deine E-Mail-Adresse aktiv ist.

Wenn du bereits Spam erhältst, können dir Spamfilter helfen. Informiere dich bei deinem webbasierten E-Mail-Dienst oder in der Hilfe deines E-Mail-Programms am Computer, wie du Spamfilter nutzen kannst.

E-MAIL,SPAM & PHISHING

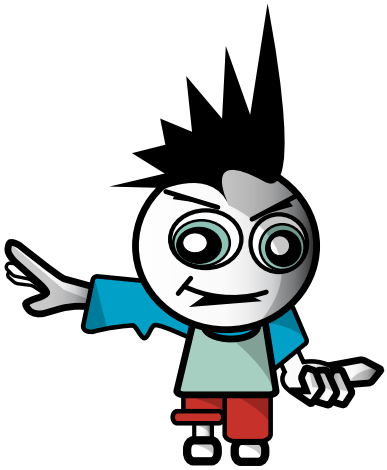


Du kannst aber einiges tun, um nicht in Zukunft noch mehr Spam zu erhalten. **DIE EINFACHSTE REGEL IST, IMMER (MINDESTENS) ZWEI E-MAIL-ADRESSEN ZU VERWENDEN:** eine, um mit Freunden, Bekannten und Familienmitgliedern E-Mails auszutauschen, und eine andere, um sich damit in Communitys zu registrieren, in Gästebüchern zu posten oder in Foren mitzudiskutieren. Die erste Adresse bleibt wahrscheinlich spamfrei, die zweite kannst du wieder löschen lassen, wenn du dorthin zu viel Müll bekommst. Spammer durchsuchen nämlich insbesondere Websites und Newsgroups nach immer neuen Adressen. Kostenlose E-Mail-Adressen erhältst du zum Beispiel bei Yahoo!, Windows Live Hotmail oder Google Mail.

Weiters besteht auch die Möglichkeit, sich in die sogenannte **„ECG-LISTE“** einzutragen. Das ist eine Liste von Personen, die eine Zusendung von Werbemails ausdrücklich nicht wünschen. Die „ECG-Liste“ wird in Österreich von der Rundfunk und Telekom Regulierungs-GmbH (RTR) geführt. Auf der Website der RTR gibt es nähere Infos, wie du dich in die Liste eintragen kannst, sowie eine ausführliche Spam-Broschüre zum kostenlosen Download.
(www.rtr.at/de/tk/E_Commerce_Gesetz).

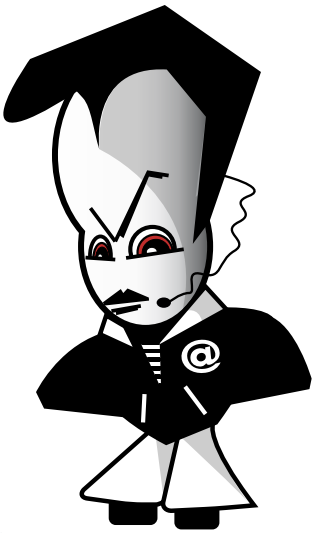
3. DARF ICH SELBST SPAM VERSENDEN?

Angenommen, du besuchst eine HTL und wartest regelmäßig für Geld PCs oder programmierst Websites. Willst du deine Dienstleistung mittels E-Mail bewerben, solltest du die oben geschilderten Punkte beachten. Kein Problem hast du, wenn alle EmpfängerInnen vorher zugestimmt haben. Eine Abstrafung durch das Fernmeldebüro oder ein Gericht kann dich bis zu EUR 37.000,- kosten.



E-MAIL,SPAM & PHISHING

4. WIE ERKENNE ICH „PHISHING“-MAILS?



Eine besondere Form des **ONLINE-BETRUGS** ist das so genannte „Phishing“. Dabei versuchen BetrügerInnen **mittels gefälschter Websites und E-Mails** an die Passwörter ahnungsloser InternetnutzerInnen für Online-Bankkonten, Auktions-Plattformen, Online-Shops oder Ähnliches zu kommen. Der/die UserIn erhält meist eine täuschend echte E-Mail, in der er oder sie aufgefordert wird, auf einen Link zu klicken und sich unter irgendeinem Vorwand in seinen/ihren 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. Denk immer daran:

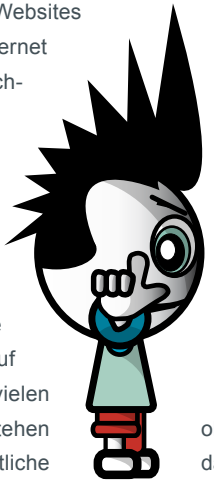
+ Banken, Online-Shops, Auktionshäuser etc. fragen sensible Daten Ihrer Kunden **NIEMALS** via E-Mail ab – ignoriere solche Nachrichten daher!

+ 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!

COMPUTERSICHERHEIT & PASSWÖRTER

VIREN UND TROJANER SIND IN ALLER MUNDE

Mailserver brechen zusammen, Websites sind nicht erreichbar und das Internet generell für Tage nur mäßig brauchbar. Die heutige Generation von Viren (und, korrekt ausgedrückt, Trojanern) schadet nicht mehr (ausschließlich) der- oder demjenigen, die/der den Virus hat. Frühere Virengenerationen löschten einfach die Festplatte oder gewisse Arten von Files auf dem verseuchten Rechner. Hinter vielen aktuellen Schadprogrammen stehen heute handfeste wirtschaftliche



Interessen: Einerseits das Sammeln von E-Mail-Adressen (die auf den verseuchten Computern zu finden sind), andererseits werden diese Computer als so genannte „Zombies“ missbraucht. Über sie werden später zigtausende Spams versendet. Viele andere Missbrauchsmöglichkeiten sind denkbar, da die befallenen Rechner für HackerInnen völlig offen sind und von außen jederzeit gesteuert werden können – ohne, dass die BenutzerInnen etwas davon merken.

WIE KANN ICH MICH VOR VIREN SCHÜTZEN?

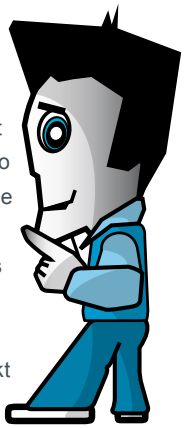
Die einfachste – aber leider nicht immer ausreichende – Regel zum Schutz vor Viren ist, **KEINE UNBEKANNTEN DATEIANHÄNGE („ATTACHMENTS“) HERUNTERZULADEN ODER GAR ZU ÖFFNEN** bzw. auszuführen. Attachments mit Viren können durchaus von bekannten AbsenderInnen stammen, da sich viele Viren über die Adressbücher der befallenen Rechner selbstständig weiterversenden. Deaktiviere auch unbedingt im Browser und im E-Mail-Programm sowie im ZIP-Programm die Voreinstellung, dass heruntergeladene Dateien sofort ausgeführt werden. Solltest du nämlich doch versehentlich einen Virus auf deiner Festplatte haben, so kann dieser erst aktiv werden, wenn er einmal aufgerufen wurde.

COMPUTERSICHERHEIT & PASSWÖRTER

Wenn du folgende vier Punkte beachtest, ist dein Computer 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 ein **ANTI-SPYWARE-PROGRAMM** zu verwenden.

Weitere Infos, Hilfestellungen und nützliche Links zum Thema „Computersicherheit“ und zu den verschiedenen Schutzprogrammen (sowohl kostenpflichtige als auch kostenlose) erhältst du auf der Website von Saferinternet.at.

COMPUTERSICHERHEIT & PASSWÖRTER

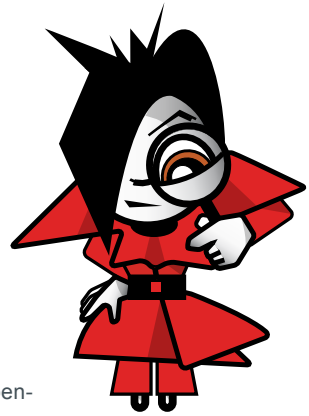
WIE SIEHT EIN SICHERES PASSWORT AUS?

+ Verwende Passwörter, die aus mindestens acht Buchstaben (variiere mit Groß- und Kleinschreibung), Zahlen und Sonderzeichen (z.B. - + = ! ? % ^ & * @ # $ ( ) [ ] \ ; : " / , . < >~) bestehen.
+ 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!

MERKE: 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. Bestimmt hast du auch schon davon gehört, dass Zahnbürsten regelmäßig gewechselt werden sollten – genauso ist es mit Passwörtern.

EIN TIPP ZUM MERKEN VON PASSWÖRTERN:

Hilf dir mit Eselsbrücken, z.B. für das Passwort „IbegFvFM4!“:
„**I**ch **b**in **e**in **g**roßer **F**an **v**on **FM4**!“.



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 aufbewahren.
+ Verschlüssele dein Passwort zusätzlich, z.B. durch Buchstaben-, Silben- oder Zahlendreher (schreibe z.B. statt „13“ „31“).

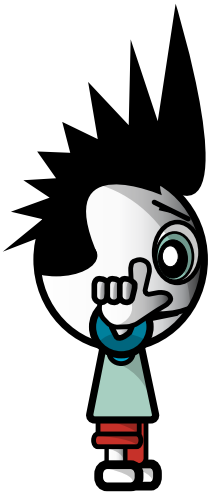
Wenn du glaubst, dass jemand anderer dein Passwort herausgefunden hat, solltest du es am besten sofort ändern! Ändere deine Passwörter am besten überhaupt regelmäßig.

COMPUTERSICHERHEIT & PASSWÖRTER

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:

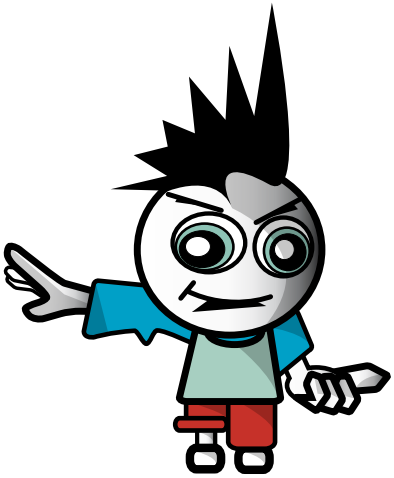
1. Speichere nie deine Login-Daten: Hast du dich auf einer bestimmten Website (z.B. zum Checken deiner E-Mails oder deines Community-Profils) eingeloggt, melde dich auch stets wieder mit Klick auf „Logout“ o.ä. ab. Es reicht nicht, einfach das Browserfenster zu schließen oder eine andere Internetadresse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



2. Lass 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 Webbrowser 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“ und lösche dort den gesamten Browserverlauf. Bei Firefox findest du diese Möglichkeit unter „Extras >> Einstellungen >> Datenschutz“. Mit dem „In Private Browsing“-Modus des Internet Explorer 8 werden von Haus aus keine Verläufe, temporäre Dateien oder Cookies gespeichert. Das gilt auch für den „privaten Modus“ bei Firefox ab Version 3.5. Diese Funktionen bieten sich also grundsätzlich beim Surfen auf gemeinsam benutzten Computern an.

COMPUTERSICHERHEIT & PASSWÖRTER



4. Lass niemanden zuschauen: Achte bei der Nutzung eines öffentlichen Computers immer darauf, dass dir niemand Fremder über die Schulter schaut und dabei vertrauliche Daten ausspionieren könnte.

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

6. Vorsicht bei drahtlosen Netzwerken: Wenn du dich mit deinem Laptop in einen öffentlichen „Hotspot“ 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 neusten Stand sind.

TAUSCHBÖRSEN (FILE-SHARING-NETZWERKE)

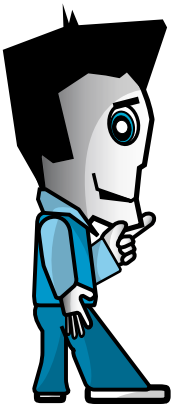
SO BELIEBT WIE UMSTRITTEN SIND ONLINE-TAUSCHBÖRSEN, WO MUSIK, VIDEOS ODER AUCH SOFTWARE GETAUSCHT WERDEN KÖNNEN.

Millionen UserInnen verwenden täglich kazaa, limewire, verschiedene BitTorrent-Clients oder ähnliche Programme. Durch das Herunterladen eines Werks von einer derartigen Tauschbörse verstößt du in der Regel gegen das Urheberrecht.

Ein Werk ist eine individuelle geistige Schöpfung im Bereich der Musik, der Literatur, der bildenden Kunst oder der Filmkunst. Diese Schöpfung muss eine gewisse kreative Leistung sein. Computerprogramme gelten nach österreichischem Urheberrecht als Sprachwerke, also als Werke der Literatur. Das gilt auch für Computerspiele.

