ispa
Internet Service Providers Austria

internet sicher nutzen

ein leitfaden der ispa

BUNDESKANZLERAMT ÖSTERREICH

JUSTIZ
BUNDESMINISTERIUM FÜR JUSTIZ

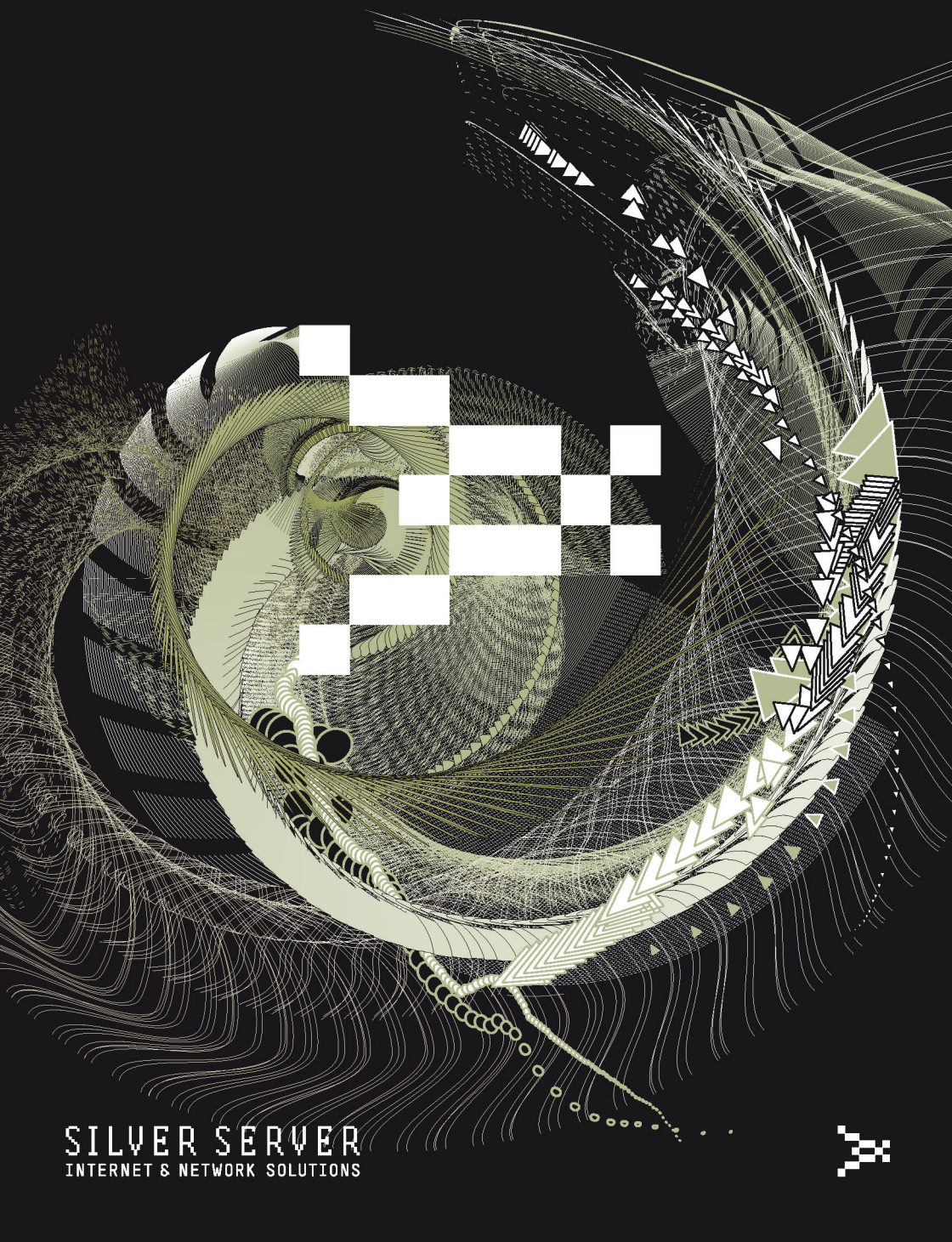
KSÖ

Saferinternet.at
Das Internet sicher nutzen!

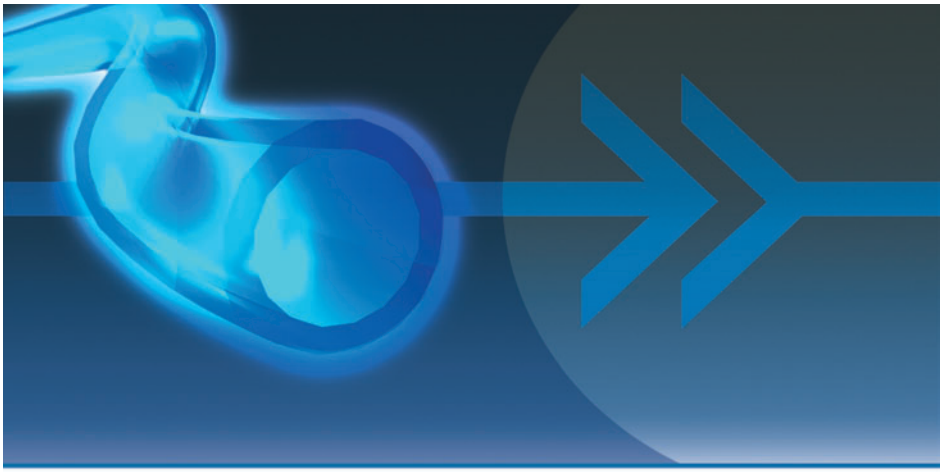
A1

Microsoft

WWW.SIL.AT // TELEFON 059944



SILVER SERVER
INTERNET & NETWORK SOLUTIONS



100% sicher!

hightechnologytransferproducts://
kapper.net
internet | communication | solutions

KAPPER NETWORK-COMMUNICATIONS GmbH, Löblichgasse 6, A-1090 Wien, T:: +43 1 319 55 00, F:: +43 1 319 55 02, @:: secure@kapper.net, www:: http://kapper.net

www.cablelink.at und 0800/660 660

Fernsehen. Internet. Telefonie.

TEUFLISCH HEISS

3 aus einer Hand: *CableLink* –
das ***teuflisch heiße*** Kabel der Salzburg AG.
Fernsehen. Internet. Telefonie.

CableLink
by Salzburg AG

Vorwort von

Bundesministerin Dr. Beatrix Karl

Im Alltag ist das Internet nicht mehr wegzudenken – die ehemals virtuelle Welt ist mit unserer Realität mittlerweile eng vernetzt. Ob Shopping per Mausklick, Kontaktanbahnung und Kontaktpflege in Social Networks, die Beschaffung und Verbreitung von Informationen oder die Übermittlung von Nachrichten, der Download von Filmen oder Musik – die Möglichkeiten des wohl schnellsten Mediums unserer Zeit sind nahezu unbegrenzt.

Wir alle nutzen und schätzen diese Möglichkeiten, gleichzeitig wird aber auch die Notwendigkeit eines verantwortungsvollen Umgangs mit dem WWW unterschätzt. Die Gefahr des Datenmissbrauchs, Betrug bei Online-Shopping, Urheberrechtsverletzungen, aber auch neue Phänomene wie Mobbing im Internet oder das sogenannte „Grooming" sind nur ein Teil der rechtlichen Dimension des Internets. Dazu kommt eine ungeahnte zivilrechtliche Komplexität – die Gültigkeit von Vertragsabschlüssen, Gewährleistungsansprüchen etc. sind nur ein weiterer Teil der riesigen juristischen Dimension.

Das Internet ist also alles andere als ein rechtsfreier Raum, auch wenn es oft einen täuschenden Eindruck zu vermitteln vermag. Bei der Rechtsdurchsetzung freilich treten spezifische Probleme auf: Es gibt kein einheitliches „Internetrecht", verschiedenste nationale und internationale Normen sind zu berücksichtigen. Dazu kommt oft noch die Unklarheit, welche Rechtsordnung im oft grenzüberschreitenden Verkehr im speziellen Fall anzuwenden ist. Hinter der Informationsflut verbirgt sich also auch noch ein nicht nur für den Laien oft schwer durchschaubarer rechtlicher Dschungel.

Deshalb begrüße ich das Erscheinen dieser Broschüre, die Unternehmen und Organisationen, aber auch Privatpersonen einen Überblick verschafft, sie über ihre Rechte und Pflichten aufklärt und damit einen immens wichtigen Beitrag zur sinnvollen und sicheren Nutzung der modernen Kommunikationstechniken.

Dr. Beatrix Karl
Bundesministerin für Justiz

Vorwort von

Staatssekretär Dr. Josef Ostermayer

Das Internet ist die wohl wichtigste „revolutionäre“ Entwicklung der letzten Jahrzehnte, es wird zunehmend zur Basisinfrastruktur unserer Informations- und Wissensgesellschaft. Bereits rund 75 Prozent der österreichischen Bevölkerung nutzen das Netz für die Suche nach Informationen aller Art, für die E-Mail-Kommunikation, zum Online-Shopping und immer häufiger für soziale Netzwerke wie Facebook.

Dies zeigt aber auch, dass demnach 25 Prozent der Bevölkerung noch nie das Internet genutzt haben. Viele der bisherigen Offliner nutzen das Netz auch deshalb nicht, weil sie es für nicht „sicher genug“ erachten. Ein Befund, der übrigens auch von vielen NutzerInnen geteilt wird. So hat etwa auch die jüngst veröffentliche Studie „EU Kids Online“ gezeigt, dass viele Eltern die Gefahren unterschätzen, die das Internet für ihre Kinder bergen können. Eines der zentralen Probleme besteht vor allem darin, dass die meisten viel zu sorglos mit ihren höchst persönlichen Daten umgehen. Man muss sich stets bewusst sein, dass man, sobald man sich ins Internet „begibt“, Spuren hinterlässt.

Daher ist jede Initiative zu begrüßen, die dazu beiträgt, dass NutzerInnen mehr Informationen und mehr Wissen erhalten, um sich etwa vor Betrugsfällen beim Online-Shopping besser zu schützen oder ihre Computer vor Schadsoftware und Spam-Emails besser abzusichern. All diese Informationen bietet die vorliegende Broschüre der ISPA. Hier findet nicht nur der Internet-Laie sondern auch der Internet-Vielnutzer wertvolle Tipps und Hilfestellungen für einen kompetenten und sicheren Umgang mit dem Netz. Das Beruhigende daran: Oftmals reicht die Befolgung einfacher Regeln, um die größten Risiken zu vermeiden und die Vorteile des Internets gefahrlos ausschöpfen zu können. Oder, wie es das geschäftsführende Mitglied der Datenschutzkommission kürzlich ausgedrückt hat: *„Stelle nie etwas ins Internet, was du nicht in den Abendnachrichten sehen willst!“*

Dr. Josef Ostermayer
Staatssekretär für Medien und Koordination
im Bundeskanzleramt

Vorwort von

ISPA Präsident Dr. Andreas Koman

Liebe Leserinnen und Leser!

Seit mehr als 20 Jahren ist das Internet in Österreich verfügbar und es hat in dieser Zeit das private, berufliche und öffentliche Leben nachhaltig verändert. Als Interessensvertretung der österreichischen Internetwirtschaft war und ist es das Ziel der ISPA, das Internet in Österreich zu fördern. Es ist der ISPA aber ebenso ein Anliegen dazu beizutragen, die Nutzung des Internet zu einem positiven und sicheren Erlebnis zu machen.

In diesem Zusammenhang freut es uns Ihnen die dritte, aktualisierte Ausgabe unserer Broschüre „Internet sicher nutzen“ präsentieren zu können. Wie auch schon die letzte Ausgabe bietet Ihnen die rechtlich und inhaltlich aktualisierte Broschüre Informationen etwa zu den Themenbereichen Shopping, Auktionen und Bezahlen im Netz, zu Sozialen Netzwerken, Kontaktbörsen, Communities, Foren und Chats sowie zur sicheren Nutzung des Internets durch Kinder und Jugendliche. Abgedeckt werden zudem Fragestellungen verbunden mit der Erstellung eigener Webseiten oder Weblogs, dem Download und Anbieten von Videos oder Musik und Schutz vor Viren, Trojanern oder Phishing Mails.

Bedanken möchten wir uns an dieser Stelle auch für die Unterstützung durch das Bundeskanzleramt, das Bundesministerium für Justiz, das Kuratorium Sicheres Österreich, die Europäische Union, unsere Projektpartner von Saferinternet sowie die Bank Austria und die Erste Bank und Sparkassen.

Ich wünsche Ihnen eine interessante Lektüre und hoffe, dass Sie unsere Anregungen und Tipps gut nützen und umsetzen können.

