SAFER SURFING

TIPPS & TRICKS ZUM SICHEREN UMGANG MIT DEM INTERNET

Saferinternet.at
Das Internet sicher nutzen!

BUNDESMINISTERIUM FÜR GESUNDHEIT FAMILIE UND JUGEND

Microsoft

Bist du dir sicher – mit uns Dreien?

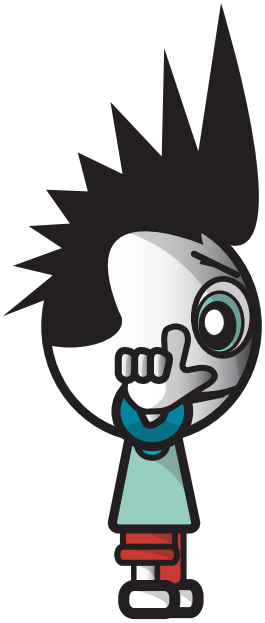
Und wie! Mit uns beiden auf den ersten Blick, mit meinem PC auf den ersten Klick.
Dank der Programme von Microsoft. Die sind einfach, aktuell, schnell und automatisch sicher, vom Start weg. Klar gehört meine Software gepflegt – wie meine Beziehung auch.
Das ist aber einfach und geht sehr schnell. Wie?

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)

EINLEITUNG



Das Internet hat sich in den vergangenen 15 Jahren als eines der wichtigsten Kommunikationsmittel für Beruf, Schule und Freizeit etabliert.

Trotzdem wissen die Benutzer/innen (wir wollen sie einfach User/innen nennen) oft erstaunlich wenig, wie es um ihre Rechte und Pflichten im Netz bestellt ist, was man im Netz tun kann, darf und soll, was als guter Stil und was als böse Beleidigung gilt und welche Konsequenzen daraus entstehen können.

Wir, die Initiative „Saferinternet.at - Das Internet sicher nutzen“, wollen mit dieser Broschüre mithelfen, einige dieser Wissenslücken zu schließen und unangenehme Überraschungen zu vermeiden.

Impressum:
Medieninhaber, Herausgeber, Verleger:
ISPA – Internet Service Providers Austria Verband der österreichischen Internet-Anbieter, 1090 Wien, Währinger Straße 3/18, www.ispa.at, im Rahmen von Saferinternet.at, Bildmaterial bereitgestellt von SAFT

ÜBER SAFERINTERNET.AT

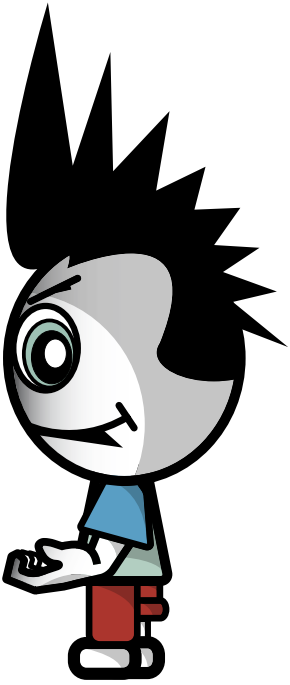
Die Initiative Saferinternet.at unterstützt Internetnutzer/innen, insbesondere Kinder und Jugendliche, bei der sicheren Nutzung des Internet. Saferinternet.at ist der österreichische Informations- und Koordinationsknoten im europäischen Safer Internet Netzwerk.

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 plus Programm" der EU-Kommission (GD Informationsgesellschaft & Medien), das Bundeskanzleramt, Ministerien und Sponsoren aus der Wirtschaft.

Mehr Informationen über die Initiative Saferinternet.at findest du auf unserer Website: http://www.saferinternet.at

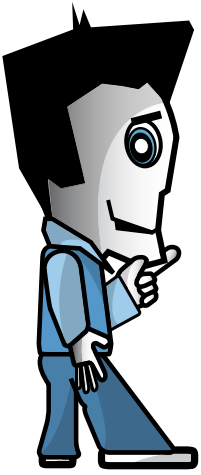
Viel Spaß beim Lesen dieser Broschüre wünscht dir das Team von Saferinternet.at.



P. S.: Noch ein Hinweis zum Umgang mit dieser Broschüre: Wir haben auf den letzten Seiten alle Worterklärungen in einem Glossar zusammengestellt und auch alle Links der im Text erwähnten Webseiten und Organisationen aufgelistet. Wenn dir im Text etwas unklar ist, so ist es durchaus möglich, dass du dort die Lösung findest...

INHALT

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?

Sagen wir mal, Ausnahmen bestätigen die Regel. Es ist sicher eine gute Idee, im Internet nur das zu sagen (schreiben) und zu tun, was man auch im realen Leben tun würde, ohne ein schlechtes Gewissen zu haben.

Natürlich ist das „Gewissen" eine sehr subjektive Angelegenheit, aber für die meisten Menschen doch ein brauchbarer Leitfaden durchs Leben.

WERDEN WIR KONKRETER:
Würdest du deinen Chef oder deine Lehrerin 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 Gasse setzen und jeden, der vorbeikommt, einladen, eine Kopie davon zu machen? **NEIN?** Siehst du, so einfach ist das.

DOS AND DON'TS

Viele Leute glauben leider, 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 einfach **„NEIN!"**, die längere ist etwas komplizierter:

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 User/in im Internet etwas macht (z.B. Chatten, ein 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 zum Computer bzw. zur Telefonnummer des/der entsprechenden Users/Userin.

DOS AND DON'TS

Die meisten Straftaten können also relativ schnell und problemlos aufgeklärt werden.

Auch andere Benutzer/innen desselben PCs können sich ansehen, welche Webseiten ihre Vorgänger/innen 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 ein hohes Maß an technischem Wissen voraus und sind trotzdem nicht unfehlbar. Wenn jemandem eine genügende Anzahl an Daten (Logfiles, verwendete Nicknames, Passwörter etc.) zur Verfügung steht, kann er/sie meist auch den technisch versiertesten Bösewichten das Handwerk legen. Denn irgendwann macht jeder einen Fehler.

WAS TUN?

Was also kannst du tun, wenn dich jemand geärgert hat, wenn du Wut im Bauch hast?

EINE MAILBOMBE VERSCHICKEN?

EINEN FLAME-WAR STARTEN?

Bedenke, dass ein E-Mail, einmal abgesendet, nicht mehr zurückgeholt werden kann, ebenso wenig eine Message im Chat oder ein Posting in einem Diskussionsforum.

Deshalb lautet Großmutters Hausrezept dagegen einfach „warten".

Gib dir selbst ein paar Stunden oder einen Tag Zeit bis der erste Ärger verraucht ist und du wieder klar denken kannst. Dann schreib dein Mail, 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:

;-)

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 ALLEIN ABSCHLIESSEN?

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

7–13 JAHRE:

Jugendliche dürfen bis zu ihrem 14. Geburtstag nur kleine alltägliche Geschäfte allein 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 müssten.

Sobald Geschäfte aber deinen Lebensunterhalt gefährden, müssen sie von einem Elternteil genehmigt werden. Bestellst du immer wieder Sachen auf Pump und übersteigen die Ratenzahlungen insgesamt schon dein Einkommen oder Taschengeld, ist für weitere Geschäfte jedenfalls eine Zustimmung eines Elternteils nötig.

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. Search Engines und Preisvergleichs- und Testbericht Seiten (z.B. Ciao, Dooyoo oder Geizhals) können ein guter Ausgangspunkt für eigene 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 Kasten).

√ **FAUSTREGEL:** Je weiter ein Versandhaus von dir weg ist, desto schwieriger ist es, sich zu beschweren oder zu reklamieren. Händlern innerhalb Österreichs solltest du daher den Vorzug geben, bei Bestellungen in anderen EU-Mitgliedstaaten kann es schon haariger werden, ist aber immer noch relativ sicher. Bei Händlern außerhalb der EU solltest du nur bestellen, wenn diese sehr bekannt sind oder wenn du das Produkt nur dort bekommst (siehe Kasten).

√ **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 irgendjemand über irgendjemand anderen schreibt, aber generelle Anhaltspunkte über die Seriosität eines Händlers lassen sich doch fast immer finden.

SHOPPING IM NETZ

√ **BEACHTE DIE ZAHLUNGSMODALITÄTEN:** Wenn ein Händler nur Kreditkarten nimmt, du aber keine zur Verfügung hast, so scheidet dieser wohl aus. Die in Österreich immer noch verbreitete Lieferung per Nachnahme ist zwar meist etwas teurer, aber dafür sehr sicher, da du erst bezahlst, wenn du das Paket schon in Händen hältst.

√ **BEACHTE ALLFÄLLIGE GÜTESIEGEL ODER VERBANDSMITGLIEDSCHAFTEN** auf der Webseite des Verkäufers. Allerdings ist nicht jedes Gütesiegel gleich viel wert. Auf der Webseite des „E-Commerce Gütezeichens" (www.guetezeichen.at) findest du Informationen zu Shops, die als vertrauenswürdig einzuschätzen sind.

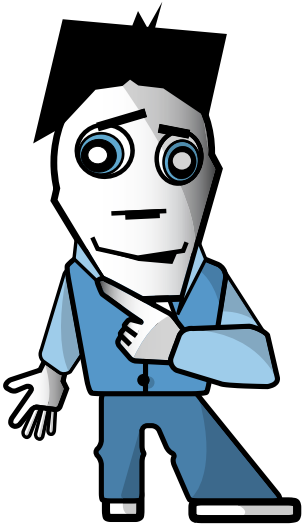
Was sind ALLGEMEINE GESCHÄFTSBEDINGUNGEN?

Du bestellst einen Computerbildschirm über das Internet. Wegen eines Produktionsfehlers explodiert der Bildschirm, du wirst verletzt und möchtest Schmerzensgeld. Der Verkäufer verweist auf seine allgemeinen Geschäftsbedingungen, wonach jede Haftung ausgeschlossen ist.

ALLGEMEINE GESCHÄFTSBEDINGUNGEN (AGB) SIND STANDARDVERTRÄGE, DIE UNTERNEHMEN ALLEN IHREN GESCHÄFTEN ZUGRUNDE LEGEN. Die Anwendung von AGBs auf eine bestimmte Bestellung muss zuvor zwischen Unternehmen und Kunden vereinbart werden. Dafür reicht es, dass der Unternehmer deutlich zu erkennen gibt, dass seine AGBs angewendet werden sollen und man die AGBs vor der Bestellung lesen und speichern kann. Das ist der Fall, wenn es auf der Seite mit dem Bestellformular den Link „AGBs" gibt, der eben die Seite mit den allgemeinen Geschäftsbedingungen öffnet. Wer AGBs verwendet, möchte sich natürlich möglichst umfangreich gegen alle denkbaren Ansprüche absichern. AGBs sind für Kunden und Kundinnen daher oft nachteilig. Besonders nachteilige Bestimmungen in AGBs sind allerdings ungültig. 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

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



Auch im Internet kommt ein Vertrag (diesfalls zwischen Händler und Konsument) durch ein Angebot und dessen Annahme zustande. Ein von dir ausgefülltes Bestellformular gilt als dein Angebot, etwas zu kaufen. Ist die Bestellung dem Händler zugegangen, bist du daran eine gewisse Zeit gebunden (nicht aber der Händler, denn der muss ja dein Angebot erst annehmen!). Die Bindungsdauer ist bei elektronischen Formularen oder E-Mails eher kurz (etwa drei Arbeitstage).