Der/die UrheberIn hat das alleinige Recht, sein/ihr Werk öffentlich zugänglich zu machen, zu vervielfältigen, zu verbreiten, zu senden, zu verleihen und aufzuführen. Auf Tauschbörsen und auch Websites werden vor allem zwei Rechte verletzt: **EINERSEITS WIRD DAS WERK ANDEREN ÖFFENTLICH ZUGÄNGLICH GEMACHT, ANDERSEITS DURCH DIE ABSPEICHERUNG VON KOPIEN VERVIELFÄLTIGT.**

TAUSCHBÖRSEN
(FILE-SHARING-NETZWERKE)



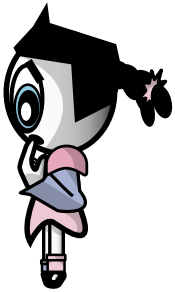
DARF ICH MUSIK ODER VIDEOS AUS DEM INTERNET DOWNLOADEN?

Ob der reine Download von illegal bereitgestellter Musik oder Videos aus dem Internet erlaubt ist, ist unter JuristInnen umstritten. Die einen sehen darin eine erlaubte Vervielfältigung zum privaten Gebrauch, die anderen meinen, auch diese Vervielfältigung zum privaten Gebrauch sei nicht erlaubt, wenn bereits die Vorlage selbst unrechtmäßig hergestellt oder erworben wurde.

EINE EINDEUTIGE ANTWORT AUF DIESE FRAGE IST LEIDER DERZEIT NICHT MÖGLICH, DU BIST ABER AUF DER SICHEREN SEITE, WENN DU ES NICHT TUST.

Der Download ist jedenfalls dann nicht rechtswidrig, wenn dieser von einem dazu Berechtigten angeboten wird. Das kommt allerdings bei gewöhnlichen Tauschbörsen fast nie vor.

Es gibt aber auch Portale, von denen du gegen Bezahlung Musikfiles erwerben kannst. Einzelne Files werden oft als Gratiszugaben oder Kostproben angeboten. Manchmal wird der Download auch durch Werbung finanziert. Bei solchen Musik-Plattformen großer Anbieter kannst du davon ausgehen, dass die Angebote legal sind.

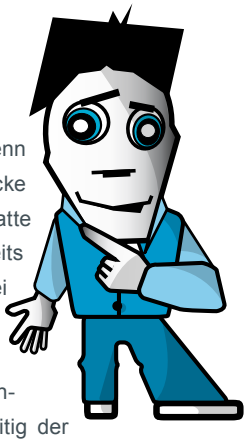


TAUSCHBÖRSEN (FILE-SHARING-NETZWERKE)

DARF ICH MUSIK ODER VIDEOS ZUM DOWNLOAD ANBIETEN?

Hier ist die rechtliche Situation eindeutig: **OHNE ERLAUBNIS DES RECHTEINHABERS ODER DER RECHTEINHABERIN DARF NICHTS ZUM DOWNLOAD ANGEBOTEN WERDEN**.

Besondere Vorsicht ist bei Downloads über BitTorrent oder ähnliche Programme geboten: Sobald du einen Download startest, können andere ebenfalls auf diese Datei zugreifen und diese wiederum von deinem Computer laden. Auch wenn du selbst erst Bruchstücke eines Files auf der Festplatte hast, bist du dadurch bereits Anbieter! Außerdem ist bei den meisten verwendeten Programmen der Ordner, in den die Dateien downgeloadet werden, gleichzeitig der zum Upload freigegebene Ordner. **EIN DOWNLOAD IST DAMIT PRAKTISCH GLEICHBEDEUTEND MIT DER ÖFFENTLICHEN ZURVERFÜGUNGSTELLUNG DERSELBEN DATEI UND SOMIT STRAFBAR**.



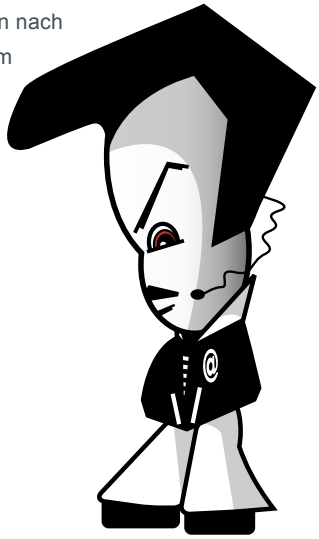
KANN MAN MICH ÜBERHAUPT ERWISCHEN?

Ja, und zwar ganz einfach über die IP-Adresse deines Computers und den Zeitpunkt, zu dem du mit dem Programm online warst. Die Zahl der Abmahnungen und Klagen wegen Anbietens urheberrechtlich geschützter Werke hat auch in Österreich massiv zugenommen. Meistens enden diese Verfahren mit einem Vergleich, der die Zahlung einiger tausend Euro beinhaltet. File-Sharing kann also ein ziemlich teures Vergnügen werden!

TAUSCHBÖRSEN
(FILE-SHARING-NETZWERKE)

WAS GILT BEIM DOWNLOAD VON PROGRAMMEN?

Auch Software ist, wie gesagt, urheberrechtlich geschützt. Für Software ist allerdings nicht einmal eine Vervielfältigung zum Eigengebrauch gestattet. **EIN DOWNLOAD OHNE ZUSTIMMUNG DES/DER URHEBERS/URHEBERIN ODER EINES/EINER NUTZUNGSBERECHTIGTEN – BEI TAUSCHBÖRSEN WOHL DER REGELFALL – IST SOMIT JEDENFALLS ILLEGAL**. Stellt der/ die UrheberIn oder ein/e Nutzungsberechtigte/r selbst ein Programm als Freeware zur Verfügung, ist der Download erlaubt. Oft besteht die Möglichkeit, sich Demoversionen von Programmen von der Website des/der UrheberIn downzuloaden, die man nach einiger Zeit (z.B. 30 Tage) bezahlen oder – wenn dies nicht passiert – vom Computer löschen muss. Das Besorgen von Entsperrcodes für solche Demoversionen (in einschlägigen Foren) ist natürlich auch illegal.



ICH IM NETZ

MEINE HOMEPAGE, MEIN BLOG, MEINE PROFILSEITE

Viele Jugendliche haben heutzutage eine private Homepage, ein Blog (das ist eine Art „Online-Tagebuch“) oder eine Profilseite in einer Online-Community (z.B. Facebook, schülerVZ, Netlog), auf der/dem sie sich selbst darstellen und der Internetgemeinde präsentieren. Varianten gibt es viele. Möglichkeiten, in Schwierigkeiten zu geraten, auch.

DARF ICH BILDER ODER MUSIK AUF MEINER HOMEPAGE / MEINEM BLOG / MEINER PROFILSEITE VERWENDEN?

Du machst eine eigene Website oder Profilseite, wofür du der Einfachheit halber diverse Bilder im Internet zusammensuchst und eine gerippte Musikdatei von einer CD für das Intro verwendest. Ist das erlaubt?

Auch Fotos und Grafiken sind wie Musikstücke, Videos und Programme urheberrechtlich geschützt. Wenn du ein fremdes Foto auf deine Website stellen willst, kannst du dies daher nur mit Zustimmung des/der HerstellerIn (und zwar nur dann!) tun.

Es ist also keine gute Idee, ein x-beliebiges Bild eines bekannten Stars auf deine Homepage, dein Blog oder deine Profilseite zu stellen, auch keinen Cartoon von Bart Simpson. Allerdings gibt es von bekannten Persönlichkeiten oder Fernsehserien meistens Pressefotos, die zur Veröffentlichung freigegeben wurden. Diese findest du oft auf den offiziellen Websites. Bitte beachte aber die dortigen Hinweise, z.B. über die Nennung des Fotografen/der Fotografin in einer Bildunterschrift (sollte man ohnehin immer tun, gehört zum guten Ton).

Sehr riskant ist es, Musikstücke zum Downloaden auf die eigene Website zu stellen oder dort abspielen zu lassen. Ein Verstoß gegen das Urheberrecht besteht schon dann, wenn jedem das Musikstück unabhängig von Zeit oder Ort zugänglich ist. Willst du ein bestimmtes Musikstück trotzdem verwenden, kannst du dich zum Erwerb der nötigen Rechte an die AKM (Gesellschaft der Autoren, Komponisten, Musikverleger) wenden: www.akm.or.at. Diese sorgt für die Wahrnehmung von Urheberrechten im Bereich der öffentlichen Zurverfügungstellung, Aufführung und Sendung von Musik.

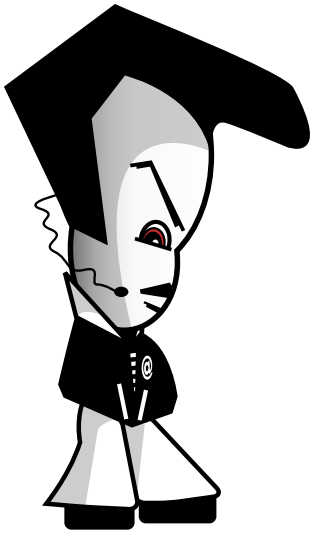
Eine Ausnahme stellen Bilder, Musikstücke oder Videos mit einer so genannten **„CREATIVE COMMONS-LIZENZ“** dar. So gekennzeichnete Werke dürfen unter bestimmten Bedingungen, wie z.B. Nennung des Urhebers/der Urheberin, auf der eigenen Homepage, Blog oder Profilseite frei verwendet werden. Mehr dazu im Kapitel „Quellen überprüfen und angeben“ auf Seite 64.

ICH IM NETZ

DARF ICH SELBST GESCHOSSENE FOTOS VON ANDEREN PERSONEN AUF MEINE HOMEPAGE/MEIN BLOG/MEINE PROFILSEITE STELLEN?

Du machst auf einer Party zu fortgeschrittener Stunde Fotos von verschiedenen betrunkenen BesucherInnen 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.

Bei der Veröffentlichung von Bildern anderer Personen ist immer das **„RECHT AM EIGENEN BILD“** zu beachten:
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 nachteilig ist (z.B. Aufnahme einer schwänzenden Klassenkollegin am Vormittag in der Stadt oder Oben-ohne-Abbildung am Strand), heißt es: Finger weg von der Veröffentlichung! Im privaten Bereich sind Interessen noch viel früher beeinträchtigt, dies gilt auch für private geschlossene Veranstaltungen (z.B. Partys bei dir oder bei FreundInnen). Veröffentlichte Fotos dürfen die Abgebildeten nicht „bloßstellen“ oder „herabsetzen“, dies kann bei Bildern von Party-Exzessen 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).



Wenn du Bilder veröffentlichen willst, frage am besten immer bei den abgebildeten Personen nach, ob sie damit einverstanden sind – das erspart dir in jedem Fall Schwierigkeiten!

ICH IM NETZ

WAS TUN, WENN ICH EIN PEINLICHES FOTO VON MIR IM INTERNET FINDE?

Entdeckst du ein für dich nachteiliges Bild im Internet, so hast du das Recht auf Löschung dieses Bildes, denn auch hier gilt natürlich das „Recht am eigenen Bild“ (siehe vorige Seite). Am besten du kontaktierst die Person oder das Unternehmen, das dein Bild veröffentlicht hat, und bittest um Entfernung. Sollte dies nichts nützen, kannst du mit einer Unterlassungsklage und Schadenersatzforderungen drohen.

DARF ICH AUF ILLEGALE SEITEN LINKEN?

Setzt du einen Link auf eine fremde, rechtsverletzende Website, bist du nicht für diese fremde Website mitverantwortlich, wenn dir die Rechtswidrigkeit der Seite nicht aufgefallen ist (z.B. wenn Fotos ohne Erlaubnis der Abgebildeten auf der Seite veröffentlicht wurden). Bemerkst du aber, dass du einen Link auf eine illegale Website (z.B. Kinderpornografie) gesetzt hast, und willst nicht mitverantwortlich sein, musst du den Link sofort entfernen. Der bloße Hinweis, dass du für fremde Inhalte nicht haftest, nützt dir nichts, wenn du bewusst illegale Inhalte zugänglich machst. Es ist also immer gut, sich eine Seite genauer anzusehen, bevor man einen Link dorthin legt. **WENN DIR JEMAND SAGT, DASS DIE VON DIR VERLINKTE SEITE ILLEGALE INHALTE VERBREITET (Z.B. NEONAZI-PROPAGANDA), DANN MUSST DU DEN LINK SOFORT LÖSCHEN!**

Auch wenn man auf deiner Website oder in deinem Blog Kommentare (z.B. in einem Gästebuch) posten kann, bist du für den Inhalt (und somit auch für angegebene Links) verantwortlich, wenn du die Beiträge nicht so rasch wie möglich entfernst.

ICH IM NETZ

WELCHE ANGABEN MUSS ICH AUF MEINER HOMEPAGE/MEINEM BLOG MACHEN?