Dr. Andreas Koman
Präsident
ISPA – Internet Service Providers Austria

Mit freundlicher Unterstützung von

Bank Austria Member of UniCredit ERSTE SPARKASSE

Inhalt

Shopping 10
Bei wem sollen Sie bestellen? 11
Wie kommt ein Vertrag im Internet zu Stande? 12
Allgemeine Geschäftsbedingungen 13
Wie können Sie einen Kauf bzw. eine Bestellung rückgängig machen? 14
Kein Rücktrittsrecht besteht bei Verträgen über ... 15
Was können Sie tun, wenn die Ware nicht geliefert wird? 15
Was können Sie tun, wenn die bestellte Ware mangelhaft ist? 16
Was können Sie tun, wenn der Fehler nicht behoben wird? 17
Dürfen Ihre Kinder Verträge abschließen? 18

Bezahlen im Netz 20
Zunächst die gute Nachricht 21
Nun aber die schlechte Nachricht 21
Die meistverwendeten Zahlungsmittel 22
Das anonyme Zahlungsmittel 23
Die mobilen Zahlungsmittel 23
Die direkten Zahlungsmittel 23

Auktionen 26
Worauf sollten Sie beim Kauf achten? 27
Bewertungssysteme 28
Was ist wichtig, wenn Sie selbst verkaufen bzw. versteigern? 29

Soziale Netzwerke (Facebook, Twitter & Co.) 30
Sollen Sie sich bei Sozialen Netzwerken überhaupt registrieren? 32
Welche Möglichkeiten zum besseren Schutz der Privatsphäre gibt es? 32
Einige Verhaltensregeln für Soziale Netzwerke 34
Was tun, wenn Daten über Sie existieren, die zu Ihrem Nachteil sind? 36
Ausstieg aus Sozialen Netzwerken, oder: Digitale Leichen 37
Location Based Services 38

Sicherheit für Kinder & Jugendliche 40
„Meine Freundin/mein Freund hat ...“ 41
Überwachung des Nachwuchses per Software 41
Elterliche Medienkompetenz 42
Maßnahmen zum Schutz Ihrer Kinder 43
Für die Jüngsten 43
Positivlisten 44
Kommerzielle Filterprogramme 44
Cyber-Mobbing 46
Happy Slapping 47
Sexualität & Internet 47
Virtuelle Jugendsünden – Persönliche Daten 48
Prepaid Kreditkarten für Jugendliche 50

Communitys, Foren, Chats 52
Regel Nummer 1: Erst lesen, dann schreiben 53
Regel Nummer 2: Nie mit Wut im Bauch schreiben 53
Regel Nummer 3: Vorgesetzte lesen mit 54
Ehrenbeleidigung 54
Üble Nachrede 55
Verleumdung 56
Kreditschädigung 56
Illegale Foren und Chats 56

Eigene Homepage & Weblog	**58**
Dürfen Sie Bilder oder Musik auf Ihrer Homepage/in Ihrem Blog verwenden?	59
Domain-Grabbing	59
Dürfen Sie auf illegale Seiten verlinken?	60
Welche Angaben müssen Sie auf Ihrer Website machen?	60
Die Impressumspflicht	62
§ 5 ECG – Informationen	63
E-Mail: Spam, Phishing, Viren	**64**
Verschicken von Mails	65
Was können Sie gegen Spam tun?	67
Wie kommen Spammer zu den Adressen?	69
Gibt es auch legale E-Mail-Werbung?	69
Phishing: Woran erkennen Sie Phishing Mails?	70
Vorsicht vor zweifelhaften Jobs!	72
Viren, Trojaner und Konsorten	73
Wie können Sie sich vor Viren schützen?	74
Wie werden Sie einen Computervirus wieder los?	75
Hoaxes	75
419 Scams	76
Wie sorgen Sie dafür, dass Ihre Passwörter sicher sind?	76
Kontaktbörsen	**80**
Worauf sollten Sie achten, wenn Sie sich entschieden haben?	81
Persönliche Daten	82
Das erste Date	83
Filesharing, BitTorrent & Streaming	**84**
Dürfen Sie Musik oder Videos aus dem Internet downloaden?	85
Dürfen Sie Musik oder Videos zum Download anbieten?	86
Streaming	87
Cybercrime	**88**
Was ist im Netz erlaubt und was nicht?	89
Ab welchem Alter können Sie sich strafbar machen?	89
Pornografie im Internet	89
Nationalsozialistische Wiederbetätigung	90
Hacking	91
Stalking	91
Strafbare Postings	92
Internet am Arbeitsplatz	**94**
Darf Internetnutzung am Arbeitsplatz kontrolliert werden?	96
Elektronische Signatur und E-Government	**98**
Anonymität & Identität	**102**
Anonymität	103
Identität	104
Was können Sie tun, um Ihre Identität im Netz zu schützen?	105
Wer hilft Ihnen weiter?	**108**
Beschwerden über Inhalte von Websites oder Communitys	109
Probleme beim Internet-Einkauf	109
Illegale Inhalte	109
Glossar	**110**
Impressum	112

Shopping

56% der österreichischen Bevölkerung ab 14 Jahren haben schon einmal Waren im Internet bestellt. Den höchsten Anteil erzielte die Altersgruppe der 25- bis 34-Jährigen. Die beliebtesten Produktgruppen sind Bücher und Zeitschriften (44%), sowie Kleidung und Sportartikel (42%).
39% haben Reisen und Urlaubsunterkünfte über das Internet gebucht. Die Online-Beschwerdestelle des österreichischen Internet Ombudsmannes hat im Jahr 2010 in etwa 10.000 Beschwerdefälle bearbeitet, wobei ein Großteil dieser Beschwerden unter so genannte vermeintliche Gratis-Angebote fielen.

Quelle: Statistik Austria, Jahresbericht des Internet Ombudsmanns 2010

Bei wem sollen Sie bestellen?
Wie kommt ein Vertrag im Internet zu Stande?
Allgemeine Geschäftsbedingungen
Wie können Sie einen Kauf bzw. eine Bestellung rückgängig machen?
Kein Rücktrittsrecht besteht bei Verträgen über ...
Was können Sie tun, wenn die Ware nicht geliefert wird?
Was können Sie tun, wenn die bestellte Ware mangelhaft ist?
Was können Sie tun, wenn der Fehler nicht behoben wird?
Dürfen Ihre Kinder Verträge abschließen?

Nicht nur wegen der größeren Auswahl, sondern auch aus Bequemlichkeit wird das Shoppen im Internet immer beliebter. Doch gerade hier müssen Sie einige Dinge beachten:

Im Gegensatz zum normalen Einkauf können Sie die Ware nicht begutachten, bevor Sie sie kaufen. Nichtsdestotrotz sollten Sie sich ein Bild davon machen, ob die Ware das bietet, was Sie suchen, und welche Gesamtkosten auf Sie zukommen (z. B. Versandkosten). Es gibt im Internet bereits zahlreiche Websites, die sich des Problems annehmen und Preisvergleiche und/oder Erfahrungs- und Testberichte anbieten (z. B. → Geizhals, Idealo, Ciao oder Dooyo).

www.geizhals.at
www.idealo.at
www.ciao.de
www.dooyoo.at

Bei wem sollen Sie bestellen?

Abgesehen vom Preis des Produktes gibt es, wie beim normalen Einkaufen auch, noch andere Entscheidungsfaktoren:

- **Die allgemeinen Geschäftsbedingungen** des Unternehmens lesen! Auch wenn es lange dauert und die Geschäftsbedingungen teilweise schwer verständlich sind, zur Sicherheit sollten Sie die wichtigen Passagen zumindest kurz überfliegen.
- **Faustregel:** Je weiter ein Versandhaus von Ihnen entfernt ist, desto schwieriger kann es sein, sich zu beschweren oder zu reklamieren. Bestellungen in anderen EU-Mitgliedstaaten können komplizierter werden, sie sind aber immer noch relativ sicher. Außerhalb der EU sollten Sie nur bestellen, wenn das Produkt nur dort erhältlich ist und es sich um ein bekanntes Unternehmen handelt.
- **Lesen Sie Berichte über das Unternehmen** (z. B. in den → Groups auf Google oder Yahoo, oder mittels Websuche nach dem Firmen- oder Inhabernamen). Glauben Sie nicht alles, was im Internet geschrieben wird, aber generelle Anhaltspunkte über die Seriosität einer Anbieterin oder eines Anbieters lassen sich fast immer finden. Beachten Sie die Zahlungsmodalitäten:

→ groups.google.com
→ groups.yahoo.de

- **Wenn eine Firma nur Kreditkarten nimmt,** Sie aber keine zur Verfügung haben oder die Kreditkartendaten nicht per Internet bekannt geben wollen, so scheidet diese Zahlungsform wohl aus. Als Alternative bieten Banken mit der → eps Online-Überweisung eine Möglichkeit der Bezahlung an, für die nur ein Internet-Zugang erforderlich ist. Die in Österreich immer noch verbreitete Lieferung per Nachnah-

→ www.eps.or.at

me ist zwar meist etwas teurer, aber dafür sehr sicher, da erst bezahlt wird, nachdem das Paket geliefert wurde. Ausführlichere Informationen über Bezahlmöglichkeiten im Netz finden Sie im Kapitel „Bezahlen im Netz“ auf S. 20.

- **Beachten Sie allfällige Gütesiegel** oder Verbandsmitgliedschaften auf der Website der Firma. Allerdings ist nicht jedes Gütesiegel gleich viel wert. Auf der Website des → Internet-Ombudsmanns finden Sie Informationen über das Österreichische → E-Commerce-Gütezeichen. Shops, die dieses Zeichen führen, sind im Allgemeinen als vertrauenswürdig einzustufen.

→ www.ombudsmann.at
→ www.guetezeichen.at

Wie kommt ein Vertrag im Internet zu Stande?

Auch im Internet wird ein Vertrag (in diesem Fall zwischen Unternehmen und Käuferin oder Käufer) durch ein Angebot und dessen Annahme abgeschlossen, egal ob über eine Ware oder eine Dienstleistung (wie etwa eine Reise). **Rechtsgültig kommen Kaufverträge also per E-Mail oder per Mausklick nach Ausfüllen eines Bestellformulars und der entsprechenden Bestätigung des Unternehmens über den wesentlichen Inhalt des Geschäftes zu Stande.**

Bitte beachten Sie, dass es sich bei Ihrem E-Mail oder Bestellformular um ein von Ihnen gelegtes Angebot handelt, an das Sie gebunden sind und das vom anbietenden Unternehmen erst angenommen werden muss. Die Website ist nur eine Warenpräsentation, wie etwa ein Schaufenster.

Auf Grund der allgemein im Vertragsrecht geltenden Formfreiheit ist für das gültige Zustandekommen eines Vertrages im Allgemeinen keine ausdrückliche Erklärung notwendig. Der Vertrag kann auch dadurch geschlossen werden, dass Sie vom Unternehmen die Ware geliefert bekommen. Dann kann Ihnen aber noch ein Rücktrittsrecht zu Gute kommen.

Kommt es zu einer Lieferverzögerung und kann die Ware erst wieder z.B. in einem Monat und/oder um einen höheren Preis geliefert werden, haben Sie mangels Vertrag zwar keinen Anspruch auf den geringeren Preis, Sie haben aber die Wahl, das neue Angebot anzunehmen oder auch nicht.

Sie müssen vor Abgabe Ihrer Willenserklärung, in den meisten Fällen vor Abgabe des Angebots, u. a. über folgende Informationen verfügen:

- Name (Firma) und Anschrift,
- die wesentlichen Eigenschaften der Ware oder Dienstleistung,
- Preis der Ware oder Dienstleistung inklusive Steuern,
- allfällige Lieferkosten,
- Einzelheiten hinsichtlich Zahlung und Lieferung/Erfüllung,
- Belehrung über ein allfällig bestehendes Rücktrittsrecht,
- die Kosten für den Einsatz des Kommunikationsmittels,
- die Gültigkeitsdauer des Angebots oder des Preises,
- die Mindestlaufzeit des Vertrages, wenn dieser eine dauernde oder wiederkehrende Leistung zum Inhalt hat (z. B. Abos).

Spätestens zum Zeitpunkt der Lieferung, also der Erfüllung des Vertrages, müssen Sie eine schriftliche bzw. auf einem dauerhaften Datenträger befindliche Bestätigung über die meisten dieser Informationen erhalten haben.

Zudem müssen Sie – ebenfalls schriftlich bzw. auf einem dauerhaften Datenträger – rechtzeitig Informationen über die Bedingungen und Einzelheiten des Rücktrittsrechts, den Kundendienst und die geltenden Garantiebedingungen, die Anschrift, bei der allfällige Beanstandungen vorgebracht werden können, sowie bei unbestimmter oder mehr als einjähriger Vertragsdauer die Kündigungsbedingungen erhalten haben.

Ein Unterlassen der Informationsverpflichtung hat zwar keine direkte Auswirkung auf die Vertragsgültigkeit, aber auf das Rücktrittsrecht (siehe S. 14) sehr wohl. Nicht zu übersehen ist, dass fast immer die allgemeinen Geschäftsbedingungen des Unternehmens Vertragsinhalt werden.

Allgemeine Geschäftsbedingungen

Allgemeine Geschäftsbedingungen (AGB) sind Standardverträge, die größere Unternehmen all ihren Geschäften zu Grunde legen. Die Anwendung von AGB auf eine bestimmte Bestellung muss zuvor zwischen Unternehmen und Kundinnen oder Kunden vereinbart werden. Das Unternehmen muss zu diesem Zwecke deutlich zu erkennen geben,

dass seine AGB angewendet werden sollen. Außerdem müssen die AGB vor der Bestellung lesbar und speicherbar sein. Das ist der Fall, wenn es auf der Webpage mit dem Bestellformular den Link „AGB" gibt, der die Seite mit den allgemeinen Geschäftsbedingungen öffnet.

Wer AGB verwendet, möchte sich natürlich möglichst umfangreich gegen alle denkbaren Ansprüche absichern. AGB sind für Kundinnen und Kunden daher oft nachteilig. **Besonders nachteilige Bestimmungen in AGB sind allerdings ungültig.** Eine solche ungültige Bestimmung ist nach dem Konsumentenschutzgesetz z. B. der Ausschluss der Haftung für Schäden an Personen.