NIMMT DER VERKÄUFER DEIN ANGEBOT INNERHALB DIESER BINDUNGSDAUER AN, KOMMT DER VERTRAG ZUSTANDE, DU HAST ALLERDINGS EIN RÜCKTRITTSRECHT (SIEHE NÄCHSTE SEITE).

Erklärt der Verkäufer hingegen, er kann 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 unten.

SHOPPING IM NETZ

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

Du hast einen DVD-Brenner bestellt. Du 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. Achtung! Bei Versteigerungen gibt es in Österreich – anders als nach neuester Rechtsprechung in Deutschland – kein Rücktrittsrecht! Ein Rücktritt ist nur dann möglich, wenn es sich um keine tatsächliche Versteigerung handelt, z.B. wenn Du ein „Artikel sofort kaufen"-Angebot annimmst. Du hast ab dem Zeitpunkt der Lieferung der Ware (bei Dienstleistungen ab Vertragsabschluss) sieben Werktage Zeit, vom Vertrag zurückzutreten. Der Samstag zählt nicht als Werktag. 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 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 schon vor Ablauf der siebentägigen Frist begonnen werden (bereits aktivierter Mail-Account) und wenn dies mit dem Unternehmen vereinbart wurde.
- ✓ bei verderblichen Waren (Lebensmitteln)
- ✓ bei versiegelten Videos, CDs, Software, wenn du die Versiegelung (z.B. Plastikhülle) schon entfernt hast
- ✓ bei Zeitungen, Zeitschriften und Illustrierten; wohl aber bei Bestellung von Abos
- ✓ bei Wett- und Lotteriedienstleistungen
- ✓ bei Hauslieferungen (Fahrtendienste wie Pizza-Zustellung)
- ✓ bei Freizeitdienstleistungen

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

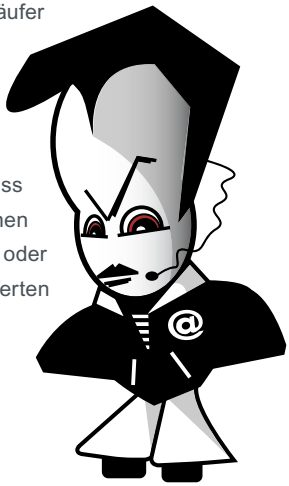
5. WAS TUN, WENN DIE WARE ÜBERHAUPT NICHT GELIEFERT WIRD?

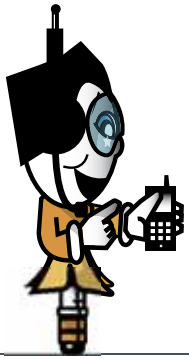
Liefert der Verkäufer die Ware nicht rechtzeitig an den vereinbarten Lieferort, spricht man von „Verzug“. Du kannst in diesem Fall weiterhin die Lieferung verlangen oder auch unter Setzung einer Nachfrist vom Vertrag zurücktreten („Ich trete vom Vertrag zurück, wenn Sie die Ware nicht binnen 14 Tagen liefern.“). Die Frist muss aber so bemessen sein, dass der Verkäufer tatsächlich noch die Möglichkeit der Nachholung hat, die Versanddauer sollte man daher einkalkulieren. Keine Rücktrittserklärung und Nachfristsetzung ist bei „Fixgeschäften“ nötig. Ein solches liegt vor, wenn klar erkennbar ist, dass der Besteller oder die Bestellerin an einer verspäteten Leistung kein Interesse hat. Beispiel: Lieferung eines Weihnachtsbaums am 7. Jänner.

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 verpflichtet sich der Verkäufer 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 Käufer/in gesetzlich zu. Der Verkäufer einer Sache muss dafür einstehen, dass die Sache 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 Sache. Verbesserung ist der Nachtrag eines fehlenden Teils. Bei einem Online-Kauf sitzt der Verkäufer meist an einem entfernten Ort. Deshalb kommt praktisch nur der gänzliche Austausch der Sache in Frage. Der Verkäufer 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 einem Privaten kaufst, so kann dieser 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 Verkäufer trotz Aufforderung nichts macht oder sein 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 Sache und Kaufpreis zurückgegeben werden.

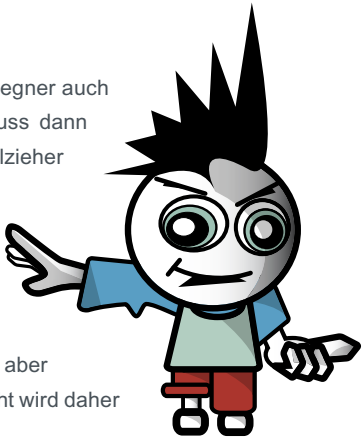
Kann man sich über Wandlung oder Preisminderung nicht einigen, muss der/die Käufer/in diese Rechte mit einer Klage geltend machen. Hat man den Kaufpreis noch nicht bezahlt, kann man sich auch klagen lassen und gegen die Klage entsprechende Einwände erheben. Da Gerichtsverfahren immer mit hohen Kosten und Risiko verbunden sind, ist eine Einigung meist die bessere Lösung. Die Erhebung einer Klage ist daneben eine derart ernste Sache, dass beide Elternteile zustimmen müssen.

SHOPPING IM NETZ

RISIKEN BEI BESTELLUNGEN IM AUSLAND

Du bestellst CDs bei einem Online-Store 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 Konsument/in kannst du eine Klage bei einem Gericht an deinem Wohnort einbringen und nur an deinem Wohnort geklagt werden. Das gilt aber nur, wenn dein Geschäftspartner innerhalb der EU sitzt. Bei Geschäftspartnern außerhalb der EU ist die Rechtslage meist kompliziert. Oft sind für die Gerichtszuständigkeit zwischenstaatliche Abkommen maßgeblich, die keinen Verbraucherschutz vorsehen. Meist ist der Wohnsitz oder Firmensitz des Beklagten maßgeblich, das bedeutet ein Gerichtsverfahren im Ausland. Bei Gerichtsverfahren im Ausland brauchst du auch einen ausländischen Rechtsanwalt. Österreichische Anwälte und 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 Gegner auch tatsächlich macht, was ihm aufgetragen worden ist. Das Urteil muss dann zwangsweise vollstreckt werden. Beispielsweise kann der Gerichtsvollzieher Sachen in der Wohnung oder im Lager des Schuldners 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 möglich. Zwischen den USA und Österreich gibt es aber nicht einmal ein Vollstreckungsabkommen, ein amerikanisches Gericht wird daher ein österreichisches Gerichtsurteil nicht vollziehen.

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

AUKTIONEN

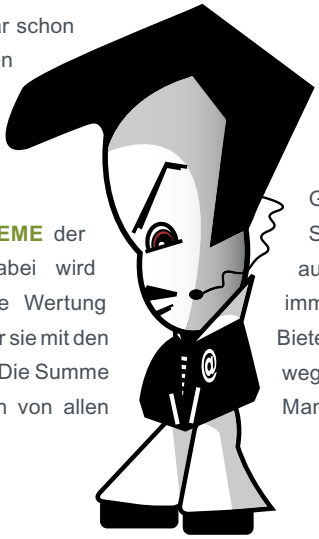
ONLINE VERSTEIGERUNGEN erfreuen sich zunehmender Beliebtheit, eBay zählt mittlerweile zu den größten Websites der Welt. Wo aber viel Licht ist, ist auch viel Schatten. Daher ist es nicht weiter verwunderlich, dass Online Auktionshäuser auch von Trickbetrügern und Abzockern aller Art bevölkert werden.

WORAUF SOLLTEST DU ACHTEN?

Wie auch beim normalen Online-Shopping ist die geografische Nähe ein wichtiger Sicherheitsaspekt. Wenn du in deiner Nachbarschaft etwas ersteigerst, kannst du es auch abholen und vor dem Bezahlen in Augenschein nehmen. Betrüger lassen sich wohl selten zu Hause besuchen... 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 eher teurer Kauf!

Ein wichtiger Hinweis auf die Seriosität eines Anbieters sind die **BEWERTUNGSSYSTEME** der einzelnen Auktionshäuser. Dabei wird jeder Käufer aufgefordert eine Wertung abzugeben, wie zufrieden er oder sie mit den Leistungen des Verkäufers war. Die Summe dieser Bewertungen kann dann von allen User/innen eingesehen werden. Leider gibt es auch unter jenen, die gute Bewertungen haben, immer wieder schwarze Schafe.

Es ist daher trotzdem Vorsicht geboten. Außerdem ergibt sich aus dem Vorhandensein von Bewertungssystemen keine Verpflichtung des Seitenanbieters zur Überprüfung der Bewertungen und zur Vornahme einer allenfalls daraus resultierenden Sperre.



Schadenersatzansprüche gegen den Seitenanbieter kommen daher nicht in Frage.

Generell ist es so, dass der Seitenbetreiber nur als Vermittler auftritt, der Vertrag kommt immer zwischen Verkäufer und Bieter zu Stande. Ansprüche, z.B. wegen Nichtlieferung, wegen Mangelhaftigkeit etc., hast du

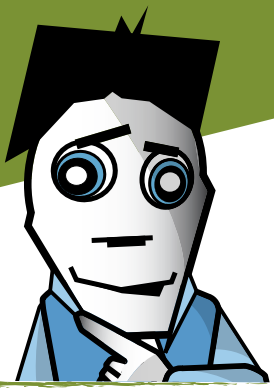
AUKTIONEN

also nur gegenüber dem Verkäufer. Das geschilderte Rücktrittsrecht bei Käufen über das Internet 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 GEGENSTÄNDE IMMER ZURÜCK GEBEN KANNST.** Am besten solltest du nur bei Anbietern kaufen, die ausdrücklich ein Rücktrittsrecht einräumen! Bitte beachte, dass es bei Auktionen von „Privat zu Privat" jedenfalls kein Rücktrittsrecht gibt. Nur bei Fehlbeschreibungen durch den Anbieter kannst du (wegen Irrtums) den Vertrag anfechten.

Bei Privat-Auktionen ist auch oft zu lesen, dass der Verkäufer 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 Konsumenten immer die bereits in unserem „Shopping"-Teil beschriebenen Gewährleistungspflichten. Sei also besonders dann vorsichtig, wenn du etwas von Privatpersonen ersteigerst! Für Unternehmen gelten übrigens die bereits in unserem „Shopping"-Teil geschilderten Regelungen. Sei also besonders vorsichtig, wenn du etwas von Privatpersonen ersteigerst! Vorsicht ist übrigens umsomehr geboten, 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 Mails sogar als offizielle eBay-Nachricht. Oft handelt es sich dabei um echte Betrüger, manchmal auch nur um Leute, die sich die eBay-Gebühren ersparen wollen. Aber auch in diesem Fall gehst du ein Risiko ein, da dir dann die Sicherheitsmechanismen des Auktionshauses nicht zur Verfügung stehen.

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

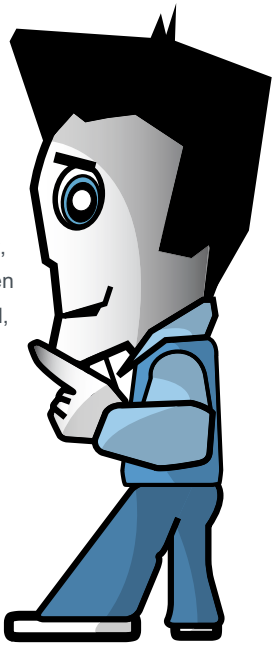


TIPPS FÜR VERKÄUFER

Es gibt nicht nur unseriöse Anbieter, auch wenn man selbst als (selbstverständlich seriöser) Verkäufer auftritt, ist man vor Scherzbolden nicht gefeit.