Auch für private Homepages oder Blogs besteht in Österreich seit 1.7.2005 eine sogenannte „Offenlegungspflicht“ nach dem Mediengesetz. Danach musst du deinen **NAMEN UND WOHNORT** (nicht aber die genaue Adresse) ständig und leicht auffindbar auf der Site zur Verfügung stellen.

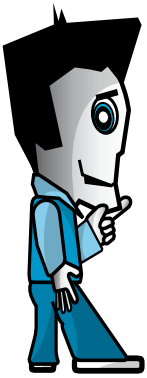
Sollte deine Homepage oder dein Blog, auf der du dich selbst darstellst und deinen persönlichen Lebensbereich präsentierst, außerdem noch z.B. politische oder sonstige Artikel enthalten, die die Meinung anderer beeinflussen, musst du zusätzlich noch die „grundlegende Richtung“ deiner Homepage angeben (also z.B. Berichte und Infos über das Thema XY).

DAS FEHLEN DIESER ANGABEN KANN DICH BIS ZU EUR 2.180,- KOSTEN.

SOBALD DU MIT DEINER HOMEPAGE ODER DEINEM BLOG ZUM BEISPIEL GELD VERDIENST, MUSS DER/DIE INHABER/IN EIN LEICHT SICHTBARES IMPRESSUM MIT DEN WICHTIGSTEN KONTAKTINFORMATIONEN VERÖFFENTLICHEN.

Es genügt schon, auf der Homepage oder dem Blog für eigene Produkte zu werben. Bewirbst du z.B. Waren oder Dienstleistungen, die du selber anbietest, sind diese Kontaktinformationen (hier nach dem E-Commerce-Gesetz) in einem „Impressum“ unerlässlich. Das Fehlen der vorgeschriebenen Angaben kann dich bis zu EUR 3.000,- kosten.

EIN IMPRESSUM MUSS DANN FOLGENDE INFOS ÜBER DEN / DIE INHABER / IN DER WEBSITE ENTHALTEN:



+ Name(n) oder Firma;
+ die genaue Adresse (Postfach reicht nicht);
+ Kontaktdaten, vor allem E-Mail-Adresse (die österreichischen Gerichte verlangen jedenfalls auch Telefon- oder Faxnummer).

Die sonst noch vorgeschriebenen Angaben werden dich kaum betreffen. Unternehmen müssen diese Angaben zum Beispiel machen, dies ist ein Zeichen für die Seriosität des/der InhaberIn einer Website:

+ Firmenbuchnummer und Firmenbuchgericht
+ Umsatzsteuer-Identifikationsnummer

Es müssen weiters die zuständige Aufsichtsbehörde und die Zugehörigkeit zu einer Kammer oder einem Berufsverband angegeben werden.

ICH IM NETZ

DIE OBERSTE REGEL IM WEB: GIB NICHT ZU VIEL VON DIR PREIS!

Ganz klar, Online-Communitys (wie z.B. Facebook, Netlog, schülerVZ) sind eine tolle Sache: Nirgendwo sonst kann man so einfach Kontakte pflegen, sich selbst im Netz präsentieren, neue Leute kennenlernen und Fotos und Videos austauschen. Andererseits: Hast du dir schon mal Gedanken darüber gemacht, was bösartige Menschen mit deinen persönlichen Infos so alles anstellen könnten? Belästigungen im Web (siehe dazu auch Kapitel „Cyber-Mobbing“ ab S. 40) sind dabei nur eine von vielen Möglichkeiten, mit nur einer Handvoll Daten kannst du heutzutage ganz einfach auch im „echten“ Leben aufgespürt werden… Bevor du etwas Privates von dir im Web veröffentlichst, frage dich daher erst mal: Würde ich dasselbe auch einem fremden Spaziergänger im Park erzählen, oder meinem unbekannten Gegenüber im Zug?

WARUM IST ES WICHTIG, PERSÖNLICHE DATEN IM INTERNET ZU SCHÜTZEN?

Viele InternetnutzerInnen sind sich gar nicht über die möglichen Konsequenzen der Preisgabe persönlicher, auf den ersten Blick vielleicht „harmloser“, Daten bewusst. Hier findest du einige gute Gründe, warum es sich lohnt, vorsichtig mit deiner Privatsphäre umzugehen:

- **Im Web ist man nicht so anonym, wie man glaubt:** Alle Inhalte, die du ins Netz stellst, sind nicht nur für deine FreundInnen zugänglich, sondern theoretisch auch für alle anderen InternetnutzerInnen auf der Welt! Auch dir unbekannte oder weniger gut gesonnene Menschen können deine privaten Informationen also unter Umständen einsehen und für böse Absichten missbrauchen.

ICH IM NETZ

√ **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.

√ **Der erste Eindruck zählt:** Communitys und andere Internetplattformen werden von LehrerInnen, potenziellen ArbeitgeberInnen, MitschülerInnen, Bekannten etc. genutzt, um mehr über dich zu erfahren. Glaubst du, dass sie mithilfe deiner Online-Angaben zu Interessen, Hobbys, Vorlieben, Freunden, Einstellungen etc. ein von dir erwünschtes Bild von deiner Person vermittelt bekommen?

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

WIE SCHÜTZE ICH MICH UND MEINE DATEN IN COMMUNITYS?

Beachte beim Umgang in Online-Communitys folgende Punkte, damit du später keine Probleme bekommst:

√ Gib keine persönlichen Daten (voller Name, Adresse, Wohnort, Telefonnummer etc.) bekannt, die es Fremden ermöglichen, dich auch im „echten" Leben aufzuspüren oder zu belästigen.

√ Veröffentliche keine Bilder oder Texte, die dir oder anderen später einmal peinlich sein oder zu deinem Nachteil verwendet werden könnten. Bedenke, dass du keine Bilder von deinen FreundInnen veröffentlichen darfst, die diese „nachteilig" darstellen. Auch wenn Bilder nur für kleinere NutzerInnengruppen freigegeben sind, kannst du nicht ausschließen, dass sie irgendwann in falsche Hände geraten.

√ Nutze die Einstellungsoptionen deiner Community für mehr „Privatsphäre", z.B. indem du den Zugriff auf dein Profil und deine Inhalte nur auf „Freunde" beschränkst.

ICH IM NETZ

- Verwende sichere Passwörter (z.B. eine Kombination aus Buchstaben und Zahlen) und halte diese geheim. Gestohlene Login-Daten können dazu verwendet werden, um dein Profil zu verändern oder zu missbrauchen. Wähle auch stets verschiedene Passwörter für verschiedene Websites und ändere diese regelmäßig. Tipps zur Gestaltung sicherer Passwörter findest du im Kapitel „Computersicherheit & Passwörter“ auf Seite 25.

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

- In manchen Communitys kann es auch vorkommen, dass Schadprogramme verbreitet werden. Sei daher vorsichtig, wenn du Programme erhältst. Speichere diese nicht auf deinem Computer oder verwende zumindest ein regelmäßig aktualisiertes Anti-Viren-Programm.

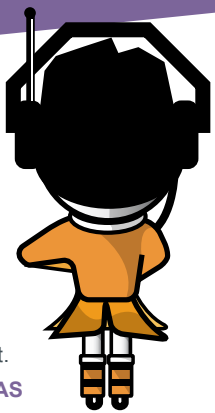
- Sollten dich NutzerInnen in einer Community belästigen, so kannst du sie in der Regel sperren lassen. Kontaktiere den/die BetreiberIn der Seite, falls die unerwünschte Kontaktaufnahme nicht aufhört.

ICH HÄNGE STÄNDIG IM NETZ – KANN MIR DAS SCHADEN?

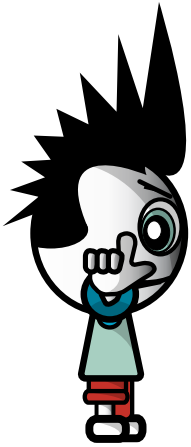
Die Antwort darauf ist: **JEIN!** Tägliches Surfen alleine ist natürlich nicht gefährlich – wenn folgende Aussagen allerdings überwiegend auf dich zutreffen, solltest du deine Internetnutzung eventuell überdenken:

+ Meine Gedanken kreisen ständig um das Internet, auch wenn ich „offline“ bin.
+ Zu meinen „realen“ FreundInnen habe ich kaum noch Kontakt, ich habe hauptsächlich Online-FreundInnen.
+ Selbst wenn ich will, kann ich mich nur ganz schwer von meinem Computer losreißen.
+ Ich habe ständig Angst, im Netz etwas zu verpassen.
+ Wenn ich traurig oder schlecht drauf bin, ist das Internet mein „Seelentröster“.
+ Mit meinen Eltern gibt es andauernd Streit wegen meiner Computernutzung.
+ In der Schule / Ausbildung / Arbeit bin ich nicht mehr so aufmerksam und so gut wie früher.
+ Ich gehe in meiner Freizeit kaum mehr raus, ich bin viel lieber im Netz unterwegs.
+ Wenn ich nicht an meinen Computer kann, bin ich unruhig und gereizt.

ICH IM NETZ

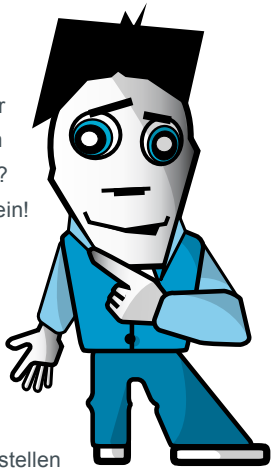


Ob du zur Online- bzw. Computer-Sucht neigst, kannst du auch mit diesem Selbsttest unter www.psychotherapiepraxis.at/surveys/test_internet-sucht.phtml überprüfen. Oder du probierst mal einen Tag – oder noch besser – eine ganze Woche auf das Internet zu verzichten: Wenn dir der Verzicht nicht besonders schwer fällt, bist du wohl eher nicht gefährdet. Merkst du aber, dass du nur an den Computer denken kannst, unruhig wirst und etwas sehr stark vermisst, solltest du gegensteuern, bevor es zu spät ist. Denn „Sucht" ist eine echte Krankheit – **UND WER WILL SCHON, DASS DAS EIGENE LEBEN VON EINEM COMPUTER BESTIMMT WIRD?!**



Während Mädchen eher von Chats und Foren fasziniert sind, schenken Burschen oft stundenlang Computerspielen ihre Aufmerksamkeit. In beiden Fällen gilt: **ÜBERTREIB EINFACH NICHT UND VERSUCHE, ANDERE FREIZEITAKTIVITÄTEN, DIE NICHTS MIT DER ONLINE- ODER GAMING-WELT ZU TUN HABEN, ZU VERSTÄRKEN UND ZU FÖRDERN!** Überlege dir immer, was du sonst noch unternehmen und machen könntest, anstatt dich an den Computer zu setzen. Rede doch einmal mit deinen FreundInnen – eine Party, ein Konzert, ein Sportplatz, ein Billardtisch, ein Berg, irgendetwas ist immer in der Nähe. Oder probiere einmal etwas ganz anderes mit deiner Clique aus! Wenn du Hilfe brauchst, sprich mit einem Erwachsenen, dem du vertraust, oder wende dich an eine professionelle Suchtberatungsstelle. Adressen und Links dazu findest du im Kapitel „Wer hilft mir weiter?" ab Seite 68.

BELÄSTIGUNG & CYBER-MOBBING



Hat jemand schon einmal über dich im Internet Lügen verbreitet oder peinliche Fotos in eine Community gestellt? Das Passwort von deinem E-Mail-Postfach geknackt und in deinem Namen böse E-Mails verschickt? Oder dich per Messenger beschimpft? Das kann ziemlich unangenehm sein! Hier erfährst du, was du dagegen tun kannst.

WAS IST CYBER-MOBBING?

Unter „Cyber-Mobbing“ (auch „Cyber-Bullying“ oder „Cyber-Stalking“ genannt) versteht man das absichtliche Beleidigen, Bedrohen, Bloßstellen oder Belästigen von Personen im Internet oder über das Handy und das über einen längeren Zeitraum hinweg. Personen, die andere schikanieren, verwenden dabei unterschiedlichste Internet- und Handydienste wie z.B. im Internet: E-Mails, Instant Messenger, Chatrooms, Online-Communitys, Foto- oder Videoportale bzw. am Handy: SMS, lästige Anrufe oder die Handykamera.

BESONDERHEITEN VON CYBER-MOBBING:

+ Inhalte im Internet verbreiten sich rasch und an ein großes Publikum. Einmal Eingestelltes ist oft nicht mehr zu entfernen.
+ Cyber-Mobbing endet nicht mit Schul- oder Arbeitsschluss und macht auch vor den eigenen vier Wänden nicht Halt – es sei denn, du nutzt in deiner Freizeit kein Handy oder Internet…
+ Menschen, die andere online mobben, tun dies oft (scheinbar) anonym. Deshalb sinkt bei den TäterInnen die Hemmschwelle, weil sie den Opfern nicht in die Augen sehen müssen. Über Konsequenzen wird meist kaum nachgedacht – auch nicht über die rechtlichen.