Wie können Sie einen Kauf bzw. eine Bestellung rückgängig machen?

Auf Grund des Konsumentenschutzgesetzes besteht ein **Rücktrittsrecht** bei im Internet abgeschlossenen Verträgen **innerhalb von 7 Tagen ab Zeitpunkt der Lieferung**, bei Dienstleistungen ab Abschluss des Vertrages. Samstage, Sonn- und Feiertage werden nicht in die Frist eingerechnet, in Deutschland ist diese Frist derzeit sogar länger. Bei Problemen mit Bestellungen innerhalb der EU können Sie sich auch an das → Europäische Verbraucherzentrum Österreichs des VKI (Verein für Konsumenteninformation) wenden.

→ www.europakonsument.at

Dieses Rücktrittsrecht haben allerdings nur Konsumentinnen und Konsumenten. Kaufen Sie als Unternehmen etwas ein, schützt Sie das Konsumentenschutzgesetz nicht.

Die Rücktrittserklärung muss innerhalb dieser Frist abgesendet werden. Es ist daher optimal, wenn Sie sich eine Bestätigung über den Sendezeitpunkt aufbewahren (eingeschriebener Brief oder wenigstens Fax oder E-Mail). Die Ware selbst kann auch etwas später zurückgeschickt werden. Ihnen muss jedoch der bereits geleistete Warenpreis zurückgezahlt werden. Die Kosten der Rücksendung können Ihnen auferlegt werden, sofern dies vertraglich (meist in den AGB) vereinbart wurde. **Doch Achtung:** Es kann von Ihnen ein angemessenes Entgelt für die Benützung des Produkts verlangt werden, einschließlich einer Entschädigung für eine damit verbundene Wertminderung.

Erhalten Sie nicht bis spätestens zum Zeitpunkt der Lieferung alle schriftlichen Informationen des Unternehmens (Name, Anschrift, Preis, Lieferkosten etc.), verlängert sich Ihr Rücktrittsrecht auf 3 Monate. Mustergültige Bestellvorgänge, bei denen sämtliche Informationspflichten berücksichtigt werden, finden Sie bei den meisten großen Online-Handelshäusern (z. B. → Otto-Versand, Amazon, MyToys etc.).

→ www.otto.de
→ www.amazon.at
→ www.mytoys.de

Kein Rücktrittsrecht besteht bei Verträgen über ...

- Dienstleistungen, die vereinbarungsgemäß schon vor Ablauf der 7-tägigen Frist begonnen haben (z. B. bereits aktivierter Mail-Account),
- verderbliche Waren (Lebensmittel),
- versiegelte Videos, CDs, Software, wenn Sie die Versiegelung (z. B. Plastikhülle) schon entfernt haben,
- Zeitungen, Zeitschriften und Illustrierte, wohl aber bei Bestellung von Abos, Wett- und Lotteriedienstleistungen,
- Hauslieferungen (Fahrtendienste wie Pizza-Zustellung),
- Freizeitdienstleistungen,
- Waren, die auf persönliche Bedürfnisse zugeschnitten sind.

Beachten Sie aber, dass Sie auch weitere Rechte haben: Wenn Sie von einem Angebot eines Online-Handelshauses getäuscht wurden, können Sie diese Irreführung geltend machen, selbst wenn Ihnen kein Rücktrittsrecht zusteht. Das ist vor allem dann wichtig, wenn das Unternehmen versucht, Ihre Rechte zu umgehen.

Was können Sie tun, wenn die Ware nicht geliefert wird?

Wird die Ware nicht rechtzeitig an den vereinbarten Lieferort geliefert, wird von einem „Verzug“ gesprochen. **In diesem Fall können Sie entweder weiterhin die Lieferung verlangen, oder 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 die Verkäuferin oder der Verkäufer tatsächlich noch die Möglichkeit der Nachholung hat, sprich: die Versanddauer muss einkalkuliert sein.

Keine Rücktrittserklärung und Nachfristsetzung ist bei Fixgeschäften nötig. Ein solches liegt vor, wenn klar erkennbar ist, dass Sie an einer verspäteten Leistung kein Interesse mehr haben (z. B. Geburtstagstorte oder Weihnachtsbaum).

Was können Sie tun, wenn die bestellte Ware mangelhaft ist?

Bei mangelhafter Ware wird häufig nicht ganz korrekt der Begriff Garantie verwendet. Bei einer Garantie – die ausdrücklich vereinbart werden muss – verpflichtet sich die Anbieterin oder der Anbieter selbst, jeden Mangel zu beheben, auch wenn der Mangel erst nach der Übergabe der Ware entsteht. Normalerweise haben Sie aber keine Garantie-, sondern nur Gewährleistungsansprüche.

Bei der Gewährleistung muss verschuldensunabhängig (d. h. unabhängig davon, ob die Verkäuferin oder den Verkäufer die Schuld trifft) dafür eingestanden werden, dass die Ware zum Zeitpunkt der Übergabe keinen Mangel hat. **Bei beweglichen Sachen (alles außer Liegenschaften) haben Sie eine Frist von 2 Jahren ab dem Zeitpunkt der Übergabe bzw. der Lieferung der Ware, um einen Mangel geltend zu machen.**

Innerhalb der ersten 6 Monate haben Sie eine Beweiserleichterung, da davon ausgegangen wird, dass der Mangel bereits von Anfang an bestanden hat. Nach Ablauf dieser 6 Monate müssen Sie beweisen, dass bereits beim Kauf des Produktes ein Mangel bestanden hat.

Zunächst können Sie eine Verbesserung (also z. B. Reparatur oder Nachtrag eines fehlenden Teiles) oder einen Austausch verlangen. Wenn die Verbesserung oder der Austausch nicht möglich ist, oder wenn das Handelsunternehmen nicht dazu bereit ist, können Sie Preisminderung verlangen oder – sofern es nicht um einen geringfügigen Mangel geht – den Vertrag auflösen („Wandlung“).

Gewährleistung kann nach dem Konsumentenschutzgesetz nicht ausgeschlossen oder eingeschränkt werden. AGB, die das nicht beachten, sind unwirksam. Das gilt aber nur bei Verbrauchergeschäften.

Vorsicht ist jedoch bei Verträgen zwischen Privatpersonen geboten, da hier das Konsumentenschutzgesetz nicht gilt und somit die Gewährleistung beschränkt werden kann (z. B. Privatverkauf über Online-Auktionshäuser).

Probleme können bei mangelhaften Waren entstehen, wenn sich das **Handelsunternehmen außerhalb der EU** befindet und fraglich ist, welches Recht anzuwenden ist, wo geklagt werden muss und ob ein erlangtes Urteil im Niederlassungsstaat auch durchsetzbar ist. Daher ist bei Kaufverträgen mit Unternehmen, deren Sitz sich nicht innerhalb der EU befindet, jedenfalls doppelte **Vorsicht geboten.** Vergessen Sie nicht: beim Kauf außerhalb der EU haben Sie unter Umständen auch noch die Zollgebühren zu bezahlen!

Was können Sie tun, wenn der Fehler nicht behoben wird?

Erst wenn das Unternehmen trotz Aufforderung nichts unternimmt, oder sein Verbesserungsversuch fehlschlägt, können Sie eine Herabsetzung des Kaufpreises oder die Rückgängigmachung des Vertrags verlangen. Zwischen Preisminderung und Wandlung besteht ein Wahlrecht.

Wird über Wandlung oder Preisminderung keine Einigung erzielt, müssen die Rechte auf gerichtlichem Weg geltend gemacht werden. Ist der Kaufpreis in solchen Fällen noch nicht bezahlt, haben Sie auch die Möglichkeit, erst nach dem Einklagen des Geldbetrags durch die Firma entsprechende Einwände zu erheben. **Da Gerichtsverfahren immer mit hohen Kosten und Risiko verbunden sind, ist eine Einigung meist die bessere Lösung.**

Haben Sie ein Gerichtsverfahren gewonnen, bedeutet das aber noch nicht, dass die Gegenpartei auch tatsächlich macht, was ihr vom Gericht aufgetragen wurde. Das Urteil muss in solchen Fällen " zwangsweise vollstreckt" werden. Beispielsweise kann durch ein Gerichtsurteil festgelegt werden, dass Sachen in der Wohnung oder im Lager der verurteilten Person gepfändet werden. Aus dem erzielten Versteigerungspreis wird dann der bezahlte Kaufpreis zurückerstattet.

Innerhalb der EU ist die Vollstreckung von Urteilen der Mitgliedsstaaten möglich. Zwischen den USA und Österreich gibt es kein Vollstreckungsabkommen. Ein US-amerikanisches Gericht wird daher ein österreichisches Gerichtsurteil nicht vollziehen.

Dürfen Ihre Kinder Verträge abschließen?

Kinder im Alter von 7 bis 13 Jahren dürfen nur kleine Geschäfte des alltäglichen Lebens allein abschließen (z. B. Kauf eines Kaugummis oder einer Wurstsemmel).

Da **Geschäfte über das Internet** wohl nicht als alltäglich angesehen werden können, ist dafür **die Zustimmung eines Elternteils bzw. des Erziehungsberechtigten erforderlich.**

Bis zur Einwilligung des gesetzlichen Vertreters ist das Geschäft „schwebend unwirksam" (so genanntes „hinkendes Rechtsgeschäft"). Verweigert der gesetzliche Vertreter seine Genehmigung, ist das Geschäft endgültig unwirksam.

Zwischen dem 14. und 18. Geburtstag darf das Taschengeld bzw. das eigene Einkommen nach eigenem Ermessen ausgegeben werden. **Sobald ein Geschäft** jedoch **den Lebensunterhalt des Kindes gefährdet,** ist auch hier eine **Genehmigung eines Elternteils** erforderlich. Fehlt diese, kommt kein gültiger Vertrag zu Stande.

Unseriöse Gratisangebote – Internetabzocke

Mit vermeintlich kostenlosen Angeboten locken heute viele Internetseiten. Von Gratis-SMS über Hausübungshilfen bis hin zu Lebenserwartungsprognosen und IQ-Tests ist praktisch alles scheinbar gratis im Internet zu finden. Das System dahinter ist meist dasselbe: Es reicht eine einfache Registrierung mit Angabe von ein paar persönlichen Daten.

Einige Tage nach der Registrierung folgt eine Rechnung oder gar eine Zahlungsaufforderung. Daher ist es wichtig, die allgemeinen Geschäftsbedingungen (AGB) oder die Nutzungsbedingungen zu lesen, die meist nur versteckt auf ein kostspieliges Abo hinweisen.

TIPP

Seien Sie bei Gratisangeboten und Gewinnspielen stets misstrauisch. Auch im Internet ist selten etwas wirklich „gratis". Oft handelt es sich um Lockangebote, bei denen später laufende Kosten entstehen.

Lesen Sie die Allgemeinen Geschäftsbedingungen (AGB) der Anbieterin oder des Anbieters immer genau, bevor Sie diese bestätigen! Oft verstecken sich darin Verpflichtungen wie jene, ein kostenpflichtiges Abo zu erwerben. Achten Sie speziell auf die angegebenen Fristen und auf eventuell entstehende Kosten.

Stornieren Sie Testzugänge sofort, wenn Sie diese nicht brauchen bzw. geben Sie zum unverbindlichen Testen von Onlinediensten niemals Ihre persönlichen Daten an. Bedenken Sie, Ihre persönlichen Daten sind (z.B. für Werbedatenbanken) bares Geld wert.

Stornieren Sie unerwünscht bzw. versehentlich eingegangene Verträge (bzw. kostenpflichtige Anmeldungen) immer per Post mit einem eingeschriebenen Brief und behalten Sie eine Kopie des Schreibens.

Wenn Sie trotz aller Vorsicht auf ein derartiges Angebot eingegangen sind oder Ihre Kündigung nicht akzeptiert wird, **wenden Sie sich sofort an eine Konsumentenschutzorganisation (z. B. → Internet-Ombudsmann, Arbeiterkammer, Verein für Konsumenteninformation). Sie werden zumeist nicht das einzige Opfer der unseriösen Abzocke sein. Je schneller Sie diese melden, umso schneller kann dagegen vorgegangen werden.** Warten Sie nicht bis das erste Schreiben einer Geldeintreibe-Firma in Ihrem Postkasten liegt. Die Abzocker spekulieren teilweise darauf, dass sich Betroffene nicht trauen sich zu melden, da es Ihnen peinlich ist, auf eine Abzockfalle hereingefallen zu sein.

→ www.ombudsmann.at
→ www.vki.at
→ www.arbeiterkammer.at

Das → Bundesministerium für Soziales und Konsumentenschutz bietet Ihnen einen Informationsfolder zum Thema „Internet-Abzocke – Gratisangebote im Internet".

→ broschuerenservice.bmask.gv.at

Bezahlen im Netz

Rund 52% aller im Internet getätigten Transaktionen werden in Österreich per Banküberweisung (Zahlschein, Bankeinzug) durchgeführt. Kreditkarten werden bei 30% der getätigten Zahlungen verwendet, immerhin 13% der gehandelten Güter werden per Nachnahme bezahlt. Alle übrigen Zahlungsmittel, die speziell für die Bezahlung im Internet entwickelt wurden, finden in Österreich nur geringe Anwendung. Die Unsicherheit bei der Bezahlung wird beim Kauf von Waren im Internet als zweiter Grund genannt, NICHT im Internet einzukaufen.