Beispielsweise gibt es immer wieder Spaßbieter, die Auktionen in ungeahnte Höhen treiben und sich dann nicht mehr melden. In diesem Fall kannst du den Artikel neu einstellen und sparst dir die neuerliche Einstellgebühr.

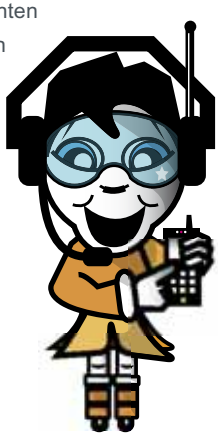
Ärgerlich ist es aber allemal, als Hobbyverkäufer sollte man also ausreichend Zeit und Geduld mitbringen und sich nicht ärgern lassen. Bevor du das erste Mal etwas anbietest ist es übrigens nützlich, ein wenig Zeit zu investieren, um sich mit dem System vertraut zu machen, nach Erfahrungsberichten im Internet zu suchen, und sich so selbst ein Bild zu machen. 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 JEGLICHE GEWÄHRLEISTUNGBEIMVERKAUFVON GEBRAUCHTEN SACHEN KOMPLETT AUSSCHLIESSEN, damit an dich keine Ansprüche wegen allfälliger Mängel gestellt werden können! Der Ausschluss der Gewährleistung verhindert jedoch nicht, dass das abgeschlossene Geschäft wegen Irrtums angefochten werden kann. Achte bei der Beschreibung der von dir angebotenen Waren immer darauf, dass du diese genau beschreibst – je mehr, desto besser – und deine Angaben auch der Wahrheit entsprechen! Auch auf kleine Mängel oder sonstige Schönheitsfehler musst du aufmerksam machen, das sichert dich ebenfalls ab. Sonst kann das Geschäft nämlich angefochten werden und die erhaltenen Leistungen müssen wieder zurückgestellt werden, d.h., du musst das erhaltene Geld zurückbezahlen, bekommst aber auch deine Sache wieder.



ABER ACHTUNG

WENN DU REGELMÄSSIG SACHEN VERSTEIGERST UND DU DIE ABSICHT HAST, DARAUS AUCH „GEWINNE“ ZU ERZIELEN, KANN DAS BALD ALS „GEWERBLICH“ EINGESTUFT WERDEN. Du müsstest in so einem Falle dann einen Gewerbeschein beantragen. Deine Tätigkeit musst du auch beim Finanzamt melden, wenn du Einkünfte über EUR 730,- pro Jahr aus solchen Versteigerungen erzielst! Weiters kann in diesem Falle die Gewährleistung **NICHT** ausgeschlossen werden, d.h., du musst für allfällige Mängel an den von dir verkauften Sachen einstehen. Es stellt sich hier natürlich die Frage, was unter „gewöhnlich vorausgesetzten Eigenschaften“ bei Gebrauchtwaren zu verstehen ist.

E-MAIL & SPAM

E-Mail war eine der ersten Anwendungen im Internet und ist bis heute auch eine der wichtigsten. In letzter Zeit häufen sich allerdings verschiedenste Sicherheitsprobleme. Hier eine kurze Übersicht, worauf man aufpassen sollte:

1. VERSCHICKEN VON MAILS

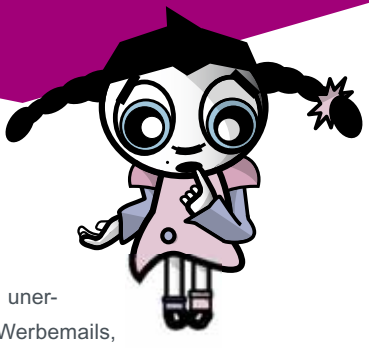
In den Anfangstagen des Netzes wurden Neulinge immer darauf hingewiesen, doch erst die Netiquette zu lesen, bevor sie ein E-Mail versenden oder in einer Newsgroup mitdiskutieren. In dieser Sammlung von Benimmregeln stand unter anderem noch zu lesen, dass man keine Umlaute verwenden soll, denn viele Empfänger/innen können diese nicht darstellen. So streng sind die Regeln heute zum Glück nicht mehr, trotzdem kann man sich 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 Empfänger/in vorgewarnt wurde. Es ist ganz schlechter Stil, ein leeres Mail zu versenden und den Text in eine angehängte Word-Datei zu packen.

HTML-MAILS (Nachrichten mit Bildern, Farben, verschiedenen Schriftstilen etc.) können heutzutage 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 (zum Beispiel bei einer schön gestalteten Einladung), ansonsten ist normaler Text ausreichend. Niemand benötigt zum Verständnis der Nachricht „Ich komme heute etwas später“ einen Blümchenhintergrund aus dem Outlook-Repertoire, solche 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 ihr Mail.

Mails an viele verschiedene Empfänger/innen sollten als **BCC** (Blind Carbon Copy) verschickt werden. Diese Einstellung bewirkt, dass die Empfänger/innen untereinander nicht sehen, wer das Mail noch bekommen hat. Dadurch wird die Vertraulichkeit der E-Mail-Adressen gewahrt, außerdem werden die Mails kleiner und sehen professioneller aus.

E-MAIL & SPAM



2. WAS TUN MIT SPAM?

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

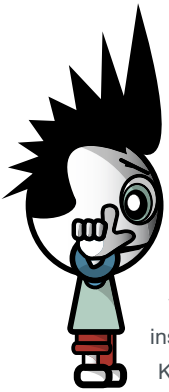
Eine Zusendung von Werbemails an Private ist ohne vorherige Einwilligung des Adressaten nicht erlaubt, ebenso Zusendungen an mehr als 50 Personen, deren Einwilligung nicht vorliegt.

Erlaubt wäre eine Zusendung von Werbemails in folgendem Fall: Du hast deine Mailadresse bei einer Bestellung dem Vertragspartner bekannt gegeben und hast bei der Bestellung Gelegenheit gehabt, die Zusendung von Werbemails abzulehnen (z.B. Ankreuzen eines Kästchens mit dem Text „Ich wünsche keine weiteren Informationen per E-Mail“). In der einzelnen Werbemail darf der Absender aber nur eigene Produkte bewerben und muss dir die Gelegenheit geben, weitere Werbemails abzulehnen.

Erhältst du unerlaubte Werbemails, könntest du gegen den Absender Anzeige beim Fernmeldebüro erstatten. Der Absender muss dann Strafe bezahlen. Dies wird aber bei Zusendung von Werbemails aus dem Ausland kaum ein zielführendes Mittel sein. In diesem Fall ist auch eher davon abzuraten, ein Mail mit einer Ablehnungserklärung („remove me!“) zurückzusenden. Oft bekommt man nur noch mehr Spam, wenn man auf Spam reagiert (wenn auch ablehnend). Die Spam-Versender wissen dann nämlich, dass deine E-Mail-Adresse auch wirklich gültig ist.

Wenn du bereits Spam erhältst, kannst du also kaum etwas dagegen tun. Informiere dich auf der Webseite deines E-Mail-Providers, ob dieser einen Spamfilter anbietet und ob dieser von dir konfiguriert werden kann oder überhaupt erst aktiviert werden muss. Auch die meisten E-Mail Programme bieten heutzutage mehr oder minder effiziente Spamfilter.

E-MAIL & SPAM



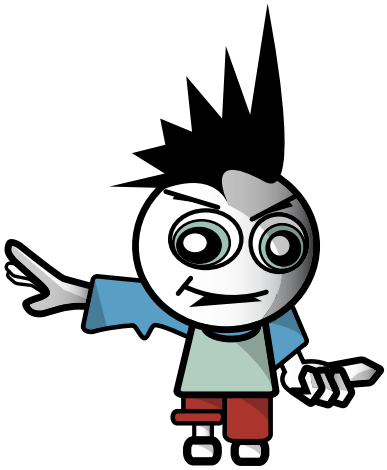
Du kannst aber einiges tun, um nicht in Zukunft noch mehr Spam zu erhalten. **DIE EINFACHSTE REGEL IST, IMMER (MINDESTENS) ZWEI E-MAIL-ADRESSEN ZU VERWENDEN:** eine, um mit Freunden, Bekannten und Familienmitgliedern Mails auszutauschen, und eine, um sich damit auf Webseiten zu registrieren, in Gästebücher zu posten oder in Foren mitzudiskutieren. Die erste Adresse bleibt höchstwahrscheinlich 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!, MSN Hotmail oder GMX.

Weiters besteht auch die Möglichkeit, sich in die sogenannte **„ROBINSONLISTE“** einzutragen. Das ist eine Liste von Personen, die eine Zusendung von Werbemails ausdrücklich nicht wünschen. Eine „Robinsonliste“ wird in Österreich von der Rundfunk und Telekom Regulierungs-GmbH (RTR) geführt. Auf der Homepage der RTR gibt es nähere Infos, wie du dich in die Liste eintragen kannst, sowie das ausführliche Spam-Infoblatt zum kostenlosen Download (http://www.rtr.at).

E-MAIL & SPAM

3. DARF ICH SELBST SPAM VERSENDEN?

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



VIREN

VIREN UND TROJANER SIND IN ALLER MUNDE

Mailserver brechen zusammen, Webseiten sind nicht erreichbar und das Internet generell über Tage hinweg nur mäßig brauchbar. Die neueste Generation von Viren (und, korrekt ausgedrückt, Trojanern) schadet nicht mehr (ausschließlich) demjenigen, der den Virus hat. Frühere Virengenerationen löschten einfach die Festplatte oder gewisse Arten von Files auf dem verseuchten Rechner. Vieles deutet aber heute darauf hin, dass hinter den aktuellen Viren handfeste ökonomische Interessen stecken: Die Virenschreiber scheinen einerseits E-Mail-Adressen zu sammeln (die auf den verseuchten Computern zu finden sind), andererseits werden diese Computer als Zombies missbraucht, über die dann später Spams versendet werden können (so genannte „Open Relays“). Viele andere Missbrauchsmöglichkeiten sind denkbar und können, nachdem die befallenen Rechner für Hacker/innen völlig offen sind, jederzeit inszeniert werden. Die nachstehenden Ausführungen sind nur für jene interessant, die aktuelle Microsoft Windows-Betriebssysteme verwenden. Benutzer/innen von Linux, Mac OS oder anderen Betriebssystemen sind vergleichsweise sicher, da kaum Viren im Umlauf sind, die diesen Computern schaden können.

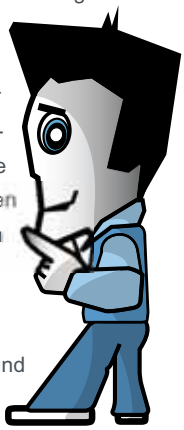
MEIN COMPUTER HAT EINEN VIRUS! WIE WERDE ICH IHN WIEDER LOS?

Zunächst musst du feststellen, ob du wirklich einen Virus hast. Dabei hilft dir ein Antivirus-Programm mit aktuellen Virusinformationen („Virus-Definitions“). Solltest du kein solches Programm besitzen oder es bereits zu alt sein, so ist es in jedem Fall eine gute Idee, dir eines zu besorgen. Weitere Informationen, Hilfestellungen und nützliche Links zum Thema Viren und den verschiedenen Antiviren-Programmen erhältst du auf der Webseite von Saferinternet.at.