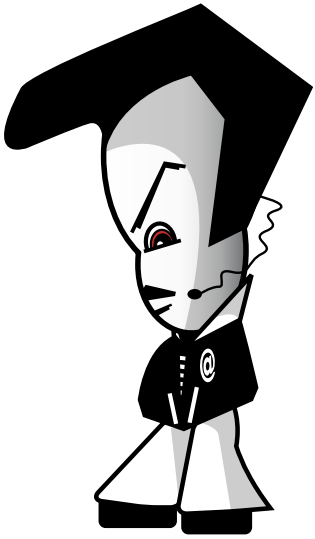
BELÄSTIGUNG & CYBER-MOBBING

WAS SAGT DAS GESETZ?

Für Mobbing gibt es keine Rechtfertigung und es ist kein Kavaliersdelikt. **MOBBING ÜBER DAS INTERNET KANN STRAFBAR SEIN!** Dazu gibt es eine Reihe an gesetzlichen Bestimmungen, zum Beispiel:

Stalking (also das beharrliche Verfolgen von Opfern, § 107a StGB) ist seit 2006 in Österreich strafbar – das gilt auch für die „virtuelle" Welt. Aber auch durch üble Postings in Online-Foren oder -Communitys, die den Tatbestand der **Beleidigung**, der **Üblen Nachrede** oder der **Verleumdung** erfüllen, kann man sich strafbar machen. Mehr Infos dazu findest du im Kapitel „DOs & DONT's" ab Seite 8. Es besteht gesetzlich auch ein **Recht auf Wahrung der Privatsphäre**. Dieses Recht verbietet die Veröffentlichung und Verwertung von privaten Informationen. Ein Schadenersatz ist hier insbesondere für bloßstellende Veröffentlichungen vorgesehen. Auch Briefe, Tagebücher und andere vertrauliche Aufzeichnungen dürfen ohne Zustimmung des Verfassers/der Verfasserin nicht veröffentlicht werden.

Bis zum 14. Geburtstag gilt man als unmündige/r Minderjährige/r und ist damit nicht strafbar, selbst wenn man gegen ein Gesetz verstößt. Ab 14 Jahren bis zur Volljährigkeit kommt betreffend des Strafausmaßes das Jugendstrafrecht zur Anwendung. Jedoch können Eltern in jedem Fall schadenersatzpflichtig werden, wenn sie ihre Aufsichtspflicht verletzt haben!



BELÄSTIGUNG & CYBER-MOBBING

10 TIPPS – SO WEHRST DU DICH GEGEN CYBER-MOBBING:

1. Bleib ruhig! Lass dich nicht von Selbstzweifeln beherrschen. Denn: Du bist okay, so wie du bist – an dir ist nichts falsch.

2. Sperre die, die dich belästigen! Die meisten Websites und Online-Anbieter geben dir die Möglichkeit, bestimmte Personen zu sperren. Blockierte NutzerInnen können dann nicht mehr auf dein Profil zugreifen und dir auch keine Nachrichten schicken. Die Einstellungsoptionen dafür findest du normalerweise im eigenen Profil bzw. im Profil der/des entsprechenden UserIn oder in den Einstellungen zur „Privatsphäre". Nutze dieses Angebot, denn du musst dich nicht mit jemandem abgeben, der dich belästigt. Wenn du mit Anrufen oder SMS belästigt wirst, kannst du auch deine Handynummer ändern lassen.

3. Antworte nicht! Reagiere nicht auf Nachrichten, die dich belästigen oder ärgern. Denn genau das will der/die AbsenderIn. Wenn du zurückschreibst, wird das Mobbing wahrscheinlich nur noch schlimmer.

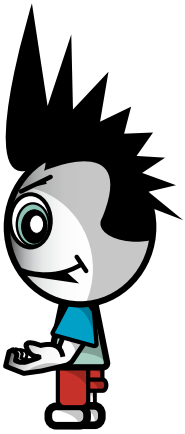
4. Sichere Beweise! Lerne, wie du Kopien von unangenehmen Nachrichten, Bildern oder Online-Gesprächen machen kannst. Sie werden dir helfen, anderen zu zeigen, was passiert ist. Außerdem kann mit den Beweisen auch dein/e PeinigerIn gefunden werden.

5. Rede darüber! Wenn du Probleme hast, wende dich an Erwachsene, denen du vertraust, z.B. deine Eltern, eine/n LehrerIn oder eine JugendbetreuerIn. Bei „147 – Rat auf Draht" (www.rataufdraht.at) erhältst du kostenlos, anonym und rund um die Uhr telefonische Hilfe, wenn du einmal nicht mehr weiter weißt. Weitere Beratungsstellen findest du im Kapitel „Wer hilft mir weiter?" ab Seite 68.

6. Melde Probleme! Nimm Belästigungen nicht einfach hin, sondern informiere umgehend die BetreiberInnen der Website. Informationen, wie du in den verschiedenen Sozialen Netzwerken Missbrauch melden kannst, findest du auf der Saferinternet.at-Website unter „Soziale Netzwerke". Vorfälle, die illegal sein könnten, solltest du den Behörden melden.

7. Unterstütze Opfer! Wenn du mitbekommst, dass jemand anderer per Handy, Internet oder SMS belästigt wird, dann schau nicht weg, sondern hilf ihm/ihr und melde den Vorfall. Wenn der/die TäterIn merkt, dass das Opfer nicht alleine gelassen wird, hören die Beleidigungen oft schnell auf.

BELÄSTIGUNG & CYBER-MOBBING



8. Schütze deine Privatsphäre!

Sei vorsichtig, welche Angaben du im Internet machst. Deine persönlichen Daten (E-Mail-Adresse, Wohnadresse, Handynummer oder private Fotos) können auch von „Cyber-Bullys" gegen dich verwendet werden. Achte insbesondere darauf, deine Zugangsdaten geheim zu halten und ein sicheres Passwort zu verwenden (siehe Kapitel „Computersicherheit & Passwörter" ab Seite 23).

9. Kenne deine Rechte!

Wenn du es nicht erlaubst, darf niemand Fotos von dir ins Internet stellen, die dir peinlich sein könnten. Außerdem darf dich niemand vor anderen verspotten oder beleidigen. Wenn Cyber-Mobbing besonders ernst ist, kann dies für den/die TäterIn rechtliche Konsequenzen haben.

10. Vertraue dir!

Wichtig ist, dass du an dich selbst glaubst und dir nichts von anderen einreden lässt. Lass dich nicht fertigmachen und mach keine anderen fertig!

GROOMING

Beim so genannten „Grooming" versuchen sich Erwachsene aus sexuellem Interesse gezielt mit Kindern und Jugendlichen „anzufreunden". Menschen mit dieser Neigung werden im allgemeinen Sprachgebrauch als „pädophil" bezeichnet. Sie gehen dabei sehr geschickt vor und geben sich in Chats, Foren und Online-Communitys oft als gleichaltrig aus. So versuchen sie sich, das Vertrauen der Minderjährigen zu erschleichen und ihnen möglichst viele Informationen über Wohnort, Interessen, Schule etc. zu entlocken. Oft schicken Pädophile auch anzügliche Fotos (sowohl von Erwachsenen als auch von Kindern) und bezeichnen das als „normal" – aber normal ist das sicher nicht! Ziel dieser Menschen sind meist ganz klar „reale" Treffen mit ihren Opfern und dabei möchten sie sicher nicht nur auf ein Eis gehen… **TRIFF DICH DAHER NIE ALLEINE MIT FREMDEN INTERNET-BEKANNTSCHAFTEN, SONDERN NUR IN BEGLEITUNG EINES ERWACHSENEN, DEM DU VERTRAUST. WENN DIR ETWAS KOMISCH VORKOMMT, BEENDE AM BESTEN SOFORT DEN KONTAKT!**

SHOPPING IM NETZ

Ob CDs, Computer, MP3-Player oder Bücher: Einkaufen im Internet wird immer beliebter. Wir sagen dir hier, worauf du dabei achten solltest:

WELCHE GESCHÄFTE DARFST DU ALLEINE ABSCHLIESSEN?

Bis zu deinem 18. Geburtstag kannst du nur beschränkt Geschäfte ohne Zustimmung eines Elternteils abschließen. Entscheidend für das Ausmaß der Beschränkung sind das Alter und das Geschäft:

7–13 JAHRE:

Jugendliche dürfen bis zu ihrem 14. Geburtstag nur kleine alltägliche Geschäfte alleine abschließen, z.B. Kaugummis oder eine Musikzeitschrift kaufen. Geschäfte über das Internet sind aber wohl nie als alltäglich anzusehen, daher benötigst du dafür immer die Zustimmung eines Elternteils bzw. Erziehungsberechtigten!

14–17 JAHRE:

Zwischen ihrem 14. und 18. Geburtstag dürfen Jugendliche ihr eigenes Einkommen (sofern vorhanden) bzw. ihr Taschengeld prinzipiell nach eigenem Ermessen ausgeben.

Wenn du also über das Internet CDs oder Bücher bestellst, die du von deinem Taschengeld bezahlst, kommen diese Geschäfte wirksam zustande, ohne dass deine Eltern zustimmen müssen.

Sobald Geschäfte aber deinen Lebensunterhalt gefährden, müssen sie von einem Elternteil genehmigt werden.

SHOPPING IM NETZ

1. SCHAUEN KOSTET NICHTS

Bevor du etwas bestellst, solltest du dir ein Bild davon machen, was genau du möchtest, was es wo kostet und welche Spesen zusätzlich zum Preis zu bezahlen sind (z.B. Versandkosten). Suchmaschinen sowie Preisvergleichs- und Testbericht-Sites (z.B. Ciao, Dooyoo oder Geizhals) können ein guter Ausgangspunkt für Recherchen sein.

2. BEI WEM SOLL ICH BESTELLEN?

Abgesehen vom Preis des Produktes gibt es noch andere Faktoren, die du beachten solltest:

- √ Lies die **ALLGEMEINEN GESCHÄFTSBEDINGUNGEN** des Händlers (siehe nächste Seite).
- √ **FAUSTREGEL:** Bei ausländischen Unternehmen ist es schwieriger, sich zu beschweren oder zu reklamieren. Händlern innerhalb Österreichs solltest du daher den Vorzug geben, bei Bestellungen in anderen EU-Mitgliedstaaten kann es schon komplizierter werden, ist aber immer noch relativ sicher. Bei Händlern außerhalb der EU solltest du nur bestellen, wenn diese sehr bekannt sind oder du das Produkt nur dort bekommst.
- √ **LIES BERICHTE ÜBER DEN HÄNDLER** z.B. in den Groups auf Google, Yahoo! oder Geizhals oder mittels Websuche nach dem Händlernamen. Man soll zwar nicht alles glauben, was im Internet geschrieben wird, aber generelle Anhaltspunkte über die Seriosität eines Händlers lassen sich doch fast immer finden.
- √ **BEACHTE DIE ZAHLUNGSMODALITÄTEN:** Grundsätzlich ist das Bezahlen im Netz besser als sein Ruf. Mittlerweile werden verschiedenste Zahlungsmittel angeboten: von Kreditkarten über Prepaid-Karten (z.B. „paysafecard“), Bezahlen mit dem Handy (z.B. „paybox“) und der „eps Online-Überweisung“ bis hin zu „PayPal“ und „ClickandBuy“. Jedes Zahlungsmittel ist aber prinzipiell nur so sicher, wie du es verwendest (Tipps dazu siehe auf Seite 47)! Komplett abzuraten ist von Vorauskasse-Zahlungen mit Banküberweisung: Hier liefert der Anbieter

SHOPPING IM NETZ

die Bestellung erst NACHDEM du den Geldbetrag überwiesen hast. Sollte ein unseriöser Händler nicht liefern, ist dein Geld in der Regel verloren. Bei der Lieferung per Nachnahme wiederum bezahlst du erst, wenn du das Paket schon in Händen hältst. Allerdings kannst du nicht sofort kontrollieren, ob sich im Paket tatsächlich die gewünschte Bestellung befindet. Außerdem ist die Lieferung per Nachnahme meist mit Zusatzkosten verbunden.

√ **BEACHTE ALLFÄLLIGE GÜTEZEICHEN** auf der Website des Verkäufers. Allerdings ist nicht jedes Gütezeichen gleich viel wert. Auf der Website des „Österreichischen E-Commerce Gütezeichen“ (www.guetezeichen.at) findest du Informationen zu Shops, die vertrauenswürdig sind.

WAS SIND ALLGEMEINE GESCHÄFTSBEDINGUNGEN?