Quelle: Österreichische Nationalbank

Die meistverwendeten Zahlungsmittel
Das anonyme Zahlungsmittel
Die mobilen Zahlungsmittel
Die direkten Zahlungsmittel

Zunächst die gute Nachricht:

Bezahlen im Netz ist besser als sein Ruf! Trotz der unzähligen Horrormeldungen von gestohlenen Kreditkartennummern, gehackten ☛ *Servern* und unseriösen Webshops, ist Einkaufen im Netz im Großen und Ganzen relativ sicher. Oder würden Sie nicht mehr in ein Einkaufszentrum gehen, nur weil dort möglicherweise Ihre Geldbörse gestohlen wird?

☛ Server:
Rechner, auf dem Dateien gespeichert sind, die von anderen Rechnern (Clients) gelesen oder verarbeitet werden können.

Nun aber die schlechte Nachricht:

Leider ist im Netz vieles etwas kompliziert. Wenn Sie z. B. lesen, dass ein Online-Shop, in dem Sie eingekauft haben, gehackt wurde, so wissen Sie nicht sofort, ob Sie betroffen sind. Dass Shops normalerweise Kreditkarten-Informationen von Kundinnen und Kunden nicht speichern, d. h. diese daher auch nicht durch Hacking erbeutet werden können, ist nur ein schwacher Trost für Sie, wenn Sie befürchten, Opfer eines Online-Diebstahls geworden zu sein.

Oft ist der Kundenrechner, der durch einen ☛ *Trojaner* ausspioniert wird, die undichte Stelle beim Online-Kauf. Wir empfehlen Ihnen daher, genau darauf zu achten, dass Ihr Computer viren- und trojanerfrei ist, bevor Sie Zahlungen tätigen, und dass Sie eine sichere Internetverbindung zum Shop oder zur Bank aufgebaut haben. Nähere Informationen zur Bekämpfung von Viren und *Trojanern* finden Sie im Kapitel „E-Mail: ☛ *Spam,* ☛ *Phishing,* Viren“. Im Kapitel „Shopping“ finden Sie alle Informationen zu Ihrem rechtlichen Status beim Online-Einkauf.

☛ Trojaner:
Ein Programm, das vorgibt, etwas anderes zu sein, als es tatsächlich ist. Die Grenze zwischen Trojanern und Viren ist heute nur noch schwer zu ziehen, da die meisten derartigen Schädlinge beide Funktionen beinhalten.

TIPP

Achten Sie bei der Bezahlung bei der Eingabe Ihrer Daten immer darauf, dass diese über eine SSL-verschlüsselte Internetseite eingegeben werden. Die SSL-Verschlüsselung erkennen Sie daran, dass die Webseite mit https://www beginnt und im Browser das Schlosssymbol geschlossen aufscheint.

☛ Spam:
Ein Sammelbegriff für jede Art von unerwünschter E-Mail.

☛ Phishing:
Kunstwort aus „password“ und „fishing“. Ist eine kriminelle Methode, um Logins und Passwörter herauszufinden und z. B. Bankkonten zu plündern.

Die meistverwendeten Zahlungsmittel

Fast jeder Online-Shop bietet die Möglichkeit, per Kreditkarte zu bezahlen. **Die Vorteile des Bezahlens via Kreditkarte liegen klar auf der Hand:** Kreditkarten sind weit verbreitet und werden online fast überall akzeptiert, der Bezahlvorgang ist einfach und schnell. Jedoch Vorsicht: Sie sind durch die Verwendung der Kreditkarte nicht anonym, und unseriöse Shops können Ihre Karteninformationen daher missbrauchen.

Die Kreditkartenunternehmen sind jedoch bemüht, die Rahmenbedingungen für die Bezahlung mit Kreditkarte sicherer zu machen und bieten mittlerweile **Prepaid-Kreditkarten** an. Diese Art der Kreditkarte kann immer wieder mit einem vom Kunden **festgelegten Betrag aufgeladen werden** und auch nur bis zu diesem Betrag belastet werden. Sollten Sie Opfer eines Kreditkartenbetrugs werden, kann im schlimmsten Fall nur der vorher einbezahlte Betrag behoben werden.

Diese Art der Kreditkarte eignet sich aber auch besonders für Jugendliche, denen eine Möglichkeit für die Bezahlung im Internet eröffnet werden soll. Per Überweisung oder Bareinzahlung auf das Kartenkonto kann - wie mit einer ganz normalen Kreditkarte - überall dort wo die Kreditkarte akzeptiert wird, eingekauft werden. Auch eine Barbehebung mit einem Code ist, bis zu dem eingezahlten Betrag, möglich.

→ www.cardcomplete.com/e-commerce

Immer mehr Online-Unternehmen bieten außerdem die Möglichkeit eines gesicherten → Kreditkarten-Zahlungsverfahren **„MasterCard Secure Code" bzw. „Verified by VISA"** an. Diese mit eigenen Logos gekennzeichneten Systeme ermöglichen es, dass die Kreditkartennummer nicht mehr im Klartext über die Leitung gesendet wird, sondern über einen verschlüsselten Code. Alle an der Transaktion beteiligten Personen werden überprüft, ob sie auch wirklich die sind, für die sie sich ausgeben. Zusätzlich zu der herkömmlichen Kreditkarten-Zahlung müssen sich dabei alle beteiligen mit einem Passwort über eine verschlüsselte Verbindung authentifizieren. Es reicht also nicht, nur die Kreditkartennummer und den Namen anzugeben, man muss zusätzlich noch das Passwort wissen. Die Anmeldung zu diesem Verfahren kann von jeder Person, die eine Kreditkarte besitzt, direkt über die Kreditkartenfirma, oder über die jeweilige Hausbank erfolgen.

→ www.eps.or.at

Ein weiteres Internet-Zahlungsmittel in Österreich ist die → eps Online-

Überweisung. Mit diesem System können Sie via Internet direkt von Ihrem Konto online Zahlungen durchführen. Über eine Schnittstelle erhält das Online-Unternehmen von der Bank sofort eine Zahlungsbestätigung. Sensible Informationen über Sie werden hierbei nicht an das Online-Unternehmen weitergeleitet, sodass ein Missbrauch ausgeschlossen ist.

Andere gebräuchliche Zahlungsmittel im Internet sind u. a. → paybox, paysafecard, PayPal und ClickandBuy.

→ www.paybox.at
→ www.paysafecard.at
→ www.paypal.at
→ www.clickandbuy.at

Das anonyme Zahlungsmittel

Wenn Sie Zahlungen im Netz völlig anonym tätigen wollen, so ist in Österreich die „paysafecard" ein verbreitetes Zahlungsmittel. Da es sich um eine so genannte **Prepaid-Karte** handelt (Sie kaufen die Karte mit einem Guthaben und können nicht ins Minus rutschen), ist ein etwaiger Missbrauch sehr begrenzt. Die „paysafecard" wird jedoch nur beschränkt von Online-Firmen akzeptiert.

Die mobilen Zahlungsmittel

Sie können Online-Angebote auch via **Mehrwert-SMS** oder „paybox" bezahlen. Besonders auf Online-Plattformen, die Klingeltöne oder Hintergrundbilder für Mobiltelefone anbieten, ist diese Möglichkeit des Bezahlens sehr beliebt. Wir empfehlen Ihnen jedoch, genau zu überprüfen, was Sie erwerben: Ist es ein einmaliger Kauf oder verpflichten Sie sich zum Bezug eines kostenpflichtigen Abos?

Die direkten Zahlungsmittel

Natürlich kann, wenn es der Online-Shop anbietet, auch **per Nachnahme** oder **Lastschriftverfahren** bzw. Überweisung bezahlt werden. Bezahlung per Nachnahme hat den Vorteil, dass Sie die bestellte Ware erst bezahlen, wenn diese geliefert wurde. Diese Bezahlmethode ist jedoch meist mit nicht unerheblichen Kosten verbunden. Sie sollten sich daher vorher vergewissern, wer diese Kosten trägt. Dies gilt natürlich auch für Transportkosten, falls diese anfallen.

Immer größerer Beliebtheit erfreut sich die **Online-Überweisung.** Je nach Unternehmen können Sie per Online-Konto klassisch überweisen.

→ www.eps.or.at

Eine andere Form der direkten Zahlung im Internet ist die → **eps Online-Überweisung:** Es ist ein einfaches, sicheres und kostenloses Zahlungssystem der österreichischen Banken für Einkäufe im Internet. Sie bezahlen mittels eps Online-Überweisung in über 800 Web-Shops bequem und schnell mit Ihrem vertrauten Online-Banking.

TIPP

Falls Sie Unregelmäßigkeiten bei der Verwendung Ihrer Kreditkarte im Internet entdecken, gilt die gleiche Regel wie in der realen Welt: sofort die Bank verständigen, um die notwendigen Sperren und Rückbuchungen zu veranlassen. Hierfür besteht in der Regel eine Frist von zwei Wochen. Überprüfen Sie daher umgehend und gewissenhaft Ihre Kreditkartenabrechnung und suchen Sie sorgfältig nach merkwürdigen Zahlungen. Oft werden nur geringe Beträge abgebucht in der Hoffnung, dass diese dem Opfer gar nicht auffallen.

Auktionen

Das bekannteste Online Auktionshaus ist nach wie vor eBay. Alternativ dazu gibt es auch noch auktionsprofi.at, hood.de, auvito.de oder 2-1deins.de.

Laut eBay wird auf dem deutschen eBay-Marktplatz alle 2 Sekunden ein Kleidungsstück, alle 2 Sekunden ein Fahrzeugteil, alle 14 Sekunden ein Handy, alle 2 Minuten ein Notebook und alle 10 Minuten eine E-Gitarre verkauft. Der teuerste Artikel der weltweit bei eBay verkauft wurde war ein Firmenjet, der für 4,9 Millionen US-Dollar seinen Besitzer wechselte.

Quelle: ebay Presse-Center April 2010

Worauf sollten Sie beim Kauf achten?

Bewertungssysteme

Was ist wichtig, wenn Sie selbst verkaufen bzw. versteigern?

Worauf sollten Sie beim Kauf achten?

Da bei Online-Auktionen wie auch im täglichen Leben immer wieder Betrügereien stattfinden, sollten Sie es tunlichst vermeiden, Vorauskasse zu leisten. **Bezahlen per Nachnahme oder per Zahlschein ist beispielsweise eine sichere Variante, natürlich auch die Barzahlung bei persönlicher Abholung.**

Weiters gibt es auch Versteigerungsplattformen, die **Treuhandsysteme** anbieten. Sie überweisen in diesem Fall den Kaufbetrag auf ein treuhändisch verwaltetes Konto. Erst wenn die Ware unbeschadet bei Ihnen angekommen ist, wird auch der Geldbetrag an die Verkäuferin oder den Verkäufer weitergeleitet. Dieses System sollten Sie vor allem bei größeren Geldbeträgen in Anspruch nehmen.

Auch die örtliche Distanz zur Anbieterin oder zum Anbieter darf nicht außer Acht gelassen werden. Liegt der Verkaufsort in Ihrer Nähe, so kann die Ware nach dem Kauf selbst abgeholt, oder vor dem Kauf besichtigt werden. Nur wenn Sie auch dem Angebot im Internet entspricht, werden Sie bei der Auktion mitbieten.

Wird die ersteigerte Sache per Post verschickt und kommt nicht oder nicht so wie vereinbart an, müssen Sie bedenken, dass es sich um eine **Privatperson** handelt, die ihre Waren versteigert, und daher das **Konsumentenschutzgesetz nicht anwendbar** ist.

Weiters kommt ein Vertrag nur zwischen Verkäuferin oder Verkäufer und Bieterin oder Bieter zu Stande. **Das bedeutet, dass das Online-Auktionshaus** (→ eBay, Auktionsprofi etc.) **nur eine Vermittlerrolle hat.** Gegen das Auktionshaus können daher keinerlei Ansprüche geltend gemacht werden. Selbst für Bewertungssysteme, die sehr hilfreich sein können, aber manchmal auch gefälscht sind, haftet das Auktionshaus nicht.

- www.ebay.at
- www.auktionsprofi.at
- www.hood.de
- www.auvito.de
- www.2-1deins.de

Prinzipiell gelten auch bei einem Handel zwischen Privatpersonen die gesetzlichen Gewährleistungsregeln. Diese können jedoch ausgeschlossen werden, indem beim Angebot der Hinweis gegeben wird, dass keine Haftung übernommen wird. Nur wenn es sich um eine Fehlbeschreibung handelt, kann der Vertrag wegen Irrtums rückgängig gemacht werden.

Beachten Sie aber immer aufmerksam die Warenbeschreibung. Ein typischer Nepp ist z. B., wenn nur die Verpackung einer Ware und nicht der Inhalt **angeboten wird.** Hier hilft nur aufmerksames und genaues Lesen der Artikelbeschreibung.

Ersteigern Sie Waren von privaten Anbieterinnen oder Anbietern, ist das bereits erläuterte Rücktrittsrecht jedenfalls ausgeschlossen, da Sie das Konsumentenschutzrecht nur bei Käufen von Unternehmen schützt. Kaufen Sie etwas bei einer so genannten **„Sofortkaufen"-Versteigerung,** handelt es sich um keine echte Versteigerung, sondern um **einen ganz gewöhnlichen Kauf.** Daher haben Sie innerhalb von 7 Tagen nach Erhalt der Ware ein Rücktrittsrecht.