VIREN

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. Insbesondere Dateien mit den Endungen .vbs, .bat, .com, .cmd, .exe, .pif, .scr und neuerdings auch .zip sind in jedem Fall verdächtig.



Solche Attachments können auch durchaus von bekannten Absendern stammen, da sich viele Viren über die Adressbücher der befallenen Rechner selbständig weiterversenden. Dreh auch unbedingt im Browser und im E-Mail-Programm sowie im ZIP-Programm die Voreinstellung ab, dass heruntergeladene Dateien sofort ausgeführt werden. Solltest du nämlich doch versehentlich einen Virus auf deiner Festplatte haben, so kann er erst aktiv werden, wenn du ihn einmal aufgerufen hast.

Viele Viren nutzen auch Eigenheiten und Sicherheitslücken in Microsofts „Outlook“-Mailprogramm aus. Alternative (und kostenlose!) Mailprogramme, wie zum Beispiel Thunderbird von Mozilla oder Eudora sind etwas sicherer, schützen aber auch nicht vor der Dummheit mancher Benutzer/innen.

Generell ist es eine gute Idee, immer sofort die neuesten Updates des verwendeten Mailprogrammes, Browsers, Betriebssystems sowie der Antiviren-Software einzuspielen. Dies mag zwar aufwändig sein, neueste Virengenerationen blockieren aber die Updatefunktionen dieser Programme und sind dann umso schwerer wieder loszuwerden.

TAUSCHBÖRSEN (FILE-SHARING-NETZWERKE)

EBENSO BELIEBT WIE UMSTRITTEN SIND ONLINE-TAUSCHBÖRSEN, WO MAN MUSIK, VIDEOS ODER AUCH PROGRAMME TAUSCHEN KANN.

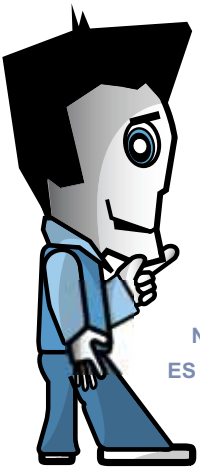
Millionen User/innen verwenden täglich Kazaa, Limewire oder ähnliche Programme. Derartige Tauschbörsen verletzen in der Regel das Urheberrecht der Schöpfer/innen der getauschten Werke.

Ein Werk ist eine individuelle geistige Schöpfung im Bereich der Musik, der Literatur, der bildenden Kunst oder der Filmkunst. Diese Schöpfung muss sich vom Alltäglichen abheben. Computerprogramme gelten nach österreichischem Urheberrecht als Sprachwerke, also als Werke der Literatur. Auch Computerspiele sind als Programme und damit als Sprachwerke anzusehen.

Der/die Urheber/in hat das alleinige Recht, sein/ihr Werk öffentlich zugänglich zu machen, zu vervielfältigen, zu verbreiten, zu senden, zu verleihen und aufzuführen. Im Zusammenhang mit Tauschbörsen und auch Homepages sind vor allem zwei Rechte berührt: **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 Musik aus dem Internet (also ohne das Musikstück selbst wieder anbieten zu wollen) erlaubt ist, ist unter Jurist/innen umstritten. Die einen sehen darin eine erlaubte Vervielfältigung zum eigenen Gebrauch, die anderen meinen, auch diese Vervielfältigung zum eigenen Gebrauch sei nicht erlaubt, wenn bereits die Vorlage selbst unrechtmäßig hergestellt 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 den Peer-to-Peer-Tauschbörsen fast nie vor.

Es gibt aber auch Portale, in 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 mp3-Plattformen großer Anbieter kannst du davon ausgehen, dass die Angebote legal sind.

Eine weitere Möglichkeit, kostenlos und legal zu guter Musik zu kommen ist übrigens das Mitschneiden von Online-Radiostationen mit dafür geeigneten Programmen (zum Beispiel dem „Quintessential Player“ oder dem Programm „Audio Jack“ für Windows). Diese Programme speichern jedes Lied, das auf einem der von dir ausgewählten Sender gespielt wird, in einer eigenen Datei ab. Du kannst später dann aussortieren, was du davon behalten willst und was nicht. Selbstverständlich ist es nicht erlaubt, diese Files dann auf Tauschbörsen anzubieten.

TAUSCHBÖRSEN (FILE-SHARING-NETZWERKE)

DARF ICH MUSIK ODER VIDEOS ZUM DOWNLOAD ANBIETEN?

Wie gesagt, manche Jurist/innen sind der Ansicht, dass der reine Download von Musik und Videos erlaubt ist. Anzumerken ist jedoch, dass Tauschbörsen in der Regel möglichst viele Dateien anbieten. Deswegen werden oft User/innen mit großem Angebot beim Download bevorzugt, während jemand, der nichts anbietet, auch nichts bekommt. Besondere Vorsicht ist übrigens auch bei Film- oder Programmdownloads über Bittorrent geboten: Sobald man selbst anfängt, eine Datei herunterzuladen, können andere ebenfalls auf diese Datei zugreifen und diese wiederum von Deinem Computer laden: Auch wenn Du selbst erst Bruchstücke eines Filmes auf der Festplatte hast, du bist 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. Eine Vervielfältigung zum Eigengebrauch scheidet somit aus. Das Anbieten von Musikstücken (oder auch Videos oder Programmen) in Tauschbörsen ohne die Zustimmung des Urhebers/der Urheberin ist nicht erlaubt. Mittlerweile werden auch in Österreich User/innen geklagt, wenn sie urheberrechtlich geschützte Werke zum Download zur Verfügung stellen. Meistens enden diese Verfahren mit einem Vergleich, der die Zahlung einiger tausend Euro beinhaltet. Filesharing kann also ein ziemlich teures Vergnügen werden!

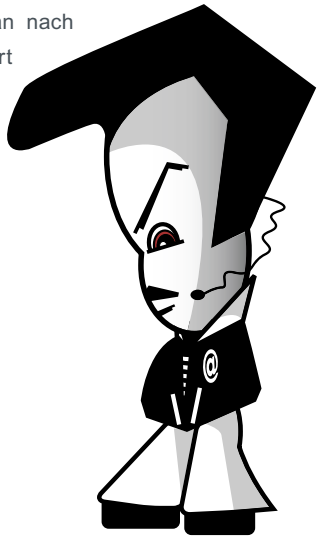
KANN MAN MICH ÜBERHAUPT ERWISCHEN?

Ja, und zwar ganz einfach über die IP-Adresse deines Computers und den Zeitpunkt, zu dem du mit dem Programm online warst. Es genügt ein einfacher Gerichtsbeschluß, mit dem dein Provider gezwungen wird, deine Daten herauszugeben. Innerhalb kurzer Zeit bekommst du dann unangenehme Post...

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 Urheber/in 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 Urhebers/der Urheberin downzuloaden, die man nach einiger Zeit (z.B. 30 Tagen) bezahlen oder – wenn dies nicht passiert – vom PC löschen muss. Das Besorgen von Entsperrcodes für solche Demoversionen (in einschlägigen Foren) ist natürlich auch illegal.



DEINE HOMEPAGE & DEIN BLOG

Viele Leute haben heutzutage schon eine private Homepage oder ein Blog (auch Online-Tagebuch oder Weblog geannnt) mit vorgegebenen oder selbst erstellten Layouts und vielleicht sogar mit einer eigenen Internetadresse (Domain). Varianten gibt es viele, Möglichkeiten, in Schwierigkeiten zu geraten, auch.

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

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

Auch Fotos sind – wie Musikstücke und Programme – urheberrechtlich geschützt. Wenn du ein fremdes Foto auf deine Homepage stellen willst, kannst du dies daher nur mit Zustimmung des Herstellers (und zwar nur dann!) tun.

Es ist also keine gute Idee, ein x-beliebiges Bild eines bekannten Stars auf deine Homepage zu stellen, auch keinen Cartoon von Bart Simpson. Allerdings gibt es gerade auch von bekannten Persönlichkeiten oder Fernsehserien meistens Pressefotos, die zur Veröffentlichung freigegeben wurden. Diese findest du oft auf den offiziellen Webseiten. Bitte beachte aber die dortigen Hinweise, z.B. über die Nennung des Fotografen in einer Bildunterschrift (sollte man ohnehin immer tun, gehört zum guten Ton). Sehr riskant ist es, Musikstücke zur Untermalung einer Website zu verwenden. Ein Verstoß gegen das Urheberrecht besteht schon dann, wenn jedem das Musikstück unabhängig von Zeit oder Ort zugänglich ist. Dies völlig unabhängig davon, ob die Musikdatei downzuloaden ist oder ob die Musik vereinfacht wiedergegeben wird, z.B. in einer MIDI-Datei oder als Handy Klingelton.

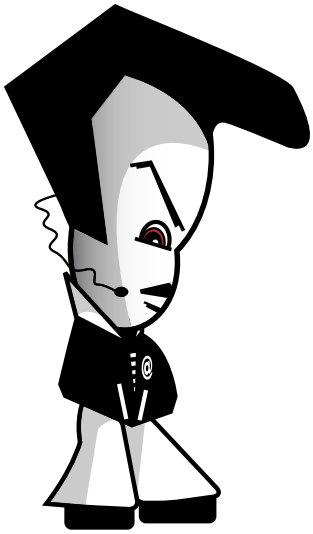
Hältst du die Verwendung von bestimmten Musikstücken dennoch für unumgänglich und möchtest rechtlich korrekt vorgehen, kannst du dich zum Erwerb der nötigen Rechte an die AKM (Gesellschaft der Autoren, Komponisten, Musikverleger) wenden. Diese sorgt für die Wahrnehmung von Urheberrechten im Bereich der öffentlichen Zurverfügungstellung, Aufführung und Sendung von Musik. Dies tut sie einerseits durch Gewährung von Lizenzen, anderseits aber auch durch Kontrollen und Klagen bei Verstößen.

DEINE HOMEPAGE & DEIN BLOG

DARF ICH SELBST GESCHOSSENE BILDER VON ANDEREN PERSONEN AUF MEINER HOMEPAGE/ MEINEM BLOG VERWENDEN?

Du machst auf einer Party zu fortgeschrittener Stunde Bilder von verschiedenen Personen und veröffentlichst diese auf deiner Homepage. In nüchternem Zustand ist diesen Personen die Veröffentlichung der Bilder 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.

Jede Veröffentlichung, die an sich oder in Verbindung mit dem Begleittext geeignet ist, die berechtigten Interessen des Abgebildeten zu verletzen, ist unzulässig. Aufnahmen an öffentlichen Plätzen sind üblicherweise unbedenklich, wenn aber der Kontext 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 die Interessen noch viel früher beeinträchtigt, dies gilt auch für private geschlossene Veranstaltungen (Partys bei dir oder bei Freund/innen). Veröffentlichte Bilder dürfen die Abgebildeten nicht bloßstellen oder herabsetzen, dies kann bei Bildern von Party Exzessen häufig der Fall sein.



Um gegen dich vorgehen zu können, reicht es aber nicht, wenn jemand meint, er würde auf einem Bild hässlich aussehen. Eine Bloßstellung muss objektiv nachvollziehbar sein (z.B. heruntergelassene Hose im Vollrausch). Die Einwilligung der abgebildeten Personen zur Veröffentlichung (sofern diese in unserem Beispiel noch zurechnungsfähig sind) erspart sicherlich Schwierigkeiten und erlaubt dir, auch diskret auf die Existenz deiner Homepage oder deinen Blog aufmerksam zu machen.