Du bestellst einen Computer über das Internet. Der Händler baut diesen falsch zusammen, weswegen dieser nach einer Woche explodiert. Du wirst verletzt und möchtest Schmerzensgeld. Der Verkäufer verweist auf seine Allgemeinen Geschäftsbedingungen, wonach jede Haftung für Schäden an Personen ausgeschlossen ist.

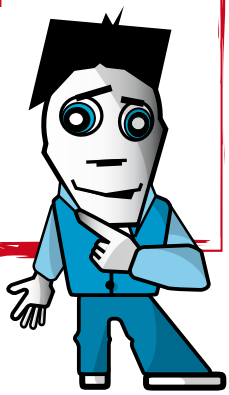
ALLGEMEINE GESCHÄFTSBEDINGUNGEN (AGB) SIND STANDARDVERTRÄGE, DIE UNTERNEHMEN ALL IHREN GESCHÄFTEN ZUGRUNDE LEGEN.

Die Anwendung von AGB auf eine bestimmte Bestellung muss zuvor zwischen Unternehmen und Kunden vereinbart werden. Dafür reicht es, dass der Unternehmer deutlich zu erkennen gibt, dass seine AGB angewendet werden sollen und man die AGB vor der Bestellung lesen und speichern kann. Das ist der Fall, wenn es auf der Seite mit dem Bestellformular den Link „AGB“ gibt, der die Seite mit den Allgemeinen Geschäftsbedingungen öffnet. Wer AGB verwendet, möchte sich natürlich möglichst umfangreich gegen alle denkbaren Ansprüche absichern. Besonders nachteilige Bestimmungen in AGB können ungültig sein. Eine solche ungültige Bestimmung ist nach dem Konsumentenschutzgesetz z.B. der Ausschluss der Haftung für Schäden an Personen. Eine AGB-Bestimmung wie im Beispiel oben hindert deshalb die Geltendmachung von Schadenersatz wegen einer Körperverletzung nicht.

SHOPPING IM NETZ

TIPPS ZUR SICHEREN VERWENDUNG VON ZAHLUNGSMITTELN IM INTERNET:

+ Nutze stets alle Sicherheitseinstellungen, die dir zur Verfügung stehen – auch freiwillige (z.B. Auswahl eines Passworts oder PIN-Codes).
+ Bewahre Zahlungsinformationen wie Kundenkennung, Passwörter, Codes etc. immer sicher und getrennt voneinander auf. Besser du lernst sie auswendig!
+ Kontrolliere regelmäßig deine Kontoauszüge bzw. Transaktionsliste.
+ Gib sensible Daten im Internet generell nur über verschlüsselte Verbindungen ein – solche erkennst du an einer mit „https://“ beginnenden Webadresse und einem Vorhängeschloss-Symbol unten auf dem Bildschirm.
+ Verwende sichere Passwörter. Tipps dazu findest du im Kapitel „Computersicherheit & Passwörter“ auf Seite 25.
+ Informiere dich vor Verwendung über die technische Funktionsweise des Zahlungsmittels. Nur so kannst du mögliche Risiken beurteilen.
+ Informiere dich vorab auch darüber, wie das Zahlungsmittel bei Verlust oder Diebstahl im Ernstfall rasch gesperrt werden kann und ob dich das etwas kostet.
+ Vorsicht bei Phishing: Zahlungsmittelbetreiber fragen ihre Kunden niemals per E-Mail nach persönlichen Zahlungsinformationen!
+ Schütze deinen Computer vor ungewollten Zugriffen von außen, indem du ein Anti-Viren-Programm und eine Firewall installierst und deine Software immer auf dem neusten Stand hältst – am besten per automatischem Update.



SHOPPING IM NETZ

3. ICH HABE ETWAS BESTELLT. MUSS ICH DAS JETZT AUCH KAUFEN?

Auch im Internet kommt ein Vertrag (in diesem Fall zwischen Händler und KonsumentIn) durch ein Angebot und dessen Annahme zustande. Ein von dir ausgefülltes Bestellformular gilt als dein Angebot, etwas zu kaufen. Du bist daran eine gewisse Zeit gebunden (nicht aber der Händler, denn der muss ja dein Angebot erst annehmen!).

NIMMT DER VERKÄUFER DEIN ANGEBOT INNERHALB DIESER BINDUNGSDAUER AN, KOMMT DER VERTRAG ZUSTANDE, DU HAST IN DER REGEL EIN RÜCKTRITTSRECHT (SIEHE PUNKT 4).

Erklärt der Verkäufer hingegen, er könne die Ware erst wieder in einem Monat und/oder um einen höheren Preis liefern, hast du mangels Vertrag zwar keinen Anspruch auf den geringeren Preis, du hast aber die Wahl, sein neues Angebot anzunehmen oder auch nicht.

Andererseits muss aber für den Abschluss eines Vertrags nicht einmal eine ausdrückliche Erklärung erfolgen. Es gilt das Prinzip der Formfreiheit. Bestellst du etwas im Internet und wird die Sache sofort und ohne weitere Erklärung geliefert, kommt der Vertrag durch diese Lieferung zustande. Hat die Sache einen Mangel, kannst du nicht einfach sagen, es ist kein Vertrag zustande gekommen, sondern musst den Mangel als Gewährleistung geltend machen. Dazu aber weiter hinten.

SHOPPING IM NETZ

4. ICH HABE ETWAS BESTELLT UND ES MIR ANDERS ÜBERLEGT. KANN ICH DAVON ZURÜCKTRETEN?

Du hast einen DVD-Brenner bestellt und überweist den Kaufpreis sofort. Zwei Tage später liest du in einer Zeitschrift einen Bericht über DVD-Brenner: Der bestellte Brenner landet im Test klar auf dem letzten Platz. Du bist schockiert und möchtest alles rückgängig machen. Was tun? Wenn du etwas über das Internet oder via E-Mail bestellst, hast du aufgrund des Konsumentenschutzgesetzes ein Rücktrittsrecht. Du hast ab dem Zeitpunkt der Lieferung der Ware (bei Dienstleistungen ab Vertragsabschluss) sieben Werktage Zeit, vom Vertrag zurückzutreten. Samstage, Sonn- und Feiertage zählen nicht als Werktage. Die Rücktrittserklärung musst du innerhalb dieser Frist absenden. Es ist daher optimal, wenn du eine Bestätigung über den Sendezeitpunkt hast (eingeschriebener Brief oder wenigstens Fax oder E-Mail).

DIE FRIST FÜR DEN RÜCKTRITT KANN SICH VERLÄNGERN, WENN DIR DER VERKÄUFER GEWISSE INFOS NICHT ZUR VERFÜGUNG GESTELLT HAT. DIESE SIND:

+ Name und Anschrift des Verkäufers (eine Postfach-Adresse reicht nicht, dorthin können Gerichte keine Klagen oder Ladungen zustellen),
+ wesentliche Eigenschaften der Ware, Dienstleistung, Lieferkosten (z.B. für Paketdienst),
+ Einzelheiten über Zahlung und Lieferung (wie und wann du zahlen musst, wie und wann geliefert wird),
+ Info über das Rücktrittsrecht,
+ die Kosten für den Einsatz des Kommunikationsmittels (von Bedeutung bei Benutzung von Programmen, die eine teurere Verbindung ins Internet herstellen),
+ wird die Leistung immer wieder erbracht (z.B. bei einem Abo), ist die Mindestlaufzeit mitzuteilen,
+ die Adresse, bei der man Beanstandungen geltend machen kann,
+ Info über Kundendienst und Garantiebedingungen (z.B. Garantie nur bei Inanspruchnahme eines Gratis-Service),
+ bei unbestimmter oder mehr als einjähriger Vertragsdauer, wie und wann man kündigen kann.

Wenn dir der Verkäufer diese Infos erst später gibt, läuft die 7-tägige Frist für den Rücktritt erst ab diesem späteren Zeitpunkt. Stellt der Verkäufer die Infos überhaupt nicht zur Verfügung, kannst du das Rücktrittsrecht innerhalb von drei Monaten ab Lieferung (bei Dienstleistungen ab Vertragsabschluss) geltend machen.

KEIN RÜCKTRITTSRECHT HAST DU BEI …

+ Dienstleistungen, die vereinbarungsgemäß schon vor Ablauf der 7-tägigen Frist begonnen haben (z.B. bereits aktivierter E-Mail-Account),
+ verderblichen Waren (Lebensmittel),
+ versiegelten Videos, CDs, Software, wenn du die Versiegelung (z.B. Plastikhülle) schon entfernt hast,
+ Zeitungen, Zeitschriften und Illustrierten, wohl aber bei Bestellung von Abos,
+ Wett- und Lotteriedienstleistungen,
+ Hauslieferungen (z.B. Fahrtendienste wie Pizza-Zustellung),
+ Freizeitdienstleistungen,
+ Waren, die auf persönliche Bedürfnisse zugeschnitten sind (z.B. ein T-Shirt mit einem Foto von dir).

Für den DVD-Brenner im vorherigen Beispiel hast du also ab der Lieferung sieben Werktage Zeit für einen Rücktritt und bekommst dein Geld zurück.

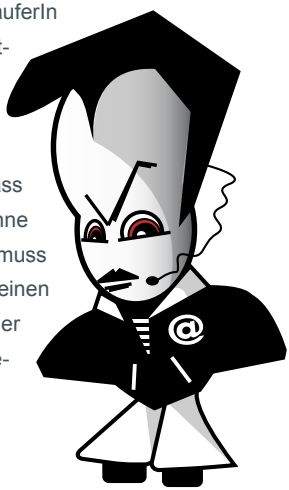
5. WAS TUN, WENN DIE WARE ÜBERHAUPT NICHT GELIEFERT WIRD?

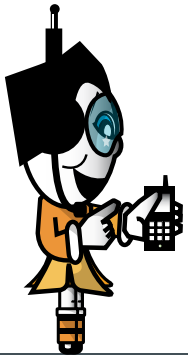
Im Konsumentenschutzgesetz ist geregelt, dass der/die HändlerIn binnen 30 Tagen ab Bestellung liefern muss – es sei denn, er/sie nimmt die Bestellung nicht an, oder es steht z.B. beim Artikel eine längere Lieferzeit. Sollte es dem Unternehmen nicht möglich sein, innerhalb der 30 Tage oder überhaupt zu liefern, muss es dir das mitteilen. Wenn du die Ware noch willst, solltest du dem/der HändlerIn eine schriftliche Nachfrist setzen, innerhalb der er/sie noch liefern kann. Wichtig ist, deutlich zu machen, dass wenn die Ware nicht binnen z.B. 10 Tagen eintrifft, du diese nicht mehr willst. Bei schriftlichen Mitteilungen an Unternehmen ist ein eingeschriebener Brief, bei dem man eine Kopie und den Aufgabeschein aufbewahrt, das sicherste und beweiskräftigste Mittel.

SHOPPING IM NETZ

6. WAS TUN, WENN DIE BESTELLTE WARE FEHLERHAFT IST?

Nicht ganz korrekt wird in diesem Zusammenhang oft der Begriff „Garantie“ verwendet. Bei einer Garantie – die ausdrücklich vereinbart werden muss – verpflichtet sich der/die HerstellerIn selbst, jeden Mangel zu beheben, auch wenn der Mangel erst nach der Übergabe der Ware entsteht. Normalerweise hat man aber keine Garantie-, sondern nur Gewährleistungsansprüche. Gewährleistung steht dem/der KäuferIn gesetzlich zu. Der/die VerkäuferIn muss dafür einstehen, dass die Ware zum Zeitpunkt der Übergabe keinen Mangel hat. Gewährleistung muss man bei beweglichen Sachen innerhalb von zwei Jahren geltend machen.
Was kannst du also tun, wenn du einen PC über das Internet bestellt hast und sich herausstellt, dass der PC beim Hochfahren dauernd abstürzt? Zunächst hast du die Wahl zwischen Verbesserung oder Austausch der Ware. Verbesserung ist der Nachtrag eines fehlenden Teils oder eine Reparatur. Bei einem Online-Kauf sitzt der/die VerkäuferIn meist an einem entfernten Ort. Der/die VerkäuferIn muss in unserem Beispiel dafür sorgen, dass der gelieferte PC ohne Probleme läuft. Er muss daher entweder einen anderen PC liefern oder zumindest den gelieferten PC reparieren.





ACHTUNG!
Wenn du von einer Privatperson kaufst, so kann diese jede Gewährleistung ausschließen. Du hast nur gegenüber Firmen zwingend Gewährleistungsansprüche.
Also Vorsicht bei Bestellungen aufgrund von Kleinanzeigen oder Ähnlichem!

SHOPPING IM NETZ

7. WAS TUN, WENN DER FEHLER NICHT BEHOBEN WIRD?

Erst wenn der/die VerkäuferIn trotz Aufforderung nichts macht oder sein/ihr zweimaliger Verbesserungsversuch fehlschlägt, kannst du eine Herabsetzung des Kaufpreises oder die Rückgängigmachung des Vertrags (Wandlung) verlangen.