Ob das Rücktrittsrecht bei gewerblichen Angeboten für Internet-Auktionen gilt, ist zwar wahrscheinlich, kann aber nicht eindeutig beantwortet werden, da es in Österreich noch keine höchstgerichtlichen Entscheidungen zu dieser Thematik gibt. Auf der sicheren Seite sind Sie jedenfalls, wenn Sie nur bei solchen Unternehmen mitsteigern, die ein Rücktrittsrecht gewähren.

Bewertungssysteme

Wenn Sie bei einem Online-Auktionshaus etwas ersteigern gibt es bei den meisten Auktionshäusern die Möglichkeit, die Verkäuferin oder den Verkäufer zu bewerten. Diese Bewertungssysteme helfen auch durchaus bei der Entscheidung, bei wem Sie bestellen sollen, im realen Leben gehen Sie ja auch oft aufgrund einer Empfehlung bei einem bestimmen Geschäft einkaufen. Andererseits haben Sie so auch die Möglichkeit, diversen Betrügereien oder Abzock-Versuchen etwas entgegenzusetzen, sollten Sie schlechte Erfahrungen mit Personen die Produkte anbieten oder kaufen, gemacht haben.

Doch Achtung: Auch hier dürfen **keine geschäftsschädigenden Aussagen** getroffen werden, die abgegebenen Bewertungen sollten sachlich und unemotional bzw. neutral formuliert sein und wenn eine Einigung erzielt worden ist, dann sollten Sie das auch vermerken. Behalten Sie im Hinterkopf, dass eine negative Bewertung für die Verkäuferin oder den Verkäufer unter Umständen existenzbedrohend sein kann und Sie für geschäftsschädigende Aussagen auch verklagt werden können.

Was ist wichtig, wenn Sie selbst verkaufen bzw. versteigern?

Auch für Verkäufe unter Privatpersonen gilt das gesetzliche Gewährleistungsrecht, jedoch kann dies ausgeschlossen werden. Ein einfacher Zusatz wie „Verkauf ohne Gewährleistung“ ist ausreichend.

Erkennbare Fehler oder Mängel des Produkts müssen aber genau beschrieben werden, sonst kommt es zu einer Haftung wegen arglistigen Verschweigens bzw. der Vertrag kann wegen Irrtums rückgängig gemacht werden. Das heißt, Sie sollten in jedem Fall auch auf kleine Mängel bzw. Fehler aufmerksam machen.

Passen Sie aber auf, wenn Sie regelmäßig Waren versteigern, und zwar mit der Absicht, daraus Gewinne zu erzielen. Diese Tätigkeit ist nämlich als „gewerblich“ einzustufen. Daher muss in diesem Fall bei der Behörde ein Gewerbe angemeldet werden.

Wenn Sie eine gewerbliche Verkäuferin oder ein gewerblicher Verkäufer sind, eine andere Einkommensquelle haben (z. B. unselbständig angestellt sind) und die Einkünfte aus den Verkäufen mehr als etwa € 730,– pro Jahr betragen (Beträge ändern sich ständig, bitte erkundigen Sie sich beim Finanzamt), müssen Sie dies dem Finanzamt bzw. eventuell auch der Sozialversicherung melden bzw. benötigen Sie eine Gewerbeberechtigung. Nur bei gewerblichen Verkäuferinnen und Verkäufern, die den Verkauf von Artikeln als ausschließliche Einkommensquelle nutzen, sind alle Gewinne bis € 10.000,– pro Jahr in der Regel einkommenssteuerfrei. Jedenfalls treten Sie durch die Regelmäßigkeit in diesem Fall als Unternehmerin oder Unternehmer auf und sollten sich über die entsprechenden rechtlichen Rahmenbedingungen bei der Wirtschaftskammer informieren oder eine Rechtsberatung einholen. Die Gewährleistung kann dann Ihrerseits nicht mehr ausgeschlossen werden.

Soziale Netzwerke

(Facebook, Twitter & Co.)

Im Februar 2009 haben sich die meisten Anbieterinnen und Anbieter von Social-Network-Plattformen zur Umsetzung der so genannten Safer Social Networking Prinzipien der EU bekannt. Im Februar 2010 wurde die Umsetzung dieser Prinzipien von der EU überprüft und die EU kam zu dem Schluss, dass von den 25 betriebenen Webseiten ein Großteil leicht auffindbare Sicherheitstipps für Kinder und Jugendliche bereitstellt. Kritisiert wurde, dass bei einigen die Profile Minderjähriger standardmäßig noch immer über Suchmaschinen zu finden und für alle einsehbar sind.

Quelle: EU-Presseaussendung Februar 2010

Sollen Sie sich bei Sozialen Netzwerken überhaupt registrieren?
Welche Möglichkeiten zum besseren Schutz der Privatsphäre gibt es?
Einige Verhaltensregeln für Soziale Netzwerke
Was tun, wenn Daten über Sie existieren, die zu Ihrem Nachteil sind?
Ausstieg aus Sozialen Netzwerken, oder: Digitale Leichen
Location Based Services

Soziale Netzwerke wie → Facebook, Twitter, Szene1.at, netlog, StudiVZ, SchülerVZ oder Xing, erfreuen sich mit ihren rasant wachsenden Nutzungsstatistiken weltweit immer größerer Beliebtheit. Während Xing (oder die englisch-sprachige Variante → LinkedIn) eher ein Business-Netzwerk ist und den Fokus auf die beruflichen Kontakte seiner Mitglieder legt, ist StudiVZ eine Plattform zur Vernetzung für Studierende aller Studienrichtungen. SchülerVZ ist StudiVZ sehr ähnlich und bietet dieselben Funktionen für Schülerinnen und Schüler an. Das größte und beliebteste Soziale Netzwerk ist aber Facebook, auch wenn Facebook immer wieder wegen seiner Datenschutzpolitik ins Kreuzfeuer der Kritik gerät. Twitter dient wiederum als Plattform zur Verbreitung von kurzen Textnachrichten (bis zu oder max. 140 Zeichen) im Internet.

→ www.facebook.com
→ www.twitter.com
→ www.szene1.at
→ www.netlog.com
→ www.studivz.net
→ www.schuelervz.net
→ www.xing.com
→ www.linkedin.com

Über Twitter funktioniert die Informationsverbreitung gerade in Ausnahmezuständen (Kriege, Naturkatastrophen) oft besser, als über die Kanäle der traditionellen Medien. Szene1.at ist ein event-orientertes soziales Netzwerk, netlog ein europäisches soziales Netzwerk, das in Österreich überwiegend von Jugendlichen genutzt wird.

Die meisten Sozialen Netzwerke funktionieren ähnlich: bei der Registrierung kann **ein Profil mit Namen, Foto und persönlichen Informationen** erstellt werden, das dann allgemein abrufbar ist. Ist erst einmal ein Profil erstellt, gibt es die Möglichkeit, Freundinnen und Freunde zum eigenen Profil hinzuzufügen, zu „adden". Durch das Hinzufügen von Freunden, Bekannten oder Verwandten zu der eigenen Freundesliste steht der Vernetzung mit der ganzen Welt nichts mehr im Wege. So können beispielsweise alle vernetzten Menschen mit so genannten „Statusmeldungen" über den eigenen Gefühlszustand am Laufenden gehalten werden, oder Nachrichten an diversen Pinnwänden hinterlassen.

Bei vielen Sozialen Netzwerken sind die **Profile standardmäßig so eingestellt, dass sie über diverse Suchmaschinen gefunden werden können.** Sucht also beispielsweise jemand bei → Google nach Ihrem Namen, erscheint in den Suchergebnissen Ihr Profil (oder Teile davon) und weltweit kann auf die oft detaillierte Darstellung der eigenen Person zugegriffen werden.

→ www.goolge.com

Sollen Sie sich bei Sozialen Netzwerken überhaupt registrieren?

Bei dieser Frage gehen die Meinungen stark auseinander. Manche Menschen verweigern sich Sozialen Netzwerken völlig und registrieren sich aus Prinzip nicht weil sie nicht wollen, dass irgendwelche Daten über sie im Internet existieren.

Auf der anderen Seite gibt es Menschen, die ihr ganzes Leben öffentlich führen, bei allen Social Network Plattformen registriert sind, einen eigenen Blog betreiben und all ihre Fotos mit dem eigenen Namen ☛ *taggen.* Sie führen sozusagen ein öffentliches Leben und haben kein Problem damit, die ganze Welt daran teilhaben zu lassen.

☛ Taggen: Das Indexieren eines Fotos mit dem eigenen Namen. Bei einer Suchanfrage können Fotos so besser gefunden werden.

Aber zwischen völliger Verweigerung oder Online-Exhibitionismus gibt es auch die Möglichkeit Soziale Netzwerke zu nutzen, ohne gleich sein komplettes Leben öffentlich preisgeben zu müssen. Beachtet man einige Spielregeln, kann der Zugriff auf das eigene Profil stark eingeschränkt und somit nur einem geschlossenen Benutzerinnen- und Benutzerkreis zugänglich gemacht werden.

Welche Möglichkeiten zum besseren Schutz der Privatsphäre gibt es?

Alle Sozialen Netzwerke anerkennen mehr oder weniger die Datenschutzbedürfnisse ihrer Userinnen und User. Bei den meisten Sozialen Netzwerken gibt es die Möglichkeit, die **Einstellungen der Privatsphäre so zu verändern, dass das eigene Profil nicht mehr in den Suchergebnissen von Suchmaschinen aufgelistet wird,** bzw. dass nicht öffentlich auf das eigene Profil zugegriffen werden kann. Es ist zu empfehlen, das eigene Profil nur den persönlich bekannten Freundinnen oder Freunden sichtbar zu machen. Soziale Netzwerke sind durchaus vergleichbar mit Ihrem privaten Wohnzimmer, zu dem Sie auch nur engsten Freunden Zutritt gewähren (und wo Sie eine Eingangstüre mit einem Schloss davor haben). Auf der sicheren Seite sind Sie, wenn Sie nur **Daten oder persönliche Details veröffentlichen, von denen es unbedenklich ist, wenn die ganze Welt sie lesen kann.** Sich seine Privatsphäre-Einstellungen einmal etwas näher anzusehen ist zwar zeitintensiv und auf den ersten Blick

verwirrend, kann Ihnen jedoch eine Menge Ärger und Unannehmlichkeiten ersparen.

Sollte Ihnen jemand eine Freundschaftsanfrage schicken, den Sie zwar flüchtig kennen, dessen Anfrage Sie aber nicht ablehnen können, so können Sie bei den meisten Sozialen Netzwerken innerhalb Ihrer Freunde noch verschiedene Gruppen definieren, denen Sie unterschiedliche Einsicht in Ihr Profil gewähren. Analog zu Ihrem realen Leben können Sie so beispielsweise einen engeren Freundeskreis definieren, der Zugriff auf all Ihre Informationen hat, eine Gruppe für Arbeitskolleginnen und -kollegen und eine Gruppe für den erweiterten Bekanntenkreis. Welcher Gruppe Sie wie viel preisgeben, bleibt Ihnen natürlich selbst überlassen.

FACEBOOK-CHECK

Überprüfung der Privatsphäre Einstellungen in 5 Schritten

Bereits mit einigen wenigen Schritten kann man auf → Facebook Vorkehrungen treffen, um den **Missbrauch persönlicher Daten zu vermeiden.** Dabei steht an erster Stelle die Überlegung, welche Informationen öffentlich preisgegeben und welche geschützt werden sollen. Da sich die Privatsphäre Einstellungen und damit die Optionen immer wieder ändern, empfehlen wir, diese **monatlich** zu **überprüfen.**

→ www.facebook.com

1. Freigabe von Statusmeldungen, Fotoalben und persönlichen Informationen

Wer welche Profilangaben und Postings sehen kann, lässt sich einstellen. Insbesondere die Sichtbarkeit von Kategorien wie Geburtsdatum, Kontaktinformation, „Status, Fotos und Beiträge“ oder „Fotos und Videos in denen du markiert wurdest“ sollte auf Freunde beschränkt werden.
Einstellen: Konto > Privatsphäre-Einstellungen > „nur Freunde“

2. Einstellungen in der Profilvorschau überprüfen

Mit der Profilvorschau sieht man auf einen Blick, wie das eigene Profil für nicht befreundete Nutzer angezeigt wird. Bei Eingabe des Namens im Anzeigefeld kann die Darstellung überprüft werden.
Einstellen: Konto > Privatsphäre-Einstellungen > Benutzerdefinierte Einstellungen > Vorschau für mein Profil

3. Anwendungen und Websites: Zugriff auf persönliche Daten minimieren

Beim Start einer Facebook-Anwendung (Spiele, Quizzes, Marktplatz etc.), ist die Zustimmung zum Zugriff auf die eigenen Daten erforderlich. Je mehr Anwendungen man verwendet, desto mehr können Dritte die Daten für eigene Zwecke weiter verarbeiten. Durch das regelmäßige Überprüfen und Löschen der Liste kann der Zugriff minimiert werden.

Einstellen: Konto > Privatsphäre-Einstellungen > Anwendungen und Webseiten > „Anwendungen, die du verwendest“

4. Öffentliche Suche deaktivieren

→ www.goolge.com
→ www.123people.at

Wer nicht möchte, dass Suchmaschinen wie → Google oder → 123people.at das eigene Profil in der Ergebnisliste führen, kann die „Öffentliche Suche“ deaktivieren. Bei unter 18-jährigen ist die Einstellung standardmäßig deaktiviert, mit dem 18. Geburtstag wird automatisch umgestellt.