DEINE HOMEPAGE & DEIN BLOG

ICH WILL MEINE EIGENE DOMAIN!

Du willst eine eigene Homepage erstellen. Die Darstellung deiner Person ist dir sehr wichtig, daher sollen möglichst viele Leute deine Homepage besuchen. Du verwendest also eine berühmte Automarke als Domain, die zufälligerweise als „.at"-Domain (www.automarke.at) frei ist. Dies ist keine gute Idee, denn der Inhaber der Marke wird dir innerhalb kürzester Zeit einen Anwaltsbrief schicken lassen, in dem du zur Löschung der Domain aufgefordert wirst. Du kannst dir durch eine einfache Websuche einen Überblick verschaffen, ob du mit deinem Namenswunsch jemandem in die Quere kommen könntest. Kleiner Tipp am Rande: Wenn du dir nicht sicher bist, dann lass es lieber bleiben. Große Firmen beschäftigen oft auch die besten Anwälte und derartige Verfahren haben oft einen schwer vorhersagbaren Ausgang. **AM SICHERSTEN IST ES, WENN DU DEINEN EIGENEN NAMEN ALS DOMAIN ANMELDEST (Z.B. KARLI-MEIER.AT) ODER DIR EINEN FANTASIENAMEN SUCHST, DEN GARANTIERT NOCH NIEMAND ANDERER HAT.** „.at" Domains kannst du übrigens bei deinem Provider anmelden (eine Liste findest du auf der ISPA-Webseite). Die meisten Provider haben auch eine Abfragemöglichkeit, mit der du feststellen kannst, ob der gewünschte Domainname noch frei ist.

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 fremden Site nicht auffallen musste (dies wird bei Kinderpornografie eher der Fall sein, als bei einer unerlaubten Verwendung von Bildern). Bemerkst du aber, dass du einen Link auf eine illegale Website gesetzt hast, und willst nicht mitverantwortlich sein, musst du den Link sofort von deiner Homepage bzw. deinem Blog entfernen. Der bloße Hinweis, dass du für fremde Inhalte nicht

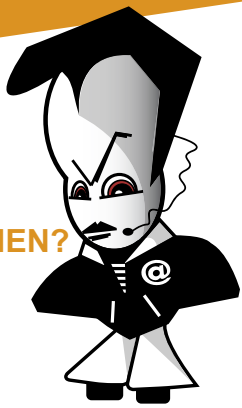
DEINE HOMEPAGE & DEIN BLOG

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 mitteilt, dass die von dir verlinkte Seite illegale Inhalte verbreitet (z.B. Neonazi-Propaganda), dann solltest du den Link sofort löschen!

DARF ICH FREMDE SEITEN IN MEINEN FRAME LINKEN?

Du gestaltest eine eigene Homepage und bietest auch eine umfangreiche Linksammlung diverser Sites an. Damit die Besucher/innen deiner Homepage einfach zu deinen eigenen Inhalten zurückwechseln können, lässt du die fremden Sites im Frame deiner Homepage öffnen. Grundsätzlich ist es erlaubt, einen Link auf eine fremde Website zu setzen. In der Verlinkung diverser Websites liegt ja das Wesen des Internets. **AUFPASSEN MUSS MAN ABER, DASS MAN NICHT EINE FREMDE WEBSITE ALS SEINE EIGENE SCHÖPFUNG VEREINNAHMT ODER GAR AUF ILLEGALE SEITEN VERLINKT.** Wenn du eine Homepage unter Verwendung von Frames machst, hast du bei der Linksetzung keine Probleme zu erwarten, wenn du die gelinkte Seite in einem neuen Fenster öffnen lässt oder zumindest den eigenen „Rahmen sprengst“. Lässt du eine fremde Seite im eigenen Frame öffnen und findet sich auf der fremden Seite immerhin ein Hinweis, dass jemand anderes der Urheber ist (z.B. ein Copyright-Vermerk mit Link auf die Homepage des Urhebers), sollte sich für dich kein Problem ergeben.

DEINE HOMEPAGE & DEIN BLOG



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

Auch für eine private Homepage oder einen Blog besteht in Österreich ab 1.7.2005 eine sogenannte Offenlegungspflicht nach dem Mediengesetz. Danach musst du deinen Namen und Wohnort (nicht aber die genaue Adresse) ständig leicht und unmittelbar auffindbar zur Verfügung stellen. Die sonst noch vorgeschriebene Angabe des Unternehmensgegenstandes wird dich wohl kaum treffen.

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 DEINE HOMEPAGE ODER DEIN BLOG AUCH EINEN KOMMERZIELLEN ZWECK VERFOLGT, MUSS DER/DIE INHABER/IN EIN LEICHT SICHTBARES IMPRESSUM MIT DEN WICHTIGSTEN KONTAKTINFORMATIONEN SCHALTEN.

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 dann bis zu EUR 3.000,- kosten. Ob eine Website schon kommerziell ist, wenn fremde Werbebanner geschaltet werden, ist umstritten. Nimmst du Geld für die Schaltung von Werbebannern, ist ein Impressum sicher empfehlenswert.

DEINE HOMEPAGE & DEIN BLOG

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

+ Namen 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.
Das Vorhandensein dieser Angaben ist aber ein Zeichen für die Seriosität des/der Inhabers/Inhaberin einer Website:
+ Firmenbuchnummer und Firmenbuchgericht (haben nur größere Unternehmen);
+ Umsatzsteuer-Identifikationsnummer (haben nur Unternehmer).
Wenn die Tätigkeit einer behördlichen Aufsicht unterliegt, müssen weiters die zuständige Aufsichtsbehörde und die Zugehörigkeit zu einer Kammer oder einem Berufsverband angegeben werden.

MUSS ICH SONST NOCH ETWAS BEACHTEN?

Als Betreiber einer Homepage oder eines Blogs bist du ab 1.7.2005 Medieninhaber, wodurch dich eine Flut von möglichen Ansprüchen und Pflichten trifft. Die wichtigste Pflicht ist – neben der oben genannten Offenlegung deines Namens und Wohnortes – auch die **KENNZEICHNUNGSPFLICHT FÜR FREMDE WERBEBANNER, WENN DU DAFÜR GELD BEKOMMST.** Es können von dir aber auch Entschädigungsbeträge (bis zu EUR 50.000,-) gefordert werden, wenn auf deiner Webseite von dir oder Dritten z.B. als Folge eines Hacker-Angriffs rechtswidrige Handlungen gesetzt werden, wie etwa Ehrenbeleidigung, Verspottung oder Verleumdung. Für diese Handlungen müsstest du als Webseiten-Betreiber, nunmehr Medieninhaber, den Kopf hinhalten. In so einem Fall wärest du auch zur Veröffentlichung einer Gegendarstellung oder eines Urteils verpflichtet und es könnte deine Webseite im schlimmsten Fall sogar gelöscht werden. Auch wenn man auf deiner Homepage Beiträge z.B. in einem Gästebuch posten kann, bist du für den Inhalt dieser Beiträge verantwortlich, wenn du die gebotene Sorgfalt außer Acht lässt, also solche inkriminierenden Beiträge nicht so rasch wie möglich entfernst.

CYBERCRIME

Was ist im Netz erlaubt und was nicht?

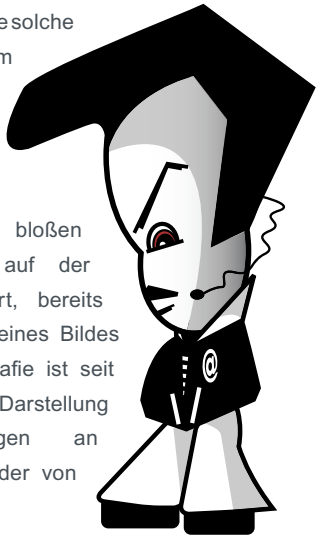
Wie schon gesagt, im Großen und Ganzen ist es so wie im wirklichen Leben – was dort verboten ist, ist im Internet auch illegal. Um dir einen Überblick zu geben, haben wir hier ein paar wichtige Punkte zusammengefasst:

AB WELCHEM ALTER KANN MAN SICH STRAFBAR MACHEN?

Du sagst „Ich bin eh erst 14, mir kann nix passieren“. Ist das richtig? Wenn du das 14. Lebensjahr vollendet hast, kannst du für strafbare Handlungen zur Verantwortung gezogen werden. Bis zur Vollendung des 18. Lebensjahrs gilt allerdings das Jugendstrafrecht, welches geringere Strafausmaße (meist die Hälfte der Erwachsenenstrafen) vorsieht.

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 Seitenbetreiber 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 bereits der Besitz strafbar. Besitz liegt dann vor, wenn eine solche Darstellung auf dem eigenen Computer gespeichert wird. In der Regel werden die Elemente einer Website schon beim bloßen Ansehen temporär auf der Festplatte gespeichert, bereits das kann als Besitz eines Bildes gelten. Kinderpornografie ist seit Mai 2004 auch die Darstellung sexueller Handlungen an Personen unter 18 oder von



CYBERCRIME

Personen unter 18 an sich selbst, an anderen oder an Tieren, sofern es sich um reißerische Darstellungen („harte Pornografie“) handelt. Pornografische Darstellungen mit Kindern unter 14 sind immer unzulässig. Es reicht bereits der Eindruck, dass es zu einer solchen Handlung gekommen ist (z.B. eine Fotomontage). Beim bloßen 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 ein Kinderpornovideo über eine Tauschbörse herunterlädt und dieses Video anderen zum Download bereitstellt, fällt unter den höheren Strafsatz.

ABER HALT, natürlich ist es nicht strafbar, wenn du mit deinem Freund oder deiner Freundin Fotos zum eigenen Gebrauch anfertigst. Das Gesetz sieht die Straflosigkeit vor, wenn der Altersunterschied der Beteiligten nicht mehr als vier Jahre beträgt. Der Gesetzgeber will sich nicht in euer privates Leben einmischen. Aber: Die Weitergabe der Bilder an andere als die Beteiligten ist nicht nur unfair, es wäre auch strafbar! Wenn du auf Kinderpornografie im Internet aufmerksam wirst, kannst du dich anonym an www.stopline.at (eine Einrichtung der Internet-Provider) wenden.

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 Jahre Haft. Noch empfindlichere Strafen gibt es für die Gründung von nationalsozialistischen Verbindungen, das Anwerben von Mitgliedern für eine solche Verbindung oder auch nur für die Beteiligung daran. Diese Handlungen sind alle auch unter Verwendung des Internets möglich.

CYBERCRIME

ONLINE-BETRUG

Du ersteigerst bei einer Online-Auktion einen PC. Der Verkäufer streift den Kaufpreis ein, obwohl der PC gar nicht existiert oder er ihn dir jedenfalls nicht zuschickt. Ein Betrug liegt dann vor, wenn jemand einen anderen täuscht, um so einen Vermögensvorteil zu bekommen. Für dich wird in einem solchen Fall natürlich die Frage bedeutsamer sein, ob und wie du das Produkt doch noch bekommen kannst oder wie du dein Geld zurückbekommst. Die Drohung mit einer Strafanzeige kann hier aber durchaus ein Druckmittel sein. Es liegt aber nicht automatisch ein Betrug vor, wenn man eine Sache nicht geliefert bekommt. Entscheidend ist, dass der Verkäufer von vornherein weiß, dass er gar nicht liefern kann/will und trotzdem abkassiert. Wenn du ein Opfer eines Online-Betrügers geworden bist, kann dir unter Umständen der Internet Ombudsmann (www.ombudsmann.at) weiterhelfen.