Zwischen Wandlung und Preisminderung besteht ein Wahlrecht. Handelt es sich aber nur um einen geringen Mangel, so besteht kein Wahlrecht, es darf nur die Preisminderung verlangt werden. Bei der Wandlung müssen verkaufte Ware und Kaufpreis zurückgegeben werden.

Kann man sich über Wandlung oder Preisminderung nicht einigen, muss der/die KäuferIn diese Rechte mit einer Klage geltend machen. Da Gerichtsverfahren immer mit hohen Kosten und Risiko verbunden sind, ist eine Einigung meist die bessere Lösung. Eine Klage ist außerdem eine derart ernste Sache, dass die Eltern zustimmen müssen.

SHOPPING IM NETZ

RISIKEN BEI BESTELLUNGEN IM AUSLAND

Du bestellst CDs bei einem Online-Shop in Deutschland oder in den USA. Eine CD hat einen massiven Kratzer und kann nicht abgespielt werden. Du forderst die Zusendung einer intakten CD oder die Rückzahlung des Kaufpreises, dem Verkäufer ist das offenbar egal.

Als KonsumentIn kannst du eine Klage bei einem Gericht an deinem Wohnort einbringen und nur an deinem Wohnort geklagt werden. Bei Geschäftspartnern außerhalb der EU ist die Rechtslage komplizierter. Oft sind für die Gerichtszuständigkeit zwischenstaatliche Abkommen maßgeblich. Bei Gerichtsverfahren im Ausland brauchst du auch einen ausländischen Rechtsanwalt. Österreichische AnwältInnen haben meistens nur die Zulassung im Inland und dürfen deswegen nicht bei ausländischen Gerichten tätig werden.

Hast du ein Gerichtsurteil, bedeutet das aber noch nicht, dass der/die GegnerIn auch tatsächlich macht, was ihm/ihr aufgetragen worden ist. Das Urteil muss dann vollstreckt werden. Beispielsweise kann der/die GerichtsvollzieherIn Sachen in der Wohnung oder im Lager des Schuldners/der Schuldnerin pfänden, diese Sachen werden dann versteigert und du bekommst aus dem Versteigerungspreis den bezahlten Kaufpreis zurück.

Innerhalb der EU ist die Vollstreckung von Urteilen der Mitgliedstaaten leichter möglich. In Ländern außerhalb der EU werden z.B. österreichische Gerichtsurteile hingegen nur in schwerwiegenden Ausnahmefällen vollzogen – was bei Konsumentenschutzverletzungen allerdings praktisch nie der Fall ist. **DAHER IST BEI KAUFVERTRÄGEN MIT UNTERNEHMEN, DEREN SITZ SICH NICHT INNERHALB DER EU BEFINDET, JEDENFALLS DOPPELTE VORSICHT ANGESAGT**. Vergiss nicht: Bei einem Kauf außerhalb der EU können auch noch hohe Zollgebühren anfallen!

All diese Informationen betreffen jedoch lediglich die rechtliche Seite. Die Vollstreckung eines Anspruchs wird aber unmöglich sein, wenn dein/e VertragspartnerIn pleite oder gar plötzlich unauffindbar ist.

AUKTIONEN

ONLINE-VERSTEIGERUNGEN (wie z.B. bei eBay und ricardo) sind aus dem Web nicht mehr wegzudenken. Daher ist es nicht weiter verwunderlich, dass Online-Auktionshäuser auch von Trickbetrügern und Abzockern aller Art bevölkert werden.

WORAUF SOLLTEST DU ACHTEN?

Wie auch beim normalen Online-Shopping ist das Herkunftsland des Anbieters/der Anbieterin ein wichtiger Sicherheitsaspekt. Wenn du in deiner Nachbarschaft etwas ersteigerst, kannst du es auch abholen. Das ist eine relativ sichere Methode, da du die Ware nach Bezahlung sofort mitnehmen kannst. Weiters gibt es auch Versteigerungs-Plattformen, die gut gesicherte Treuhandsysteme und Käuferschutzprogramme anbieten. Jedenfalls solltest du es unbedingt vermeiden, Vorauskasse zu leisten!

Preise vergleichen schadet auch bei Auktionen nicht! Erkundige dich vorher (z.B. bei Geizhals), was der angebotene Artikel in einem Geschäft kostet. So banal das klingt, aber es war schon so manches Schnäppchen ein teurer Kauf!

Ein wichtiger Hinweis auf die Seriosität eines Anbieters sind die **BEWERTUNGSSYSTEME** der einzelnen Auktionshäuser. Dabei wird jede/r KäuferIn aufgefordert eine Wertung abzugeben, wie zufrieden sie oder er mit den Leistungen des Verkäufers/der Verkäuferin war. Die Summe dieser Bewertungen kann dann von allen UserInnen eingesehen werden. Leider gibt es auch unter jenen, die gute Bewertungen haben, immer wieder schwarze Schafe. Man muss also trotzdem vorsichtig sein. Außerdem hat der Seitenanbieter durch Vorhandensein von Bewertungssystemen keine Verpflichtung zur Überprüfung der Bewertungen und zur Vornahme einer allenfalls daraus resultierenden Sperre. Schadenersatzansprüche gegen den Seitenanbieter kommen daher nicht in Frage.

AUKTIONEN

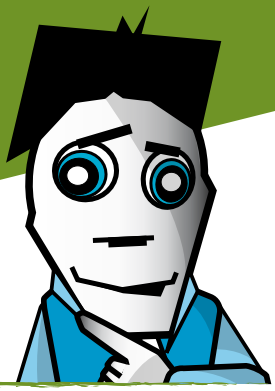
Generell ist es so, dass der Seitenbetreiber nur als Vermittler auftritt, der Vertrag kommt immer zwischen VerkäuferIn und BieterIn zu Stande. Ansprüche, z.B. wegen Nichtlieferung, Mängeln etc., hast du also nur gegenüber dem/der VerkäuferIn. Das geschilderte Rücktrittsrecht bei Käufen über das Internet (siehe Seiten 49/50) gilt auch bei Online-Auktionen, aber nur, wenn es sich um einen gewerblichen Anbieter handelt (Unternehmen, gewerblich tätige Einzelpersonen, „Powerseller"). **SEI DAHER VORSICHTIG UND VERTRAUE NICHT DARAUF, DASS DU ERSTEIGERTE WAREN IMMER ZURÜCK GEBEN KANNST**. Am besten solltest du nur bei Anbietern kaufen, die ausdrücklich ein Rücktrittsrecht einräumen! Beachte, dass es bei Auktionen von „Privat zu Privat" jedenfalls kein Rücktrittsrecht gibt. Für versprochene Eigenschaften muss der/die HändlerIn aber jedenfalls gerade stehen.

Bei Privat-Auktionen ist auch oft zu lesen, dass der/die VerkäuferIn keine Gewährleistung übernimmt. Dieser Ausschluss ist bei Privatpersonen (und nur bei diesen) zwar erlaubt, damit hast du bei Problemen mit der Ware aber praktisch keine Chance, dein Geld zurückzuerhalten. Für Unternehmen gelten gegenüber KonsumentInnen immer die bereits im Kapitel „Shopping" beschriebenen Regelungen. **SEI ALSO BESONDERS DANN VORSICHTIG, WENN DU ETWAS VON PRIVATPERSONEN ERSTEIGERST**!

Vorsicht ist übrigens auch angesagt, wenn du bei einer Auktion verloren hast und dir danach plötzlich dasselbe oder ein ähnliches Teil zu einem sagenhaft günstigen Preis per E-Mail angeboten wird. Manchmal tarnen sich diese E-Mails sogar als z.B. offizielle Nachricht eines Online-Auktionshauses. Oft handelt es sich dabei um echte Betrüger, manchmal auch nur um Leute, die sich die Auktions-Gebühren ersparen wollen. Aber auch in diesem Fall gehst du ein Risiko ein, da dir dann die Sicherheitsmechanismen des Auktionshauses nicht zur Verfügung stehen oder du von diesem gesperrt wirst.

Und zuletzt: Lies das Kleingedruckte! Wenn in einem Inserat steht „XY PC Originalverpackung", so ist damit womöglich auch wirklich NUR die Originalverpackung gemeint, und zwar ohne Inhalt! Es soll auch schon Fälle gegeben haben, in denen eine Luftgitarre ersteigert wurde, aber das ist eine andere Geschichte...

AUKTIONEN

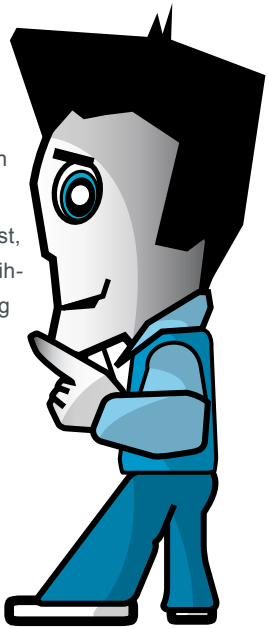


TIPPS FÜR VERKÄUFER/INNEN

Es gibt nicht nur unseriöse Anbieter, auch wenn man selbst als (selbstverständlich seriöse/r) VerkäuferIn auftritt, ist man vor BetrügerInnen nicht sicher.

Beispielsweise gibt es immer wieder SpaßbieterInnen, die Auktionen in ungeahnte Höhen treiben und sich dann nicht mehr melden. In diesem Fall kannst du den/die KäuferIn jedenfalls auf Zahlung klagen und beim Auktionshaus melden, aber auch den Artikel neu einstellen und sparst dir meist die neuerliche Einstellgebühr.

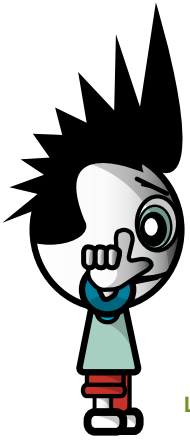
Ärgerlich ist es aber allemal, als HobbyverkäuferIn sollte man also ausreichend Zeit und Geduld mitbringen und sich nicht ärgern lassen. Bevor du das erste Mal etwas anbietest, ist es übrigens nützlich, ein wenig Zeit zu investieren, um sich mit dem System vertraut zu machen und nach Erfahrungsberichten im Internet zu suchen. Vor allem ist es wichtig, klein zu beginnen, um ohne größeren Schaden Erfahrungen sammeln zu können.



Bevor du also deine Stereoanlage oder dein Moped anbietest, beginne doch erstmal mit alten Büchern oder ungeliebten Weihnachtsgeschenken von der Großtante. Es ist wie überall, Übung macht den Meister...

AUKTIONEN

JEDENFALLS MUSST DU BEI DER BESCHREIBUNG DEINER WAREN VORSICHTIG SEIN. Achte bei der Beschreibung der von dir angebotenen Waren immer darauf, dass du diese wahrheitsgetreu beschreibst. Auf kleine Mängel oder sonstige Schönheitsfehler solltest du aufmerksam machen, das sichert dich ebenfalls ab. Sonst kann das Geschäft nämlich angefochten werden und du musst das erhaltene Geld zurückbezahlen. Deine Waren bekommst du aber wieder.

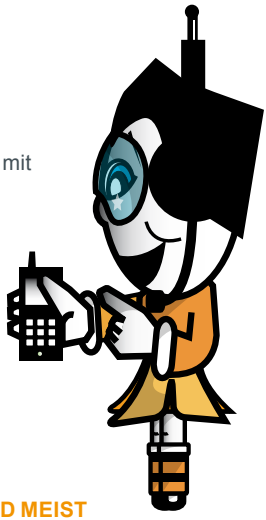


ABER ACHTUNG

WENN DU REGELMÄSSIG WAREN EINKAUFST UND MIT GEWINN VERSTEIGERST BZW. VERKAUFST, KANN DAS BALD ALS „GEWERBLICH“ EINGESTUFT WERDEN.

Du müsstest in so einem Fall dann eventuell einen Gewerbeschein anmelden, Steuern zahlen und/oder würdest unter Umständen sogar als „UnternehmerIn“ eingestuft werden, d.h. du müsstest unter anderem das Konsumentenschutzgesetz beachten und für allfällige Mängel an den von dir verkauften Sachen einstehen. Besser also, du bleibst bei den weniger komplizierten Privatauktionen…

INTERNET-ABZOCKE



DER TRICK IST IMMER ÄHNLICH: Viele Internetseiten locken mit vermeintlichen „Gratis“-Angeboten wie IQ-Tests, Referaten, Songtexten, Bastelvorlagen, Musikdownloads, Horoskopen, Führerscheintests, „Gratis“-SMS etc. Damit du diese Dienste auch in Anspruch nehmen kannst, musst du dich registrieren, also deinen Namen, Adresse, Geburtsdatum etc. eingeben. Außerdem musst du bestätigen, dass du die Allgemeinen Geschäftsbedingungen (AGB) akzeptierst und die Daten absenden.