Einstellen: Konto > Privatsphäre Einstellungen > Anwendungen, Spiele und Webseiten > Öffentliche Suche > Einstellungen bearbeiten > Deaktivieren

5. Facebook Orte: Sichtbarkeit des momentanen Aufenthaltsortes einschränken

Facebook Orte ist eine Funktion, die bei der mobilen App von Facebook integriert ist und die den aktuellen Aufenthaltsort der Benutzerin oder des Benutzers anzeigt. Wer die Funktion verwenden möchte, sollte sie auf „nur Freunde“ beschränken. Dass Freunde den Aufenthaltsort für einen angeben können, kann gänzlich gesperrt werden.

Einstellen: Konto > Privatsphäre Einstellungen >Benutzerdefinierte Einstellungen> „Orte, die du besuchst“ > „Nur Freunde“ einstellen sowie „Freunde können angeben, dass ich mich an einem Ort befinde“ sperren

Einige Verhaltensregeln für Soziale Netzwerke

Bei der Nutzung von Social Networks sollten Sie prinzipiell immer im Hinterkopf behalten, dass Sie sich im Internet in einem öffentlichen Raum bewegen und Daten sehr leicht kopiert oder weitergeschickt werden können. Nicht nur einmal ist es passiert, dass eine negative Statusmeldung

über die Arbeitgeberin oder den Arbeitgeber oder etwa kompromittierende Fotos des letzten launigen Abends jemanden den Arbeitsplatz gekostet haben. Aber auch Statusmeldungen über Beziehungen oder Ehen wie „XY läßt sich demnächst scheiden“ oder „XY will nicht mehr mit Z zusammen sein“ sind durchaus verzichtbar.

Bedenken Sie außerdem, dass zukünftige Arbeitgeberinnen oder Arbeitgeber das Internet unter Umständen dazu benutzen können, um mehr über Ihre Person herauszufinden. Headhunter (Personalvermittlungsunternehmen) durchforsten bereits routinemäßig das Internet, um sich von zukünftigen Kandidatinnen oder Kandidaten ein Bild fernab der üblichen Bewerbungsunterlagen machen zu können. Gerade hier können sich **virtuelle Jugendsünden** sehr schnell **rächen,** da das **Internet solche Texte, Fotos oder auch Videos über einen längeren Zeitraum hinweg speichert.**

Geben Sie **keine persönlichen Daten wie Telefonnummer, Adresse, Wohnort oder Arbeitsplatz im Internet bekannt,** die jemand anderer dazu nutzen könnte, Sie im realen Leben aufzuspüren oder zu belästigen. Seien Sie sehr selektiv bei der Weitergabe und überlegen Sie immer, ob Sie die Daten im realen Leben auch so leichtfertig weitergeben würden.

Wählen Sie für die Benutzung Ihres Social Network Profils ein Passwort, das nur Sie kennen und geben Sie das Passwort auf gar keinen Fall jemandem anderen weiter. Auch wenn es für Sie einen Aufwand bedeutet ist es unbedingt zu empfehlen, **für verschiedene Soziale Netzwerke verschiedene Passwörter zu verwenden** und auch **regelmäßig zu wechseln.** In den letzten Jahren sind die Fälle von ☛ *Cyber-Mobbing* aufgrund gestohlener oder ausspionierter Passwörter angestiegen, die Folgen waren für die betroffenen Personen oft gravierend.

☛ Cyber-Mobbing: Bloßstellung, permanente Belästigung oder Verbreitung falscher Behauptungen über eine Person im Internet.

Sollten Sie auf Ihrem Profil Fotos, Videos oder Texte veröffentlichen, so stellen Sie sicher, dass Sie auch die Urheberin oder der Urheber sind. Achten Sie außerdem darauf, dass Sie mit der Veröffentlichung nicht „die berechtigten Interessen der abgebildeten Person“ verletzen. Dargestellte Personen haben ein **„Recht am eigenen Bild“,** das ihnen das Recht einräumt, bei Bloßstellung oder nachteiliger Darstellung rechtlich gegen die Veröffentlichung vorzugehen. Wollen Sie sich also Ärger ersparen, fragen Sie die Betroffenen vorher um ihre Zustimmung.

Einige Soziale Netzwerke bieten die Möglichkeit, kleine Applikationen selbst zu programmieren und dann in die Seiten der Sozialen Netzwerke einzubinden. Diese Programme haben ein großes Spektrum und reichen vom Übersenden einer virtuellen Blume bis hin zu einer ausgefeilten Kalender-Applikation. Doch auch hier ist Vorsicht geboten, da einige dieser Programme auch schon dazu verwendet wurden, ☛ *Trojaner* auf die Festplatte der Nutzerinnen und Nutzer zu installieren. **Seien Sie daher immer misstrauisch, wenn Ihnen ein solches Programm anbietet, etwas auf Ihrem Computer oder Mobiltelefon zu installieren.**

☛ Trojaner:
Ein Programm, das vorgibt, etwas anderes zu sein, als es tatsächlich ist. Die Grenze zwischen Trojanern und Viren ist heute nur noch schwer zu ziehen, da die meisten derartigen Schädlinge beide Funktionen beinhalten.

☛ Spam:
Ein Sammelbegriff für jede Art von unerwünschter E-Mail.

Immer wieder benutzen **unseriöse Firmen** Social Network Plattformen auch zur **Datensammelung oder Verbreitung von** ☛ *Spam:* So passierte es schon vielen Menschen in diversen Sozialen Netzwerken, dass sie nach dem Klick auf einen Link neuerlich zur Eingabe des Passwortes aufgefordert wurden. Es handelte sich dabei um von Spammern gefälschte Login-Seiten die nur dazu dienten, an persönliche Login-Informationen zu kommen. Kurze Zeit später erschienen dann in den Gästebüchern oder Mailboxen von Freunden Werbemails, die angeblich von den betreffenden Personen abgesandt wurden. Sollte Ihnen Derartiges passieren, informieren Sie umgehend die Betreiber der Plattform, entschuldigen Sie sich bei Ihren Kontakten und ändern Sie schnell Ihr Passwort!

Was tun, wenn Daten über Sie existieren, die zu Ihrem Nachteil sind?

Als Faustregel gilt hier: **umso schneller Sie nachteilige Fotos, Videos oder Texte entdecken, umso höher ist die Wahrscheinlichkeit, dass die Verbreitung noch nicht weit fortgeschritten ist.** Entdecken Sie also beispielsweise ein Foto, das Sie angeheitert bei der letzten Party zeigt, dann wenden Sie sich an die Person die das Foto veröffentlicht hat und fordern Sie diese Person auf, es zu entfernen.

Sollte diese Person nicht reagieren oder für Sie nicht erreichbar sein, dann wenden Sie sich an die Betreiberin oder den Betreiber der Webseite. **Alle österreichischen Webseiten sind mittlerweile gesetzlich dazu verpflichtet, Informationen über die betreibenden Personen auf der Webseite offen zu legen.** Demnach muss jede Webseite Angaben über den Namen des Medieninhabers, den Unternehmensgegenstand und den

Sitz des Medieninhabers machen (genaueres im Kapitel „Welche Angaben müssen Sie auf Ihrer Webseite machen“, S. 60). Im Impressum können Sie also in der Regel Kontaktdaten finden, an die Sie sich wenden können.

In den meisten Fällen werden die betreibenden Personen auf Ihr Anliegen positiv reagieren und für die Entfernung der Daten sorgen. Sollten Sie mit all diesen Maßnahmen keinen Erfolg haben, bleibt Ihnen immer noch als letzte Möglichkeit, die österreichischen Gerichte zu bemühen.

Mittlerweile gibt es sogar so genannte **Reputation Management Agenturen,** die sich gegen Bezahlung mit dem „guten Ruf“ von Privatpersonen im Internet beschäftigen. Sie sorgen dafür, dass positive Kommentare oder Artikel über die eigene Person existieren und kümmern sich um die **Entfernung von kompromittierendem Material.**

Ausstieg aus Sozialen Netzwerken, oder: Digitale Leichen

Sollten Sie – aus welchen Gründen auch immer – Ihr Profil in einem Sozialen Netzwerk löschen wollen, so werden Sie damit konfrontiert, dass es gar nicht so leicht ist, seine virtuelle Identität einfach verschwinden zu lassen. Bei vielen Sozialen Netzwerken kann das eigene Profil nicht gelöscht, sondern nur stillgelegt werden. Auch hier gilt: An die Betreiberinnen oder Betreiber des Sozialen Netzwerks schreiben und sie dazu auffordern, das Profil endgültig zu löschen und danach überprüfen, ob Ihrem Wunsch nachgekommen wurde. Wenn Sie sich nicht sicher sind, ob Sie Ihre Daten für immer löschen möchten, bieten manche Netzwerke auch die Möglichkeit an, das eigene Profil vor dem endgültigen Löschen aus dem Internet herunterzuladen.

Im Internet existieren mittlerweile auch eigene Hilfeseiten, wie ein Social Network Profil endgültig gelöscht werden kann. Je nachdem welche Social Network Plattform benutzt wurde, gibt es dazu verschiedene Infos im Netz. Bedenken Sie: **Auch wenn Sie Ihr Profil löschen, müssen Sie immer damit rechnen, dass Daten im Netz zurück bleiben** (z. B. auf archive.org, im Google-Cache, etc.).

Location Based Services

Wo war ich gestern? Was habe ich gemacht und mit wem? Falls die eigene Erinnerung hier einmal aussetzt, bekommen diese Fragen mit so genannten ☛ *„Location Based Services"* eine völlig neue Bedeutung. Die derzeit bekanntesten Location Based Services sind → Foursquare, Gowalla und Facebook Places.

→ www.foursquare.com
→ www.gowalla.com
→ www.facebook.com

Location Based oder Check-In Services sind kleine Programme, die **per ☛ *GPS* des Smartphones den aktuellen Aufenthaltsort lokalisieren können.** Aufgrund dieser standortbezogenen Daten werden einem in der Applikation Orte vorgeschlagen (Lokale oder Plätze die sich im unmittelbarem Umkreis befinden), bei denen man sich „einchecken" kann.

☛ Location Based Services: Standortbezogene Dienste, die selektive positionsabhängige Informationen bereitstellen.

Für solche **Check-Ins oder Anmeldungen stehen bereits vorab eine Auswahl an Orten zur Verfügung,** oder es können eigenständig Orte erstellt werden. Ist also das Lieblingslokal noch nicht vorhanden und man möchte gerne einchecken, ist es mit ein paar Schritten möglich, dieses dauerhaft und für alle verfügbar anzulegen.

☛ GPS: Global Positioning System ist ein Satelitensystem das der Positionsbestimmung dient.

Durch das Einchecken oder das Erstellen von Tipps, können Punkte oder so genannte „Badges" gesammelt werden. Sie dienen als eine Art Belohnungssystem für jegliche Art von Aktivität. Checkt man sich an einem Ort öfter ein, besteht die Möglichkeit, „Mayor" („Bürgermeister") zu werden. Während man für die gesammelten Punkte oder Badges im realen Leben nicht wirklich etwas bekommt, haben manche Lokale oder Geschäfte dieses System für sich entdeckt und nutzen es als Werbeplattform: Sie bieten diverse Specials wie Gratis-Getränke oder sonstige Benefits an, meldet man sich bei ihnen über ein Location Based Service an.

Ob die Nutzung von Location Based Services Sinn macht oder nicht, sollte jeder für sich selbst entscheiden. Menschen die Wert auf ihre Daten und ihre Anonymität legen, werden diese Software vermutlich nicht auf ihrem Handy installieren. Auch wenn man sich bei manchen Services „unsichtbar" einchecken kann (um beispielsweise einen Badge oder ein Goodie zu erhalten), ist die **Kontrolle über die eigenen Daten sehr eingeschränkt.** Hat man sich einmal bei einem Ort eingecheckt, kann der Check-In nicht mehr rückgängig gemacht werden.

TIPP

Auf der Webseite von → Saferinternet.at gibt es unter dem Menüpunkt „Soziale Netzwerke“ die Frage „Wie nutze ich soziale Netzwerke sicher?“. Dort finden Sie bei „Weiterführende Links“ ausführliche Leitfäden zum Schutz der Privatsphäre für die wichtigsten Sozialen Netzwerke in Österreich als Download.

www.saferinternet.at

Sicherheit für Kinder & Jugendliche

Die Jugend-Medien-Studie des Bildungsmedienzentrums des Landes Oö kommt zu dem Ergebnis, dass 90% der befragten Jugendlichen einen Computer oder Laptop zu Hause haben. Immerhin 62% dürfen ihren Computer uneingeschränkt benützen, 86% haben in ihrem Elternhaus auch einen Internetzugang. An erster Stelle nutzen die Jugendlichen den Computer zur Informationssuche, an zweiter Stelle zum Schreiben von E-Mails, gefolgt von Musikdateien anhören, chatten und der Nutzung von Online-Communitys.

Quelle: www.bimez.at

„Meine Freundin/mein Freund hat ..."
Überwachung des Nachwuchses per Software
Elterliche Medienkompetenz
Maßnahmen zum Schutz Ihrer Kinder
Für die Jüngsten
Positivlisten
Kommerzielle Filterprogramme
Cyber-Mobbing
Happy Slapping
Sexualität & Internet
Virtuelle Jugendsünden – Persönliche Daten
Prepaid Kreditkarten für Jugendliche

Sicherheit für Kinder und Jugendliche bei der Benutzung des Internet ist ein sehr präsentes Thema geworden, da immer mehr Kinder und Jugendliche das Internet nutzen und dabei - wie bei allen Medien - die Anwendung erst erlernen müssen. Sie brauchen dabei Unterstützung, auch wenn es oft so aussieht, als ob Kinder und Jugendliche mit neuen Medien besser umgehen können, als so manche Erwachsene.