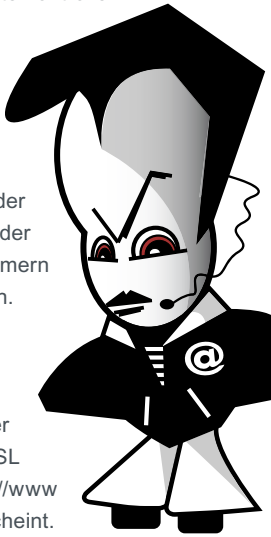
"PHISHING"

Eine besondere Form des Online-Betrugs ist das sogenannte „Phishing". Dabei versuchen Kriminelle mittels gefälschter Websites und E-Mails die Passwörter von Internet-Benutzern für Online-Konten, eBay- oder PayPal-Accounts oder Ähnliches herauszufinden. Der User erhält meist ein täuschend echtes E-Mail, mit dem er oder sie aufgefordert wird, auf einen Link zu klicken und sich in seinen Account einzuloggen, beispielsweise um dort die Userdaten zu aktualisieren. Die Website, auf die der Link verweist ist aber ebenfalls gefälscht und wenn man sich dort versucht einzuloggen, teilt man den Betrügern seine Accountdaten mit. Innerhalb kürzester Zeit ist dann beispielsweise das Online-Konto leergeräumt.

CYBERCRIME

Nachdem die Fälschungen oft täuschend echt sind, solltest du besonders sensibel mit deinen Accountdaten umgehen. Dazu noch ein paar Tipps:

- ✓ Frag' dich zuerst, ob die Bekanntgabe der gewünschten Daten Sinn macht.
- ✓ Es gehört NICHT zum üblichen Verfahren von Banken, Onlineshops, Auktionshäusern oder ähnlichem, sensible Daten der Nutzer via E-Mail abzufragen!
- ✓ Ignoriere E-Mails, in denen du zur Preisgabe deiner Daten und Passwörter aufgefordert wirst, auch wenn dir der angezeigte Absender bekannt ist. Meist strotzen solche betrügerischen E-Mails vor Rechtschreib- und Grammatikfehlern, um durch die Spamfilterkontrolle zu gelangen.



- ✓ Oft hilft auch nur ein Anruf bei der Hotline des jeweiligen Dienstleisters um herauszufinden, ob das E-Mail legitim ist oder nicht. Meist ist es das nicht...
- ✓ Persönliche Daten oder Accountinformationen solltest du weder im Chat oder Messenger-Service bekannt geben noch per E-Mail versenden. Bei der Passwortwahl vermeide leicht zu erratende Kennwörter, wie regelmäßige oder bekannte Zahlen (z.B. 12345, 4711, 0815) ebenso Geburtstage, Telefonnummern oder Ähnliches. Am besten ist eine Kombination von Buchstaben und Zahlen.
- ✓ Deine Passwörter solltest du – wenn möglich – auch regelmäßig ändern.
- ✓ Achte bei der Eingabe deiner Daten immer darauf, dass diese über eine SSL-verschlüsselte Internetseite eingegeben werden. Die SSL Verschlüsselung erkennst du daran, dass die Webseite mit https://www beginnt und im Browser das Schlosssymbol als geschlossen aufscheint. SÄMTLICHE Onlinetransaktionen bei Banken werden über solche verschlüsselten Verbindungen abgewickelt.
- ✓ Solltest du dennoch einmal eine zweifelhafte Internetseite besucht und deine Daten preisgegeben haben, ändere sofort dein Passwort und veranlasse die Sperre der TANs bei deinem Onlinebankkonto.

CYBERCRIME

Viele der aktuellsten Internetbrowser haben bereits einen Phishingfilter integriert.
Es gibt auch bestimmte Toolbars, die kostenlos downgeloaded werden können (z.B. bei eBay), die einen gewissen Schutz vor betrügerischen Websites bieten.

VIRENPROGRAMME

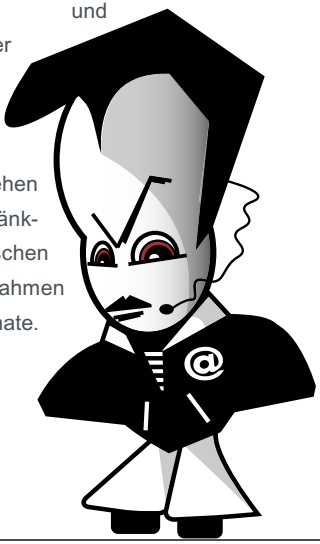
Du erhältst ein Virenprogramm als Mail-Attachment, welches deine Festplatte löscht. Das fällt unter Datenbeschädigung. Allerdings nur, wenn der Absender das Löschen beabsichtigt hat.

Versendet sich das Virenprogramm vor dem Löschen noch automatisch an alle Kontaktadressen in deinem Mail-Programm und löscht auch die Festplatten deiner Freund/innen, bist du nicht strafbar.

Der Strafrahmen beträgt bis zu 6 Monate, kann sich aber bei größeren Schäden erhöhen.

HACKING

Auch das unerlaubte Eindringen in fremde Computersysteme kann strafbar sein. Voraussetzung ist, dass Sicherheitsvorkehrungen des Systems verletzt werden. Weiters ist Hacking nur dann gerichtlich strafbar, wenn sich der Täter oder die Täterin einen Vermögensvorteil verschaffen, oder den Betreiber des Systems schädigen will (Auskundschaften und Verkauf von Betriebsgeheimnissen, Löschen der Festplatte). Auch die schwere Störung eines fremden Computernetzwerkes (DOS-Attacke, Eindringen und/oder Verändern der Daten) ist als Datenbeschädigung und Störung der Funktionsfähigkeit eines Systems strafbar. Strafbar ist weiters das Umgehen von Zugangsbeschränkungen oder technischen Sperren. Der Strafrahmen beträgt bis zu 6 Monate.



CYBERCRIME

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 gleichfalls verboten. Sowohl im Strafgesetzbuch als auch im Telekommunikationsgesetz gibt es weitere Strafbestimmungen, die es verbieten, fremde E-Mails zu lesen oder sonst Daten über fremden Telekommunikationsverkehr anzusehen oder weiterzugeben. Auch im Internet gilt: Fremde Briefe und fremde Aktenschränke öffnet man/frau nicht ohne Erlaubnis.

WEB 2.0 & COMMUNITYS

DISKUSSIONSFOREN, CHATS UND SOCIAL NETWORKS

Für viele User/innen sind Chats und Social Networks die „Einstiegsdroge“ ins Internet und gewissermaßen die Seele des Netzes. Hier kann man sich einbringen, Infos austauschen, andere Identitäten annehmen und seinen Hobbys nachgehen.

Die Urform der Diskussionsforen sind die so genannten Usenet-Newsgroups, der Stammvater aller Chats ist das IRC-Netzwerk und die klassischen Listserver hören auf den Namen Majordomo. Bereits bei der Einführung dieser Kommunikationsformen (etwa Ende der achtziger Jahre) haben sich die Menschen Gedanken gemacht, wie man sich in so etwas verhalten soll. Diese Regeln gelten grundsätzlich auch heute noch:

Die wichtigste aller Regeln:
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 auf einem karibischen Strand, in einem Drei-Hauben-Restaurant anders als in einem Pub.

Genauso ist es auch im Netz: Schon länger bestehende Communitys haben oft eigene Benimm-Regeln erarbeitet (meist kann man die auch auf den zugehörigen Webseiten nachlesen), und wenn man sich als Neuling an diese nicht 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.

Regel Nummer zwei:
ERST DENKEN, DANN SCHREIBEN

Auf blöde Fragen bekommt man auch blöde Antworten. Alteingesessene Netizens wollen nicht ständig dieselben Fragen beantworten, deshalb haben Communitys oft eine FAQ online.

WEB 2.0 & COMMUNITYS

Regel Nummer drei:
NIE MIT WUT IM BAUCH SCHREIBEN

Nachfolgende rechtliche Tipps könnten wir uns größtenteils sparen, wenn jeder, der auf jemand anderen wütend ist, zunächst einen Tag wartet, bevor er oder sie ein Posting oder einen Chat-Beitrag loslässt. Die daraus bisweilen entstehenden Flame-Wars sind zwar am Anfang (zumindest für Außenstehende) ganz unterhaltsam, enden aber meist mit dem ultimativen Argument („Du Faschist!“) und bisweilen auch vor dem Bezirksrichter. Bedenke bitte immer, dass du erstens in Diskussionsforen nicht anonym bist (siehe Seite 7) und zweitens nicht nur dein/deine Gegner/in mitliest, sondern, im Unterschied zu persönlichen E-Mails, auch eine Menge anderer Leute. Und drittens verschwinden Postings in Diskussionsforen oft nicht mehr so schnell, sie bleiben über Jahre im Netz und können von Search-Engines gefunden werden.

Welche Möglichkeiten habe ich also, mich in Communitys strafbar zu machen?

EHRENBELEIDIGUNG:

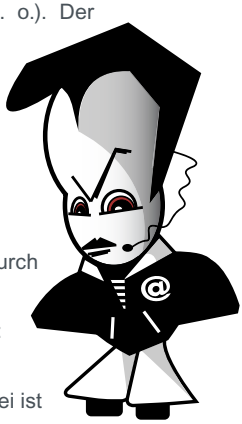
Beleidigt man eine Person unter Angabe ihres Namens von der eigenen Homepage aus, kann man sich leicht strafbar machen. Bei Foren und Chats ist das nicht so klar, da die User/innen ja meistens anonym bleiben und eine Beleidigung nicht einer realen Person zugeordnet werden kann. Vorsicht ist jedenfalls angebracht, wenn jemand seinen tatsächlichen Namen verwendet.

Manche sehen Beleidigungen jedoch schon als strafbar an, wenn der Beleidigte regelmäßig in einem Forum oder Chat unter dem gleichen Nicknamen (virtuelle Identität) auftritt und ihm durch Beleidigungen die Verwendung des Nicknamens verleidet wird. Gerade bei Foren und Chats ist es vom dort üblichen Umgangston abhängig, ab wann eine Ehrenbeleidigung vorliegt. Handelt es sich um Foren oder Chats, die überhaupt nur den Zweck haben, sich durch Austausch wüster Beschimpfungen abzureagieren, gilt wohl der Grundsatz „Teilnahme auf eigene Gefahr“. Unter den Begriff „Ehrenbeleidigung“ fallen Schimpfwörter und Spott in der Öffentlichkeit (z.B. „dämlich“, „bescheuert“).

WEB 2.0 & COMMUNITYS

Öffentlichkeit liegt dann vor, wenn die Handlung in Gegenwart von mehr als zwei weiteren Personen begangen wird und diese die Handlung wahrnehmen können. In Foren, Chats und auf Homepages kann man eigentlich immer von öffentlicher Begehung ausgehen.

Entschuldigt ist aber, wer sich zu einer Beleidigung hinreißen lässt, weil er sich über ein Verhalten des Beleidigten begreiflicherweise aufregt („hundsordinärer taktloser Rüpel"). Der „Gegenschlag" muss aber rasch nach dem Verhalten des Beleidigten erfolgen, dies ist vor allem bei Chats bedeutsam. Empfehlenswert ist diese Vorgangsweise aber trotzdem nicht (s. o.). Der Strafrahmen beträgt bis zu drei Monate, meist gibt es hier Geldstrafen.