DIE KOSTEN FÜR DIE ANGEBOTENEN DIENSTLEISTUNGEN SIND MEIST GUT VERSTECKT, SODASS DER/DIE WEBSITE-BESUCHER/IN GLAUBT, ALLES SEI GRATIS – IN WIRKLICHKEIT SITZT MAN ABER SCHNELL IN DER ABZOCKE-FALLE.

DER HAKEN DABEI: Die Informationen über die Kosten der Dienstleistungen sind oft so versteckt, dass du sie sehr leicht übersehen kannst. Die Abzocker arbeiten mit vielen Tricks, um es dir schwerer zu machen, die wahren Kosten erkennen zu können: Manchmal siehst du die Kosten erst, wenn du auf der Seite ganz nach unten scrollst oder der Preis steht nur in Worten und nicht wie üblich in Ziffern auf der Website.

INTERNET-ABZOCKE

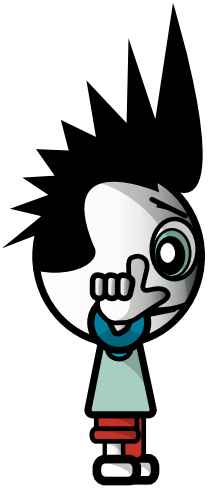
DIE WICHTIGSTEN ABZOCKE-TRICKS VERMEINTLICHER „GRATIS“-ANGEBOTE SIND:

+ Durchaus professionell gestaltete Websites locken mit ansprechenden Themen (Songtexte, Hausaufgaben, „Gratis“-Games etc.).
+ Die Kosten sind oft so versteckt, dass sie in der Hektik, mit der die meisten Menschen Internetseiten überfliegen, übersehen werden.
+ Ohne Bekanntgabe von Adressdaten und dem Akzeptieren der Allgemeinen Geschäftsbedingungen (AGB) ist die Nutzung der angebotenen Dienstleistung nicht möglich.
+ Nach der Registrierung versuchen Anbieter durch Drohungen (von Inkassobüros, Anwälten etc.) KonsumentInnen zur Zahlung zu bewegen.

DIE GUTE NACHRICHT IST: Falls du trotz aller Vorsicht einmal in eine Abzocke-Falle getappt bist, musst du in der Regel **nicht zahlen** – auch wenn die Abzocke-Firmen probieren, dich mit allen möglichen Drohungen einzuschüchtern. Bis jetzt wurde in Österreich noch kein/e KonsumentIn von einer Abzocke-Firma geklagt. Wenn auch nur ein kleiner Teil der Betroffenen bezahlt, ist das für die unseriösen Unternehmen im Internet noch immer ein gutes Geschäft. **LASS DICH ALSO NICHT VERUNSICHERN UND WENDE DICH Z.B. AN DEN INTERNET OMBUDSMANN (WWW.OMBUDSMANN.AT)!**

INTERNET-ABZOCKE

SO VERMEIDEST DU GRATIS-FALLEN IM INTERNET:



1. **Misstrauisch sein!** Sei bei „Gratis“-Angeboten und Gewinnspielen stets misstrauisch. Auch im Internet hat selten jemand etwas zu verschenken. Oft handelt es sich um Lockangebote, bei denen später laufende Kosten entstehen.
2. **Alles genau lesen!** Lies die Allgemeinen Geschäftsbedingungen (AGB) des Anbieters immer durch, bevor du diese bestätigst. Oft verstecken sich darin Verpflichtungen wie z.B. ein kostenpflichtiges Abo zu erwerben. Achte besonders auf die angegebenen Fristen und eventuell entstehenden Kosten.
3. **Keine persönlichen Daten angeben!** Gib zum unverbindlichen Testen von Online-Diensten niemals deine persönlichen Daten an. Storniere außerdem Testzugänge innerhalb der Frist wieder, wenn du sie nicht mehr brauchst.
4. **Alles dokumentieren!** Wenn du dir ein Gratis-Angebot sorgfältig angeschaut hast und überzeugt bist, dass es sich um eine tatsächlich kostenlose Dienstleistung handelt, speichere dir zur Sicherheit alle wichtigen Informationen (AGB, Angebotsseite, deine eingegeben Daten etc.) und druck sie dir aus. Damit hast du im Streitfall wichtige Beweise zur Hand.

INTERNET-ABZOCKE

WAS TUN, WENN ICH TROTZDEM IN EINE FALLE GETAPPT BIN?

Wenn du trotz aller Vorsicht auf ein unseriöses Angebot hereingefallen bist, gilt zunächst einmal: **KEINE PANIK!** Wenn du die folgenden vier Schritte einhältst, sollte dir nichts passieren:

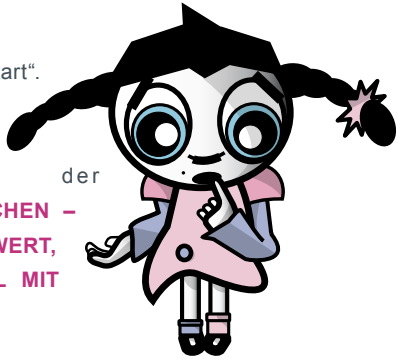
1. Lass dich durch Drohungen (Inkassobüro, Anwalt, Klage, Pfändung etc.) nicht einschüchtern. In der Regel besteht kein Anspruch der unseriösen Firma auf Zahlung.
2. Wende dich an eine Konsumentenberatungsstelle (z.B. Internet Ombudsmann, Arbeiterkammer, Verein für Konsumenteninformation). Sie berät dich oder deine Eltern, was in einem konkreten Fall zu tun ist, und stellt dir einen Musterbrief zur Verfügung, Alle Kontaktinfos und Links dazu findest du im Kapitel „Wer hilft mir weiter?“ ab Seite 68).
3. Mit dem Musterbrief begründest du bzw. ein Elternteil von dir, warum du die Rechnung nicht bezahlst. Schick den Musterbrief eingeschrieben an das Unternehmen und hebe dir den Aufgabeschein und eine Kopie des Schreibens gut auf.
4. Nachdem du die obigen Schritte erledigt hast, kannst du alle weiteren Zahlungsaufforderungen und Drohungen der Abzocke-Firma ignorieren.

VERZEICHNIS VON ABZOCKE-SEITEN

Der Internet Ombudsmann (www.ombudsmann.at) führt eine so genannte „Watchlist“, in der Unternehmen aufgelistet sind, gegen die mehrere Beschwerden vorliegen. Diese Negativliste hilft dir dabei, bekannte Abzocke-Seiten zu erkennen.

Leider tauchen aber fast täglich neue „Gratis“-Fallen im Internet auf. Umso wichtiger ist es, Abzocke-Seiten mit Hilfe der zuvor genannten Kriterien identifizieren zu können.

DATING



Die Partnersuche im Internet ist eine weit verbreitete „Sportart". Viele tragen sich nur aus Neugier oder zum Spaß auf Dating-Plattformen ein. Es soll aber auch schon vorgekommen sein, dass plötzlich der/die Märchenprinz/essin vor der Tür stand. **TROTZDEM SIND – VOR ALLEM FÜR MÄDCHEN – GEWISSE VORSICHTSMASSNAHMEN EMPFEHLENSWERT, INSBESONDERE, WENN MAN SICH ZUM ERSTEN MAL MIT JEMANDEM VERABREDET.**

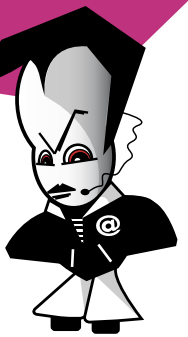
VORSICHT VOR BETRÜGERN!

Besonders als Mann bekommt man öfter Angebote von verlockenden jungen Damen, die vorgeben, zu ihrer eigenen „Sicherheit" eine besondere Telefonnummer zu haben (deren Vorwahl mit 0900, 0901, 0930, 0931 oder 00 beginnt). Der Anruf bei einer solchen Nummer führt jedenfalls mit Sicherheit dazu, dass deine Telefonrechnung schwindelnde Höhen erreicht (oft kosten diese Gespräche EUR 3,- pro Minute oder mehr). Ein Date mit diesen Damen kommt aber praktisch nie zustande. **MERKE:** Mädels, die dich wirklich kennen lernen wollen, haben keine Mehrwertnummer...

DAS ERSTE DATE

Wenn du dich zum ersten Mal mit jemandem verabredest, solltest du als Vorsichtsmaßnahme einen Erwachsenen mitnehmen, dem du vertraust. Bei der Auswahl des Treffpunktes ist es hilfreich, wenn dieser sehr belebt ist oder wenn es sich dabei um dein Stammlokal handelt (was nicht immer angenehm sein kann).

DATING



PERSÖNLICHE DATEN

Es ist eine Grundregel im Netz, nur so viele persönliche Daten von sich zu veröffentlichen, wie unbedingt nötig. Das ist auf Dating-Sites naturgemäß nicht so einfach, denn man/frau will sich ja in einem vorteilhaften Licht darstellen und von anderen gefunden werden.

In jedem Fall solltest du keine Daten veröffentlichen, die auf deinen richtigen Namen oder deine Wohnadresse schließen lassen. Seriöse Dating-Sites erkennt man auch daran, dass sie die E-Mail-Adressen ihrer Mitglieder geheim halten und keine Profile mit Telefonnummern zulassen.

Am besten, du legst dir für diese Zwecke eine eigene E-Mail-Adresse zu (z.B. von Yahoo!, Windows Live Hotmail oder Google Mail), die nicht mit deinem richtigen Namen in Verbindung gebracht werden kann.

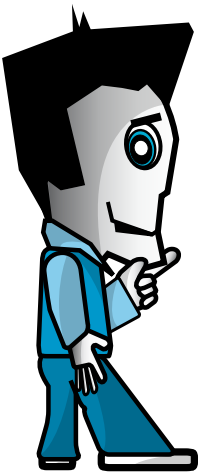
Ein Beispiel: Du registrierst dich auf einer Partnersuch-Seite unter angel-for-u@live.at. Wenn man auf Bing oder Google nach dieser Adresse sucht, findet man deinen Blog. Auf deinem Blog steht dein richtiger Name. Eine Nachfrage im elektronischen Telefonbuch findet deine Adresse und deine Handynummer; Fazit: In weniger als 10 Minuten sind die persönlichen Details aus deinem Dating-Profil mit deinen realen Daten verknüpfbar – und das wirst du sicher nicht wollen.

QUELLEN ÜBERPRÜFEN UND ANGEBEN

WAHR ODER FALSCH IM INTERNET?

Du nutzt das Internet zur Informationssuche und entwickelst aus den Online-Inhalten deine eigenen Texte oder Referate? Dann ist es notwendig, dass du dich mit Quellenkritik (Wie erkenne ich, was wahr oder falsch ist?) und Zitierregeln (siehe nächste Seite) vertraut machst.

Das Internet ist nicht nur eine unerschöpfliche Quelle von relevanten und richtigen Informationen, sondern gleichermaßen eine Sammlung von vielen Halbwahrheiten und Unwahrheiten. Diese zu erkennen ist nicht immer ganz einfach, vor allem wenn man sich neu in ein Thema einarbeitet. Folgende Fragen sollen dir helfen, wahr und falsch trennen zu können:



Inhaltsüberprüfung der Seite

+ Werden Quellenangaben angeführt?
+ Wann war das letzte Update?
+ Bestehen Interessenskonflikte in der Argumentation – ist die/der AutorIn kommerziell, politisch, organisatorisch, persönlich mit dem Thema verbunden?
+ Kann Parteilichkeit vorhanden sein? Wird z.B. ausdrücklich für eine bestimmte Position „geworben“?
+ Welche Logos oder Erkennungszeichen werden auf der Seite verwendet? Wer könnte dahinter stehen?
+ Welche weiteren Seiten werden verlinkt? Welcher Art sind diese Seiten?

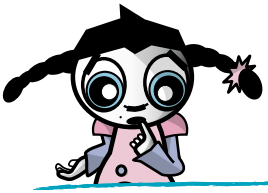
Wer ist AutorIn der Seite?

+ Gibt sich der/die AutorIn zu erkennen?
+ Steht eine Organisation/ein Unternehmen dahinter? Wenn ja, welche Interessen verfolgt die Organisation/das Unternehmen?
+ Wem gehört die Internetadresse? Vielleicht kann die Datenbank auf www.whois.net dabei helfen.
+ Ist die/der AutorIn für die Inhalte kompetent? → Name der Autorin/des Autors in Suchmaschine eingeben! Wird sie/er oft zu diesem Thema zitiert? Kommt er/sie in einem anderen Zusammenhang vor?