Prinzipiell gilt: **Sprechen Sie mit Ihrem Kind über seine Mediennutzung** und seien Sie aufmerksam, wenn es Fragen hat. Selbst wenn Sie wahrscheinlich nicht alle Fragen beantworten können ist es wichtig, auch hier ein **Vertrauensverhältnis mit Ihrem Kind aufzubauen.** Davon können beide Seiten profitieren: Ihr Kind, das somit Erwachsene als Ansprechpartnerinnen oder -partner hat wenn es in Situationen kommt, mit denen es nicht umgehen kann, und Sie, um über die Mediennutzung Ihres Kindes Bescheid zu wissen.

Sorgen Sie außerdem dafür, dass der Computer Ihres Kindes an einem Platz steht, wo Sie Ihrem Kind bei Fragen auch zur Verfügung stehen können. Ein Computer im Kinderzimmer schottet Ihr Kind ab und bedeutet eine Hürde, falls Ihr Kind Fragen hat. Wie auch beim Medium Fernseher, sollte **das Internet nie als Babysitter missverstanden werden.**

„Meine Freundin/mein Freund hat …“

Ein beliebter Satz von Kindern und Jugendlichen, um auf Situationen mit denen sie nicht umgehen können aufmerksam zu machen ist übrigens: „Stell dir vor, meinem Freund/meiner Freundin ist da etwas ganz Schlimmes passiert…“. Oft handelt es sich dabei um eigene Erlebnisse, die so viel Betroffenheit auslösen, dass darüber nur in der dritten Personen gesprochen werden kann. **Seien Sie in so einem Fall auf jeden Fall hellhörig und nehmen Sie diese Fragen ernst!** Sprechen Sie mit Ihrem Kind ausführlich darüber, erarbeiten Sie gemeinsam Lösungsansätze und vor allem: fragen Sie immer wieder nach!

Überwachung des Nachwuchses per Software

In den letzten Jahren ist es außerdem üblich geworden, dass Software-

unternehmen aller Art auf die Möglichkeit hinweisen, den Internet-Konsum von Kindern lückenlos zu überwachen. Bei den meisten handelsüblichen Betriebssystemen gibt es die Funktion, verschiedene Benutzerinnen oder Benutzer anzulegen und dann unterschiedliche Rechte für die einzelnen Konten zu vergeben. Dort können beispielsweise Zeitbeschränkungen gewählt, oder aber auch alle im Browser besuchten Seiten beschränkt oder überwacht werden.

Bevor Sie jedoch diese Maßnahmen ergreifen, sprechen Sie mit Ihrem Kind darüber. Es ist nicht sehr vertrauensfördernd, wenn Sie den Internet-Konsum Ihres Kindes heimlich überwachen und Ihrem Kind bei einer Regelübertretung den Zugang zum Internet sperren. Auch hier lautet die Devise: **Bauen Sie ein Vertrauensverhältnis auf und besprechen Sie mit Ihrem Kind, welche technischen Möglichkeiten es gibt und welche Sie davon nutzen werden.**

Setzen Sie sich gemeinsam mit Ihrem Kind hin und besprechen Sie die besuchten Seiten. Fragen Sie Ihr Kind, warum es welche Seiten besucht hat. Sollten Seiten mit problematischen Inhalten dabei sein, sprechen Sie mit Ihrem Kind offen darüber und erklären Sie, warum die besuchten Inhalte nicht kindergerecht sind. **Weisen Sie auf etwaige Gefahren hin und schlagen Sie Alternativen vor.**

Es hat keinen Sinn, Ihrem Kind zu verschweigen, dass es die Möglichkeit gibt, seinen Internet-Konsum zu überwachen. Sie können davon ausgehen, dass Schulfreundinnen und -freunde Ihr Kind über derartige Möglichkeiten aufklären werden. Außerdem: **Auch Kinder haben so etwas wie ein Recht auf eine eigene Privatsphäre,** oder hätten Sie es gut gefunden, wenn Ihre Eltern heimlich Ihr Tagebuch gelesen hätten?

Elterliche Medienkompetenz

Zu guter Letzt: Interessieren Sie sich für die Medien, die Ihr Kind nutzt. Viele Eltern vertreten die Meinung, dass Ihre Kinder ohnehin besser mit neuen Medien umgehen können, als sie selbst und haben es aufgegeben, sich damit zu beschäftigen. Aber: als Elternteil haben Sie auch hier eine Verantwortung, die Sie wahrnehmen sollten.

Eignen Sie sich selbst Medienkompetenz an und versuchen Sie, mit dem Wissen Ihrer Kinder Schritt zu halten. Sich mit neuen Medien zu beschäftigen ist auf alle Fälle eine Erweiterung des eigenen Wissenshorizonts. Mittlerweile bieten fast alle **→ Volkshochschulen Computerkurse** zu den verschiedensten Themen an, die sowohl für Anfängerinnen oder Anfänger als auch für Fortgeschrittene geeignet sind.

→ www.vhs.at

Falls Sie nicht weiterwissen, können Sie immer noch Ihre Kinder fragen. Obwohl das für Sie als Elternteil vielleicht ungewohnt ist, kann dieser Wechsel der Rollen (die normalerweise von Eltern und Kindern eingenommen werden), für beide Seiten eine lohnende Erfahrung sein. Wenn Sie also wissen, dass Ihr Kind sich gut auskennt, machen Sie Gebrauch von der Möglichkeit, Ihr Kind um Hilfe zu bitten.

Maßnahmen zum Schutz Ihrer Kinder

Im Internet kann es immer wieder passieren, dass Kinder und Jugendliche mit Inhalten konfrontiert werden, die auf den Bildschirmen von unter 18-jährigen nichts verloren haben. Es ist leider gar nicht so einfach, das Internet kindersicher zu machen und gerade bei jüngeren Kindern und Jugendlichen sind dem jeweiligen Alter entsprechende Maßnahmen notwendig. In den folgenden Absätzen finden Sie eine Übersicht aller Möglichkeiten, die dazu dienen sollten, Ihren Kindern ein sicheres Surfen zu ermöglichen.

Für die Jüngsten

Es ist empfehlenswert, **jedem Kind ein eigenes Benutzerkonto** anzulegen, um die Rechte der verschiedenen Benutzerinnen oder Benutzer besser verwalten zu können. Bei jüngeren Kindern ist es zuallererst sinnvoll, eine **altersgerechte Startseite und eigene Bookmarks** (auch Lesezeichen oder Favoriten genannt) zu erstellen.

Als Startseite können Sie eine Seite wählen, die Ihr Kind gerne besucht und in den Bookmarks können Sie eine Liste von Seiten erstellen, die für Ihr Kind geeignet sind. **Nehmen Sie sich im Vorfeld Zeit, schauen Sie sich die Seiten durch und entscheiden Sie dann, ob die Inhalte für**

Ihre Kinder geeignet sind. Empfehlungen für kindgerechte Webseiten finden Sie auf diversen Kindersuchmaschinen wie → „kinder.at“, „fragFinn“, „Seitenstark“, Klick-Tipps“ oder „Blinde Kuh“.

→ www.kinder.at
→ www.fragfinn.de
→ www.seitenstark.de
→ www.blinde-kuh.de
→ www.klick-tipps.net

Meist interessieren sich jüngere Kinder ohnehin nur für eine geringe Anzahl von Webseiten, die über die Bookmarks ganz gut gesteuert werden können. Mit einer zu großen Auswahl an angebotenen Webseiten sind gerade jüngere Kinder oft überfordert. Kinder, die noch nicht lesen oder schreiben können, orientieren sich eher an Bildern und benötigen daher eine grafisch aufbereitete Oberfläche.

Positivlisten

Mit einer Positivliste können Sie eine Liste der Webseiten erstellen die Ihr Kind besuchen darf und schließen dabei gleichzeitig alle anderen Seiten aus. Einmal eingerichtet, kann Ihr Kind alle auf der Liste befindlichen Seiten auswählen und hat keine Möglichkeit andere Seiten anzusteuern, da die Verwaltung dieser Positivlisten mit einem Passwort geschützt ist.

→ support.microsoft.com
→ addons.mozilla.org

Im → Microsoft Internet Explorer gibt es den so genannten „Inhaltsratgeber“ mit dem die Positivlisten verwaltet werden können, im → Mozilla Firefox muss dazu das Add-On FoxFilter installiert sein.

Kommerzielle Filterprogramme

Programme wie

→ www.netnanny.com
→ www.internetsafety.com
→ www.cybersitter.com
→ www.cyberpatrol.com
→ www.kindersicherung.de

- Net Nanny,
- Safe Eyes,
- CyberSitter,
- CyberPatrol,
- Kindersicherung 2011

u. a. müssen auf Ihrem Computer installiert werden und regulieren, welche Websites gefiltert und welche angezeigt werden. Diese Programme verwenden dabei **eine Mischung aus Positivlisten** (also bestimmte Seiten können entweder explizit erlaubt oder verboten werden) und einer

Sperre aufgrund diverser Stichwörter (z. B. Porno, Nazi oder Sex). Zum Teil wird auch die Verwendung anderer Programme am Computer eingeschränkt (z. B. verschiedene ☛ *Instant Messaging Programme).*

☛ Instant Messaging Programme:
Instant Messaging bezeichnet den sofortigen und unmittelbaren Versand einer Textnachricht. Meist erscheint die Nachricht in Echtzeit am Bildschirm der Empfängerin oder des Empfängers.

Diese Programme gehen allerdings davon aus, dass sich Eltern auf der ganzen Welt einig sind, welche Seiten ein Kind einer bestimmten Altersstufe sehen darf und welche nicht. In der Realität ist es aber so, dass skandinavische Eltern üblicherweise ganz andere Vorstellungen von Jugendschutz haben, als Süditalienische oder Arabische.

Mit dem Erwerb eines dieser Programme **kaufen Sie** sozusagen auch **die Werthaltungen des Unternehmens,** das diese Produkte herstellt, ein. Denn welche Seiten genau gefiltert werden, ist schließlich das Geheimnis des Unternehmens und damit nicht kontrollierbar. Es ist bei Tests beispielsweise schon öfter vorgekommen, dass gerade Aufklärungsseiten, die sich an Jugendliche richten, nicht aufgerufen werden können.

Bitte bedenken Sie: **Filterprogramme können keinen vollständigen Schutz gewährleisten.** Es kommt immer wieder vor, dass ungeeignete Inhalte angezeigt werden und erwünschte Inhalte gefiltert werden. Außerdem sind Filter in Tauschbörsen, Chats und E-Mail Programmen wirkungslos und können dort keinen Schutz bieten.

Das Internet ist groß, vielfältig und ein weltweites Medium. Kinder, die dem Volksschulalter entwachsen sind, sind oft erfahrener im Umgang mit dem Netz als ihre Eltern. Dadurch besteht die Gefahr, dass nicht alles abgeschirmt werden kann oder dass die Kinder in kürzester Zeit lernen, diverse Filtermechanismen zu umgehen.

GROOMING

Als „Grooming“ wird die Kontaktanbahnung von Pädophilen mit Kindern bezeichnet, wobei sich die Erwachsenen als Jugendliche ausgeben um sich aus pädophilen Motiven mit Kindern zu befreunden. Dabei gehen sie sehr subtil vor und versuchen eine Beziehung zu ihren Opfern herzustellen und ihnen möglichst viele Informationen über ihren Wohnort, Interessen oder Hobbys zu entlocken. Oft schicken Pädophile den Kindern pornografische Bilder (sowohl von Erwachsenen als auch von Kindern),

um ein Gefühl von Akzeptanz und Normalität zu schaffen. Ziel dieser Menschen ist es, die Zurückhaltung der Kinder zu untergraben und sie durch Schuldgefühle gleichzeitig davon abzuhalten, Hilfe bei Eltern oder anderen Vertrauenspersonen zu suchen.

Cyber-Mobbing

In den letzten Jahren hat sich das so genannte Cyber-Mobbing (oder auch Bullying) unter Kindern und Jugendlichen zu einem immer größer werdenden Problem entwickelt. Cyber-Mobbing ist im Prinzip dasselbe wie Mobbing, nur dass es sich im Internet oder per Handy abspielt. Dabei handelt es sich um **absichtliches Beleidigen, Bloßstellen, Bedrohen oder Belästigen von Personen im Internet oder mit dem Handy und das über einen längeren Zeitraum hinweg.**

Solche Mobbing-Attacken können über die verschiedensten Kanäle passieren (E-Mail, Instant Messaging, in Sozialen Netzwerken, in Chatrooms, in Diskussionforen, etc.) und sind im Internet durch die rasche Verbreitung oft nur sehr schwer wieder zu entfernen.

Sollte Ihr Kind Opfer von Belästigungen werden, **unterstützen Sie es** in erster Linie **bei der Verarbeitung und seien Sie immer für ein Gespräch bereit.** Sollte Ihnen das nicht gelingen, suchen Sie sich externe Hilfe von Freunden, Bekannten, Lehrenden oder → professionellen Hotlines. Versuchen Sie außerdem die Täterin oder den Täter zu identifizieren und fordern Sie sie oder ihn auf, jegliche weitere Belästigung zu unterlassen. **Stalking (also das beharrliche Verfolgen von Opfern) ist in Österreich seit dem Jahr 2006 strafbar, Sie haben im Härtefall also Unterstützung von den Strafverfolgungsbehörden** (siehe dazu Kapitel „Cybercrime“, S. 88).