ÜBLE NACHREDE:

Üble Nachrede ist der Vorwurf einer verächtlichen Eigenschaft oder Gesinnung oder eines unehrenhaften Verhaltens. Beispiele: „Jung-Nazi", „Faschist", „Rechtsextremist". Bei der üblen Nachrede reicht schon eine Wahrnehmbarkeit durch eine einzige dritte Person als Öffentlichkeit aus. Nicht strafbar ist eine wahre Behauptung, allerdings muss der Behauptende die Wahrheit beweisen. Beispiele: zutreffende Bezeichnung als „rechtsradikaler Pornojäger", „abgehalfterter Oberzuhälter" für einen vorbestraften Besitzer mehrerer Sexclubs. Straffrei ist auch das Zitat einer fremden Äußerung, solange man sich nicht mit dem Inhalt identifiziert („In der Zeitung hab ich gelesen, dass ..."). Die Strafe kann bis zu 6 Monate betragen, wird die üble Nachrede einer breiten Öffentlichkeit zugänglich (regelmäßig bei Begehung im Internet), 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 Betroffene eine behördliche Verfolgung (durch Polizei, Staatsanwalt) zu erwarten hat („Der X 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 5 Jahre betragen.

WEB 2.0 & COMMUNITYS

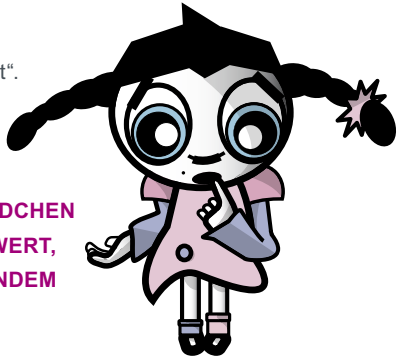
ILLEGALE FOREN UND CHATS:

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 Austausch von Adressen 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. Eine Adresse von Kinderpornoseiten zu posten, ist als Zugänglichmachen von Kinderpornografie strafbar (Strafrahmen zwei Jahre). Auch das Veröffentlichen einer Anleitung zur Herstellung von Drogen kann als Beihilfe zur Erzeugung strafbar sein (Strafrahmen 6 Monate). Weiters ist die Mitwirkung beim Selbstmord in Österreich strafbar. Es wäre denkbar, 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).

WIE SCHÜTZE ICH MICH UND MEINE DATEN?

Ähnlich wie bei der Partnersuche im Netz (siehe dort) ist es auch in Communitys angebracht, mit persönlichen Daten nicht allzu großzügig umzugehen. Einerseits ist es prinzipiell gut, sich vor professionellen Datensammlern zu schützen, darüber hinaus weiß man nie, welche Verrückten auf einer Plattform unterwegs sind. Daher gilt auch hier: Vorsicht ist die Mutter der Porzellankiste und richtige Namen, Wohnadressen, Telefonnummern etc. solltest du nur angeben, wenn du dir absolut sicher bist. In besonderem Maße gilt das auch für sogenannte „Social Networks" wie beispielsweise Friendster oder My Space. Dort wird man nicht nur eingeladen, sehr viel von sich selbst preizugeben, sondern auch, seine Freunde zu benennen und einzuladen. Im Zweifelsfall überleg' dir vorher nicht nur, ob du selbst das willst, sondern auch, ob deine Freunde das wollen!
NOCH EIN TIPP: Der Boom bei Communitys und Social Networks führte auch dazu, dass viele unseriöse Datensammler eigene Seiten eröffnet haben, die nur diesem Zweck dienen. Informiere dich am besten vor einer Registrierung (zum Beispiel mit einer Suche auf Google) ob diese Plattform seriös ist oder ob es viele Beschwerden darüber gibt.

PARTNERSUCHE



Partnersuche ist im Internet eine weit verbreitete „Sportart“. Oft trägt man sich nur aus Neugier oder zum Spaß auf Partnersuch-Seiten 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 ERSTMALS MIT JEMANDEM VERABREDET.**

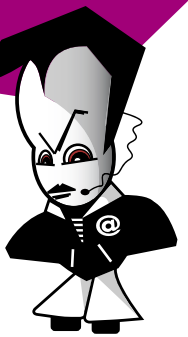
VORSICHT VOR BETRÜGERN!

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 Konversationen 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 erstmals mit jemandem verabredest, solltest du als Vorsichtsmaßnahme einen Erwachsenen oder einen Freund oder eine Freundin mitnehmen, dem oder der 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).

PARTNERSUCHE



PERSÖNLICHE DATEN

Es ist eine Grundregel im Netz, nur so viele persönliche Daten von sich zu veröffentlichen, wie unbedingt nötig. Das ist auf Partnersuch-Seiten 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, die nicht mit deinem Namen in Verbindung steht (z. B. von Yahoo!, MSN Hotmail oder GMX). Achte besonders darauf, dass dein Nick bzw. deine E-Mail-Adresse nicht mit deinem richtigen Namen in Verbindung zu bringen sind.

Ein Beispiel: Du registrierst dich auf einer Partnersuch Seite unter angel-for-u@gmx.at. Wenn man auf Google nach dieser Adresse sucht, findet man deine Homepage. Auf deiner Homepage 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 Partnersuch-Profil mit deinen realen Daten verknüpfbar – und das wirst du nicht wollen.

GLOSSAR

HIER EINE SAMMLUNG DER WICHTIGSTEN FACHBEGRIFFE, DIE IM TEXT VORKOMMEN.

ACCOUNT
Neudeutscher Ausdruck für „Benutzerkonto“. Allgemein gesprochen handelt es sich dabei um eine Berechtigung, die du benötigst, um irgendeine Art von Dienstleistung im Internet in Anspruch nehmen zu können.

ATTACHMENT
Eine an ein E-Mail angehängte Datei, beispielsweise ein Foto oder ein Programm. Auch Viren und Trojaner kommen meist als Attachments per Mail.

BCC
Verdeckte Adressierung von E-Mails („Blind Carbon Copy“, auf Deutsch etwa„ unsichtbarer Durchschlag“); wird verwendet, wenn die Empfänger/innen eines Mails nicht sehen sollen, wer das Mail sonst noch bekommen hat.

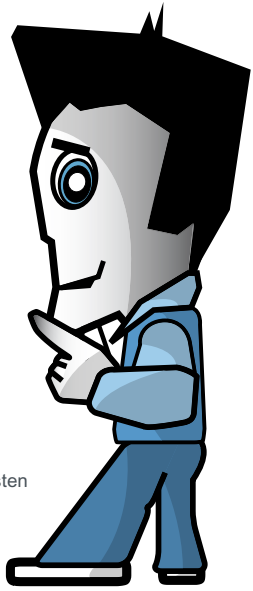
CHAT
Online-Tratsch, im Unterschied zu Diskussionsforen nicht zeitversetzt, sondern in Echtzeit.

COMMUNITY
Überbegriff für verschiedene Arten von Gemeinschaften, die sich im Internet gebildet haben. Eine Community ist dort, wo Menschen sich aufgrund von gemeinsamen Interessen zusammenfinden und sich über Diskussionsforen, Chats oder auch Linksammlungen, Datenbankeinträge etc. austauschen.

DOMAIN
Eine Domain ist ein „Namensraum“, den man bei dafür verantwortlichen Registrierungsstellen beantragen kann. Für die Vergabe der „Top-Level“-Domain „.at“ (die oberste Hierarchieebene) ist die Firma nic.at verantwortlich. Unterhalb einer Domain kann der/die Besitzer/in Namen von Services definieren, die auf verschiedene Rechner zeigen (z.B. ist www.xyz.at ein Rechnername der Domain xyz.at).

DOWNLOAD
Ein Download ist die Übertragung einer Datei von einem anderen auf den eigenen Rechner.

GLOSSAR



FAQ

„Frequently Asked Questions“, eine Zusammenstellung häufig gestellter Fragen zu einem Themenbereich oder zu einer Webseite.

FLAME-WAR

Aggressive Auseinandersetzung in einem Diskussionsforum, die meist in wüsten Beschimpfungen aller Beteiligten ausartet.

FRAMES

Frames sind eine besondere Art, Webseiten zu programmieren. Dabei wird die Seite in mehrere Bereiche aufgeteilt, die sich unabhängig voneinander ändern können.

HACKER/IN

Jemand, der sich – meist unbefugt – Zutritt zu anderer Leute Computer verschafft und es versteht, die Zugangssperren zu überwinden. „Hacking“ ist in Österreich in den meisten Fällen strafbar.

HEADER

Der „Kopf“ einer E-Mail, in dem verschiedene technische Informationen zu der jeweiligen Mail gespeichert sind (zum Beispiel, über welchen Server sie verschickt wurde).

HTML

„Hyper Text Markup Language“, jene Sprache, die zur Erstellung von Webseiten verwendet wird.

IP-ADRESSE

Die IP-Adresse ist ein numerischer Code, der jeden Rechner im Netz eindeutig identifiziert. Nachdem sich Menschen leichter Namen als Nummern merken, wurden die „Domains“ erfunden, die von Nameservern dann den IP-Adressen zugeordnet werden.

IRC

„Internet Relay Chat“, das älteste Chat-System im Internet. Um im IRC mitmachen zu können, benötigst du ein spezielles Programm, z.B. „mIRC“ für Windows oder „ircle“ für Macintosh.

GLOSSAR

LISTSERVER

Darunter versteht man einen E-Mail-Verteiler. Nachrichten werden an eine Liste geschickt, alle Mitglieder dieser Liste bekommen diese Mails dann in ihre Mailbox zugestellt. Das bekannteste Programm zur Verwaltung von Listservern ist Majordomo.

MAILBOMBE

Eine große Anzahl großer Dateien, die man jemandem schickt, um seinen oder ihren E-Mail-Account lahm zu legen.

MIDI

Ein Standard zur Wiedergabe von Musik. MIDI-Dateien sind sehr klein und leicht zu manipulieren.

NAMESERVER

Spezialisierter Server, der die Übersetzung von Domain/Rechnername (wird im Browser eingetippt) auf eine IP-Adresse (auf die der Server hört) vornimmt. Normalerweise verwendet jede/r User/in die Nameserver seines eigenen Providers.

NETIZEN

Kunstwort aus „net“ und „citizen“, frei übersetzbar mit „Einwohner des Internet“

NEWSGROUP

Diskussionsforum, das über Newsserver weltweit verteilt und gespiegelt wird. Newsgroups können mit Mail-programmen gelesen werden. Ein sehr komplettes Archiv der meisten Newsgroups findet man auf Google.

NICK(NAME)

Name einer virtuellen Identität, im realen Leben mit einem Spitznamen zu vergleichen.

OPEN RELAY

Ein Server, der E-Mails an ihre Empfänger weiterleitet, ohne zu überprüfen, wer der Absender ist. Solche Server existieren meist aufgrund von Programmier- oder Konfigurationsfehlern und werden von Spammern zum Versand von Massenmails benutzt.

GLOSSAR

PHISHING

Kunstwort aus „password“ und „fishing“. Allgemein gesprochen handelt es sich um kriminelle Methoden um die Logins und Paßwörter von Internet-Nutzern herauszufinden und diesen damit zu schaden (zum Beispiel durch das Leerräumen von Konten).