QUELLEN ÜBERPRÜFEN UND ANGEBEN

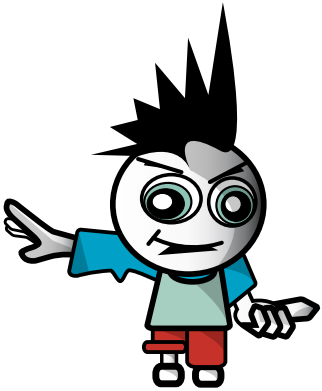
Seriosität der Seite

+ In welchem Zusammenhang (sonstige Inhalte der Website) steht der gefundene Text?
+ Wie häufig und von wem wird die Seite verlinkt (z.B. mit Bing oder Google überprüfen)? Wie seriös sind diese Anbieter?
+ Werden Quellen richtig und nachvollziehbar angegeben?
+ Was sagen andere Quellen (auch außerhalb des Internet!)?

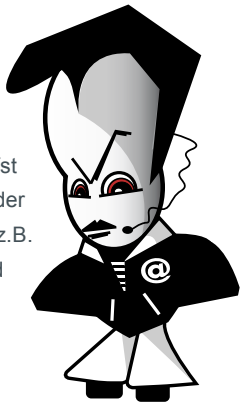


RICHTIGE VERWENDUNG VON FREMDEN INHALTEN (ZITIERREGELN)

Jeder Text, jedes Bild, jedes Video wurde von jemandem ursprünglich geschaffen, eben von einer/m „UrheberIn“. Ein/e UrheberIn kann z.B. eine Person sein, die ein Buch schreibt, ein Bild malt, einen Song textet, ein Foto aufnimmt oder eine Datenbank erstellt. Die/der UrheberIn genießt für diese Schöpfung – das geistige Eigentum – einen rechtlichen Schutz, der im Urheberrechtsgesetz festgehalten ist.



QUELLEN ÜBERPRÜFEN UND ANGEBEN



MÖCHTEST DU Z.B. MUSIK, FOTOS, TEXTE ODER FILME, DIE DU NICHT SELBST ERSTELLT HAST, AUF Z.B. DEINEM BLOG VERÖFFENTLICHEN, MUSST DU DIE/DEN URHEBERIN UM ERLAUBNIS FRAGEN. Veröffentlichst du im Internet fremde Inhalte ohne Zustimmung der Urheberin/des Urhebers, kann das im Falle einer Klage bis zu einigen tausend Euro Strafe kosten. Du darfst einen Ausschnitt („Zitat“) aus einem fremden Werk in dein eigenes übernehmen oder im Unterricht verwenden (z.B. bei einem Referat), wenn du deutlich machst, dass z.B. eine Textpassage nicht von dir stammt und du die Quelle nennst. Entscheidend ist, dass du alle verfügbaren Daten angibst, damit die/der LeserIn das Original finden kann:

1. Name des Autors/der Autorin bzw. der Institution
2. Erscheinungsjahr
3. Titel
4. Seitenangaben
5. Angaben zur Quelle (z.B. Buch oder Internet)

Wenn die Quelle das Internet ist, musst du zusätzlich anführen:

1. Vollständige Internetadresse (URL)
2. Datum des letzten Aufrufs in Klammern

BEISPIEL:

Muster, Max (2010): So zitiert man richtig. in: Magazin für Wissenschaft, Nr. 03/08, S. 12-17. Online im Internet: http://www.musteradresse.com/magazin/so-zitiert-man-richtig [01.06.2011].

Dies gilt nicht nur für geschriebene Texte, sondern auch für Fotos, Grafiken, Videos, Audiobeiträge etc.! Und es gilt nicht nur bei einer Hausaufgabe oder Schularbeit, sondern auch bei Beiträgen in Foren, Blogs, Communitys und Wikis.

QUELLEN ÜBERPRÜFEN UND ANGEBEN

WAS TUN, WENN ICH EIGENE INHALTE UNERLAUBT VERÖFFENTLICHT IM INTERNET FINDE?

Du hast ein Foto, einen Text, ein Video etc. erstellt und jemand anderer hat dein „Werk" im Internet veröffentlicht. Hier hast du als UrheberIn einen Unterlassungsanspruch und auch einen Schadenersatzanspruch. Bitte den/die Website-BetreiberIn freundlich, den Inhalt zu entfernen. Wenn das nichts nützt, kannst du eine Klage einbringen – dazu musst du allerdings einen Anwalt beauftragen und das kann ganz schön ins Geld gehen.

PLAGIATE

Wenn man von anderen erstellte Inhalte unerlaubterweise übernimmt und als die eigenen ausgibt, spricht man von „Plagiaten". „Copy and Paste", wie im Englischen das Kopieren und Einfügen am Computer genannt wird, ist verlockend einfach. Ich finde etwas im Internet, kopiere es und gebe es als meine eigene Arbeit aus.

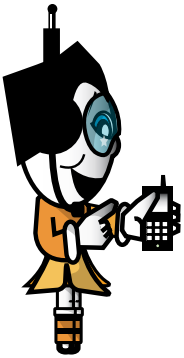
Solches Kopieren von fremden Texten und Arbeiten verletzt aber das Urheberrecht! Denn schließlich sind die Texte ja von jemand anderem geschrieben worden. Wird man erwischt, kann das im Ernstfall sogar Schadenersatzforderungen, Schulverweise, Aberkennung eines Abschlusses/einer Arbeit oder andere unangenehme Folgen haben!

CREATIVE COMMONS (CC) – der alternative Urheberrechtsschutz

Die eigenen Werke, seien es Texte, Bilder oder Musik, kann man unter einer so genannten „Creative Commons-Lizenz" (www.creativecommons.org) veröffentlichen. Damit gibt man anderen Menschen die Möglichkeit, die eigenen Werke unter bestimmten Bedingungen weiter zu verarbeiten und zu verwenden. In jedem Fall musst du die Bedingungen, unter denen du die Werke verwenden darfst, genau lesen und einhalten. CC-lizensierte Musik z.B. kann jemand anderer – meist unter Nennung des Urhebers/der Urheberin – auf der eigenen Website einbauen.

In Sammlungen und Datenbanken kann man speziell nach diesen Werken suchen und dort auch selbst anbieten. Datenbanken mit CC-lizensierter Musik findest du z.B. unter www.nolabel.at, www.jamendo.com oder http://ccmixter.org.

WER HILFT MIR WEITER?



Für die Beantwortung von weiteren Fragen zur sicheren Internetnutzung steht dir das Team von Saferinternet.at im Web unter www.saferinternet.at und www.facebook.com/saferinternetat oder per E-Mail unter beratung@saferinternet.at zur Seite.

Hilfe bei Belästigung, Cyber-Mobbing und Online-Sucht

Rat auf Draht: www.rataufdraht.at

- Kostenloser, anonymer 24h-Notruf für Kinder, Jugendliche und Eltern unter 147 (ohne Vorwahl)
- Online-Beratung auf www.rataufdraht.at

Meldung illegaler Inhalte

Stopline: www.stopline.at

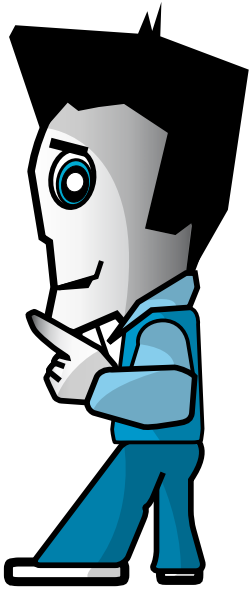
- Anonyme Meldestelle der österreichischen Internet-Service-Provider gegen Kinderpornographie und nationalsozialistische Wiederbetätigung im Internet

Bundesministerium für Inneres: www.bmi.gv.at/meldestellen

- Meldestellen gegen NS-Wiederbetätigung und Kinderpornografie

WER HILFT MIR WEITER?

Probleme mit Online-Shopping und Internet-Abzocke



Internet Ombudsmann: www.ombudsmann.at

- Kostenlose Online-Beratung und Streitschlichtung

Europäisches Verbraucherzentrum: www.europakonsument.at

- Telefonische Beratung bei Problemen mit Einkäufen im Ausland unter 0810/810 225 (kostenpflichtig), werktags von 9 bis 15 Uhr

Verein für Konsumenteninformation (VKI): www.konsument.at

- Konsumententelefon unter der Nummer 0900/91 00 24 (kostenpflichtig), täglich von 9 bis 15 Uhr
- Persönliche Beratung werktags von 9 bis 18 Uhr im VKI Info-Center, Mariahilfer Straße 81, 1060 Wien (Terminvereinbarung 01/588 770) oder in der VKI Landesstelle Tirol, Maximilianstraße 9, 6020 Innsbruck (Terminvereinbarung 0512/586878)

Arbeiterkammern: www.arbeiterkammer.at

- Telefonische Beratung
- Persönliche Beratung in den Bundesländerstellen, Kontaktinformationen in den Bundesländern siehe www.arbeiterkammer.at/kontakt

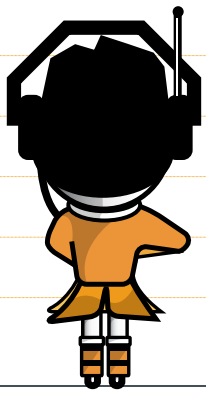
Technischer Support

- Kostenlose telefonische Unterstützung von Microsoft zu viren- und sicherheitsrelevanten Anfragen unter der Nummer 01/50222 22 55 von Montag bis Freitag von 8 bis 18 Uhr und Samstag von 9 bis 17 Uhr

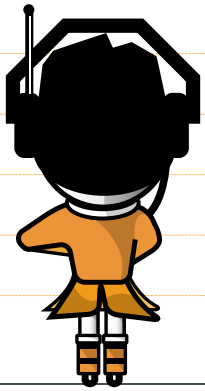
INDEX

INDEX

NOTIZEN



NOTIZEN



ORF

147

Rat auf **Draht**

***Notruf** für Kinder, Jugendliche und deren Bezugspersonen*

Wenn Du Hilfe brauchst – ruf an!

Rund um die Uhr, kostenlos, anonym, österreichweit.

Wenn du nicht mehr weiter weißt – wir hören dir zu!

Über jedes Problem kann man sprechen – oft ist eine Situation gar nicht so ausweglos, wie sie scheint!

Der Notruf für Kinder, Jugendliche und deren Bezugspersonen ist unter der Kurznummer 147 ohne Vorwahl aus ganz Österreich erreichbar!
Anonym heißt, dass du uns weder deinen Namen noch deine Adresse sagen musst.
Egal ob vom Festnetz oder Handy – dein Anruf kostet nichts.
Du brauchst dich an keine Öffnungszeiten halten, denn du erreichst uns rund um die Uhr – selbstverständlich auch am Wochenende und an Feiertagen.
***Wenn du Hilfe brauchst:** Wir haben Adressen in ganz Österreich und können im Notfall auch den direkten Kontakt herstellen.*

*Auf unserer Homepage **http://rataufdraht.ORF.at** findest du Antworten auf häufig gestellte Fragen und kannst dich auch online beraten lassen.*

rataufdraht.ORF.at

Unsere Partner:

STOPLINE

Österreichische Meldestelle gegen Kinderpornografie und nationalsozialistische Wiederbetätigung

Wer sind wir?

www.stopline.at bietet Ihnen - auch anonym - die Möglichkeit, einfach, schnell und unbürokratisch zu melden, wenn Sie im Internet auf illegales Material stoßen.

Seit der Gründung im Jahr 1998 wurden von Stopline mehr als 18.500 Meldungen bearbeitet. Erfolgreich ist Stopline national durch die enge Zusammenarbeit mit den relevanten Polizei-Meldestellen des Bundesministeriums für Inneres, den österreichischen Internet Service Providern sowie international als Mitglied von INHOPE, einer Vereinigung von mehr als 35 Hotlines gegen Kinderpornografie weltweit.

Wie können Sie helfen?

- ⇨ Melden Sie illegale Inhalte im Internet unter **www.stopline.at**.
- ⇨ Publizieren Sie das Stopline-Logo. Sie können es ganz einfach von **www.stopline.at** downloaden und an prominenter Stelle mit einem Link zur Stopline auf Ihrer Webseite platzieren. Damit tragen Sie dazu bei, die Bekanntheit der Stopline zu fördern und illegale Inhalte im Internet zu reduzieren.

inhope

www.stopline.at

co-funded by the European Union

Einfach mit Gigaspeed lossurfen.

Gigaspeed 16. Doppelt so schnell.

Schnell ist Ihnen nicht schnell genug? Dann steigen Sie ein mit Gigaspeed 16: Surfen Sie doppelt so schnell mit bis zu 16 Mbit/s und genießen Sie das Internet von morgen – gigaschnelle Up-und Downloads inklusive.

Einfach A1.

A1.net