POSTING

Ein Beitrag in einem Diskussionsforum, zum Beispiel einer Newsgroup.

PROVIDER

Dein Provider ist jene Institution (meist eine Firma, Uni oder Schule), über die du Zugang zum Internet bekommst. Du benötigst dort einen Account, der dich als berechtigte/n User/in ausweist. Eine ziemlich vollständige Liste der österreichischen Provider findest du bei der ISPA. Besondere Arten von Providern sind z.B. E-Mail-Provider, die dir nur eine E-Mail-Adresse, nicht aber den Zugang zum Internet selbst verschaffen.

RIPPING

Slang-Ausdruck für das Überspielen einer CD oder DVD als eigenständige Files auf den Computer.

SEARCH-ENGINE

Darunter versteht man eine Datenbank und einen Index von Webseiten zum leichteren Auffinden von Informationen. Search-Engines werden in den meisten Fällen von „Spidern“ mit neuen Sites versorgt.

SPAM

Im angelsächsischen Raum verstand man unter „Spam“ ursprünglich eine bestimmte Art von Dosenfleisch, das auch bei uns durch einen Monty-Python-Sketch bekannt wurde. Heute ist „Spam“ ein Sammelbegriff für jede Art von unerwünschten E-Mails, insbesondere Massenaussendungen zur Bewerbung scheinbar günstiger Angebote.

SPIDER

Ein Programm, das das Internet ständig nach neuen Webseiten absucht und die Inhalte der Sites so verarbeitet, dass man in Search-Engines danach suchen kann.

GLOSSAR

SPYWARE

Ausdruck für kleine Programme, die unbemerkt Benutzerdaten an andere Computer schicken. Spyware kann illegal sein (beispielsweise als Teil von Viren-Programmen), kann aber auch völlig legal Teil von Programmen sein, mit deren Nutzungsbedingungen man sich einverstanden erklären muß. In der legalen Variante werden meist Informationen zu Marketingzwecken gesammelt, zum Beispiel über das Surfverhalten eines Users oder über die auf einem Computer installierten Programme.

TROJANER

Ein Trojaner ist ein Programm, das – nach dem mythologischen Vorbild des Trojanischen Pferdes – vorgibt, etwas anderes zu sein, als es tatsächlich ist. Die Grenze zwischen Trojanern und Viren ist heute nur noch schwierig zu ziehen, da die meisten derartigen Schädlinge beide Funktionen beinhalten.

UPLOAD

Die Übertragung einer Datei vom eigenen auf einen anderen Rechner, meistens auf einen Server irgendeiner Art.

USENET

Überbegriff für jenes Netz, in dem die klassischen Newsgroups zu Hause sind.

VIRUS

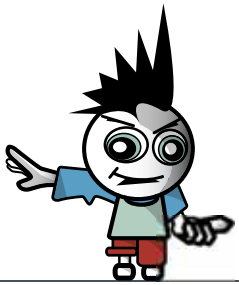
Ein Programm, das sich selbständig verbreiten kann und meist auch irgendeine Art von Schaden anrichtet.

VIRUS-DEFINITIONS

Damit Antivirenprogramme effektiv arbeiten können, benötigen sie eine Datei, in der steht, wonach sie Ausschau halten müssen. Nachdem sich Viren heutzutage innerhalb von Stunden ausbreiten können, sollten diese Definitions immer so aktuell wie möglich sein.

WEB 2.0

Ein Hauptaspekt des Web 2.0 ist, dass Inhalte nicht mehr nur zentralisiert von großen „Medien“ erstellt und an die Massen verbreitet werden, sondern auch von unabhängigen Leuten, die sich untereinander vernetzen. Typische Beispiele hierfür sind Wikis, Weblogs sowie Bild- und Videoportale und Tauschbörsen.



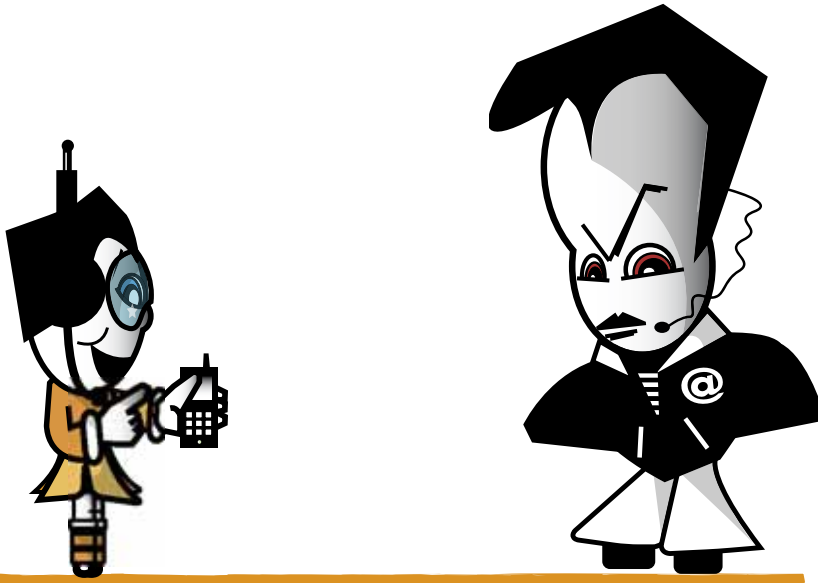
LINKSAMMLUNG

AKM	http://www.akm.co.at
BITTORRENT	http://www.bittorrent.com
BUPP	http://www.bupp.at
CIAO	http://www.ciao.de
DOOYOO	http://www.dooyoo.de
EBAY.AT	http://www.ebay.at
EBAY.COM	http://www.ebay.com
E-COMMERCE GÜTEZEICHEN	http://www.guetezeichen.at
EUDORA	http://www.eudora.com
FRIENDSTER	http://www.friendster.com
GEIZHALS	http://www.geizhals.at
GMX	http://www.gmx.at
GOOGLE	http://www.google.at
GOOGLE GROUPS	http://groups.google.at
INTERNET OMBUDSMANN	http://www.ombudsmann.at
IRCLE	http://www.ircle.com
ISPA	http://www.ispa.at
KAZAA	http://www.kazaa.com
KIDSSICHER.AT	http://www.kidssicher.at
LIMEWIRE	http://www.limewire.com
MICROSOFT	http://www.microsoft.at
MIRC	http://www.mirc.com
MOZILLA	http://www.mozilla.org
MSN HOTMAIL	http://www.hotmail.com
MY SPACE	http://www.myspace.com

LINKSAMMLUNG

NETIQUETTE	http://www.usenet.at/netiquette.html
NIC.AT	http://www.nic.at
ÖIAT	http://www.oiat.at
PRO MUSIC	http://www.pro-music.at
RAT AUF DRAHT	http://rataufdraht.orf.at
RTR	http://www.rtr.at
SAFERINTERNET.AT	http://www.saferinternet.at
STOPLINE	http://www.stopline.at
YAHOO!	http://www.yahoo.de
YAHOO! GROUPS	http://groups.yahoo.de
YAHOO! MAIL	http://mail.yahoo.de

LINKSAMMLUNG



SAFER INTERNET WEBSEITEN:

Österreich: Saferinternet.at	http://www.saferinternet.at
Österreich: Handywissen.at	http://www.handywissen.at
EU: Safer Internet plus Programm	http://www.europa.eu.int/information_society/
EU: Insafe	http://www.saferinternet.org
Deutschland: klicksafe.de	http://www.klicksafe.de

NOTES

DIE 3 FRAGEN FÜR SICHERES ONLINE SHOPPING

Wie im Alltagsleben, so sollten auch Internetnutzer beim Handel über eBay ihrem gesunden Menschenverstand vertrauen. Kaufen Sie niemals, ohne sich vorher ausreichend zu informieren, so wie Sie es sonst auch machen. Die folgenden 3 einfachen Fragen sollen Ihnen dabei helfen:

1) WER ist der Verkäufer?

Informieren Sie sich ausführlich über den Verkäufer bevor Sie ein Gebot abgeben oder einen Artikel kaufen:

eBay bietet Ihnen eine Transparenz, die es sonst nicht gibt: das Bewertungsprofil. Jedes eBay-Mitglied hat ein Bewertungsprofil, in dem Käufer und Verkäufer die Transaktionen gegenseitig beurteilen. Sehen Sie sich das Bewertungsprofil Ihres potentiellen Verkäufers an, es gibt Aufschluss über die Qualität des bisherigen Verhaltens des Verkäufers bei eBay.

2) WAS kaufe ich?

Informieren Sie sich ausführlich über den Artikel bevor Sie ein Gebot abgeben oder einen Artikel kaufen:

Lesen Sie sich die Artikelbeschreibung genau durch. Beachten Sie auch Informationen zu Zahlung und Versand des Artikels und vergleichen Sie den Artikel mit anderen, gleichartigen Artikeln. Nehmen Sie Kontakt mit dem Verkäufer auf (z.B. bezüglich Gebrauchsspuren, Höhe der Versandkosten, Rückgabebedingungen).

Stellen Sie dem Verkäufer Fragen zum Angebot, indem Sie einfach auf den Link „Frage an den Verkäufer" oben rechts auf jeder Artikelseite klicken. Ein verantwortungsvoller Verkäufer wird Ihnen gerne und ausführlich antworten.

Seien Sie besonders kritisch, wenn Neuware zu einem Festpreis eingestellt ist, der deutlich unter der Preisempfehlung des Herstellers liegt.

3) WIE bezahle und bekomme ich den Artikel?

Informieren Sie sich ausführlich über Versandkosten und Versanddauer sowie die akzeptierten Zahlungsmethoden des Verkäufers bevor Sie ein Gebot abgeben oder einen Artikel kaufen:

Sollten Sie versicherten Versand bevorzugen, damit die Sendung nachverfolgt werden kann, klären Sie dies mit dem Verkäufer vorab ab. Für hochpreisige Artikel empfiehlt eBay die Verwendung von Treuhandservices.

Wählen Sie ein sicheres Bezahlungssystem wie z.B. Überweisung, Kreditkarte, PayPal, Nachnahme oder Barzahlung bei Übergabe. Bargeldtransfers wie z.B. Western Union dürfen von Verkäufern bei eBay nicht angeboten werden.

Mehr zum sicheren Online-Shopping finden Sie auf dem Sicherheitsportal von eBay.at:
www.ebay.at/sicherheitsportal

Der Online-Marktplatz von über 1 Million Österreichern:
www.ebay.at

TELE
KOM
AUS
TRIA

Unsere Vision. Ihre Zukunft.

Das Netz von Telekom Austria.

Um die Zukunft aktiv gestalten zu können, braucht man Visionen. Gestern war es unsere Vision, die Barriere der reinen Sprachtelefonie im Festnetz von Telekom Austria zu durchbrechen. Heute ist das bereits Realität und ein Beispiel für zukunftsweisende Technologie: Das Multiservice Breitbandnetz von Telekom Austria. Es verbindet ADSL-Anschlüsse über das Netz der Sprachtelefonie mit dem Backbone und bildet damit die Basis für multimediale Applikationen. Video on Demand, WebLearning, Videokonferenzen und vieles mehr ist damit möglich geworden.

Auch heute haben wir eine Vision: Die Kommunikation von morgen noch schneller, vielfältiger, sicherer und bequemer zu machen. Freuen Sie sich auf eine spannende Zukunft. Mit neuen Technolgien, die Menschen über das zuverlässige, sichere Netz von Telekom Austria verbindet.

www.telekom.at