→ Rat auf Draht: ☎147
→ www.rataufdraht.at
→ www.saferinternet.at

In den meisten Fällen reicht es jedoch, wenn Sie die Eltern der Täterin oder des Täters informieren und sich an die verantwortlichen Personen in der Schule Ihres Kindes wenden. Das Thema Mobbing bzw. Cyber-Mobbing wird mittlerweile in den meisten Schulen sehr ernst genommen.

Um Inhalte wie Fotos, Videos oder Nachrichten entfernen zu lassen, kontaktieren Sie die betreibenden Personen der Webseiten und ersuchen Sie

um Entfernung. In den meisten Fällen werden Sie auf Entgegenkommen treffen, da die diversen Plattformen kein Interesse daran haben, mit Cyber-Mobbing in Verbindung gebracht zu werden.

Versuchen Sie Ihr Kind in diese Aktivitäten mit einzubinden damit es nicht das Gefühl hat, derartigen Belästigungen hilflos ausgeliefert zu sein. Versuchen Sie außerdem, gemeinsam Strategien zu entwickeln, damit es nicht neuerlich zu derartigen Belästigungen kommen kann (z. B. die Weitergabe von persönlichen Daten).

Als Elternteil sollten Sie außerdem damit rechnen, dass Ihr Kind unter Umständen vom Opfer zur Täterin oder zum Täter wird. Internationale Untersuchungen haben ergeben, dass sich der Wechsel zwischen diesen beiden Rollen oft relativ rasch vollzieht und dass die Eltern meist in dem Glauben leben, dass die eigenen Kinder so etwas nie tun würden.

Happy Slapping

Beim so genannten „Happy Slapping" werden Personen meist grundlos tätlich angegriffen und die dabei gefilmten Szenen werden entweder gleich an andere → Handys weitergeschickt, oder übers Internet verbreitet.

→ www.handywissen.at

Die technischen Ausstattungen der Handys machen dieses Vorgehen ohne spezielle technische Vorkenntnisse möglich, **seien Sie also aufmerksam, welche Daten Ihr Kind auf seinem Handy hat** und sprechen Sie mit Ihrem Kind über derartige Aufnahmen. Erklären Sie, warum es falsch ist, solche Aufnahmen zu verbreiten und signalisieren Sie Bereitschaft zur Hilfe, falls Ihr Kind in eine derartige Situation kommen sollte.

Sexualität & Internet

Es gehört zu einem ganz normalen Entwicklungsprozess, dass Kinder und Jugendliche ab dem Zeitpunkt ab dem sich die eigene Sexualität entwickelt, intime Fragen weniger mit den Eltern besprechen als mit gleichaltrigen. Sie versuchen auch oft, Fragen die sie über das Erwachsen werden und der damit verbundenen Entwicklung des eigenen Körpers haben,

über diverse Informationsschienen zu beantworten.

Dabei hat sich das **Internet als beliebte Quelle** aufgetan, da hier völlig anonym Antworten auf die meisten Fragen gefunden werden können. Dass Jugendliche dabei nicht immer auf Material stoßen, das ihrem Alter und dem Stand ihrer Entwicklung entspricht, kommt vor. Aber auch hier ist kein Grund zur Sorge, denn je mehr **Basiswissen zum Thema Sexualität** vorhanden ist, je größer der **positive Zugang zum eigenen Körper** und je mehr professionelle Informationsquellen zum Thema Sexualität erlaubt und angeboten werden, umso weniger werden sich Jugendliche in ihrer sexuellen Entwicklung beeinträchtigt zeigen.

Als Elternteil ist hier Ihr Einsatz gefragt, indem Sie sich Informationen zum Thema Sexualerziehung besorgen. Sprechen Sie mit Ihrem Kind über **altersadäquate Informationsmöglichkeiten aus dem Internet** oder in Form von Büchern und Broschüren. Fördern Sie das Körperbewusstsein Ihres Kindes durch z.B. Sport oder Tanzworkshops und unterstützen Sie (parallel dazu) Ihr Kind, ein kritisches Bewusstsein für den Umgang mit Medien zu entwickeln. Sollten Sie sich mit dem Thema Sexualität und Internet eingehender beschäftigen wollen, empfehlen wir den Elternratgeber „Sexualität & Internet“ von → Saferinternet.at.

→ www.saferinternet.at

SEXTING

„Sexting“ ist aus den Wörtern „Sex“ und „Texting“ (engl. Ausdruck für das Erstellen einer SMS) zusammengesetzt und beschreibt den Trend, dass Jugendliche erotische Fotos von sich selbst oder anderen machen und diese dann per Handy an Freundinnen und Freunde oder Bekannte verschicken. Oft landen diese Fotos dann in Sozialen Netzwerken oder Foto-Communitys. Die Verbreitung lässt sich nur mehr schwer stoppen.

Virtuelle Jugendsünden – Persönliche Daten

Auch wenn es den wenigsten Menschen bewusst ist: **das Internet ist eine sehr große Sammelstelle für persönliche Daten jeder Art, hat ein weltweites Publikum und es vergisst nicht sehr schnell.** Ist ein Foto

beispielsweise erst einmal irgendwo öffentlich zugänglich gespeichert, kann es beliebig oft kopiert und auch abgerufen werden (siehe dazu auch Kapitel „Soziale Netzwerke“ s. S. 30). Gerade bei den bei Jugendlichen sehr beliebten Social Network Sites werden Fotos oft auch dann noch gespeichert, wenn sie von der eigentlichen Benutzerin oder vom eigentlichen Benutzer bereits gelöscht wurden.

Klären Sie Ihr Kind darüber auf, dass **einmal veröffentlichte Fotos jederzeit kopiert und weiter verbreitet werden können** und versuchen Sie bei Ihrem Kind Bewusstsein dafür zu schaffen, dass die Veröffentlichung eines Fotos einem Anschlag am schwarzen Brett in der eigenen Schule gleichkommt.

Fotos von der letzten Party, die Ihr Kind bei den ersten Alkohol- oder Liebeserfahrungen zeigt, können sich bei der späteren Arbeitssuche nachteilig auswirken. Klären Sie Ihr Kind darüber auf, was eine freizügige Veröffentlichung von privaten Fotos oder Videos für Konsequenzen haben könnte und versuchen Sie gemeinsam Alternativen zu finden (z. B. andere Fotos oder eingeschränkter Benutzerkreis).

Sollte eine andere Person derartige Fotos von Ihrem Kind ins Netz stellen und Sie oder Ihr Kind damit nicht einverstanden sein, fordern Sie die Person auf, die Fotos zu entfernen. Rechtlich haben Sie dafür auch eine Grundlage, denn jede Person hat ein **„Recht am eigenen Bild“ bei der eine Veröffentlichung die die berechtigten Interessen der abgebildeten Person verletzen, unzulässig ist.** Klären Sie Ihr Kind über dieses Recht auf und ermuntern Sie es, zuerst eine Einwilligung von Freundinnen oder Freunden einzuholen, wenn es selbst Fotos veröffentlichen möchte.

Raten Sie Ihrem Kind, keine persönlichen Daten (Adresse, Wohnort, Telefonnummer) zu veröffentlichen, die es Fremden ermöglichen, Ihr Kind im „realen“ Leben aufzuspüren oder zu belästigen. Auch sollten Treffen mit virtuellen Bekanntschaften, so genannte **„blind dates“ niemals ohne Begleitperson** stattfinden. Erklären Sie Ihrem Kind, warum solche Treffen gefährlich sein können.

Prepaid Kreditkarten für Jugendliche

Wie bereits im Kapitel „Bezahlen im Netz“ (s. S. 20) beschrieben, gibt es mittlerweile Prepaid Kreditkarten, die sich für Jugendliche gut eignen. Diese Karten werden bereits von den meisten Kreditkarten-Firmen angeboten und können bis zu einem bestimmten Betrag (per Überweisung oder Barzahlung) aufgeladen werden. Es kann damit überall dort bezahlt werden, wo Sie normalerweise mit einer herkömmlichen Kreditkarte bezahlen, mit dem PIN-Code kann auch Bargeld behoben werden. Diese Art der Bezahlung bietet den Vorteil, dass sie relativ sicher ist und dass die Karte bei missbräuchlicher Verwendung nur bis zu dem aufgeladenen Betrag behoben werden kann.

Communitys, Foren, Chats

Eine Online-Community (Netzgemeinschaft) ist eine Sonderform der Gemeinschaft, die sich einander via Internet begegnet und austauscht. Findet die Kommunikation in einem sozialen Netzwerk statt, das als Plattform zum gegenseitigen Austausch von Meinungen, Eindrücken und Erfahrungen dient, wird auch von sozialen Medien gesprochen. Eine Online-Community entwickelt sich dann erfolgreich, wenn die treibende Kraft nicht die Marketingidee eines Unternehmens ist, sondern sie sich aus sich selbst, also den Wünschen der Gemeinschaft, entwickeln kann.

Quelle: de.wikipedia.org

Regel Nummer 1: Erst lesen, dann schreiben
Regel Nummer 2: Nie mit Wut im Bauch schreiben
Regel Nummer 3: Vorgesetzte lesen mit
Ehrenbeleidigung
Üble Nachrede
Verleumdung
Kreditschädigung
Illegale Foren und Chats

Eine ☛ *Online-Community* ist eine Art virtueller Treffpunkt für Gleichgesinnte, die entweder dasselbe Hobby oder dieselben Interessen haben und sich in Diskussionsforen oder Chats darüber austauschen möchten. Dabei gibt es einige wenige Grundregeln, die Sie beim kommunizieren einhalten sollten:

☛ Community:
Gemeinschaft, die sich aufgrund gemeinsamer Interessen zusammengefunden hat und Austausch über Diskussionsforen, Chats oder auch Linksammlungen pflegt.

Regel Nummer 1:
Erst lesen, dann schreiben

Es ist wie im richtigen Leben: Wenn Sie in einem fremden Land ein Lokal betreten, sollten Sie halbwegs im Bilde sein, wie die Bräuche dieses Landes im Allgemeinen und die Regeln eines Lokals im Speziellen sind. In einem islamischen Land werden Sie sich anders verhalten als an 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 können Sie diese auch auf den zugehörigen Websites nachlesen), und wenn Sie sich als Neuling nicht an diese halten, gelten Sie im besten Fall als unhöflich, im schlechteren als dämlich.

Deshalb ist es nützlich, sich ein wenig einzulesen, bevor Sie sich selbst zu Wort melden, und sei es nur mit einer Frage. Alteingesessene ☛ *Netizens* wollen nicht ständig dieselben Fragen beantworten, deshalb haben Communitys oft ☛ *FAQ's* online.

☛ Netizens:
Ein bereits leicht veraltetes Kunstwort aus „Network“ und „Citizen“, also sozusagen „Netzbürgerinnen oder Netzbürger“ oder „Bewohnerin/Bewohner des Netzes“.

☛ Frequently Asked Questions (FAQ):
Sind eine Zusammenstellung häufig gestellter Fragen zu einem Themenbereich oder zu einer Website.

Regel Nummer 2:
Nie mit Wut im Bauch schreiben

Die Tatsache, dass sich die teilnehmenden Personen in Online-Communitys nicht sehen können, verführt leicht zu einer etwas derberen Ausdrucksweise, als sie im richtigen Leben gebraucht wird.

Bedenken Sie daher immer, dass am anderen Ende der Leitung ein richtiger Mensch sitzt. So banal dieser Tipp ist, so wenig wird er oft beachtet.

Wenn nämlich alle ihre Wut nicht ungezügelt loslassen würden, sondern mit dem Abschicken des Postings oder des Chat-Beitrages einen Tag zuwarteten, dann wären die unten stehenden Kapitel, die sich mit rechtlichen Konsequenzen beschäftigen, obsolet.

Regel Nummer 3: Vorgesetzte lesen mit

Was von der so genannten Anonymität im Netz zu halten ist, wird in einem eigenen Kapitel erörtert (Kapitel „Anonymität und Identität“, S. 102). Wenn Sie in einer Community etwas von sich geben, gehen Sie daher immer davon aus, dass Ihre Vorgesetzten, Ihre Eltern, die Polizei und Ihre Partnerin oder Ihr Partner mitlesen.

Nur wenn Sie diese Regel beachten, werden Sie nie ein schlechtes Gewissen haben müssen. Und falls Sie darauf hoffen, dass alles irgendwann einmal gelöscht wird: Es gibt etliche → Seiten im Netz, die darauf spezialisiert sind, Inhalte von Websites oder Diskussionsforen für alle Ewigkeit zu archivieren. Diese Hoffnung ist also trügerisch.

→ www.archive.org

Wenn Sie diese drei Regeln nicht beachten: Welche rechtlichen Konsequenzen können daraus entstehen?

Ehrenbeleidigung

Beleidigen Sie eine Person auf Ihrer eigenen Homepage, können Sie sich leicht strafbar machen.

Bei Foren und Chats ist die Sache nicht so klar, da die beteiligten Personen ja meistens anonym bleiben und eine Beleidigung nicht einer realen Person zugeordnet werden kann.

Manche sehen Beleidigungen jedoch schon als strafbar an, wenn eine Person regelmäßig in einem Forum oder Chat unter dem gleichen ☛ *Nickname* auftritt und dieser Person auf Grund von Beleidigungen die Verwendung des Nicknamens verleidet wird.

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

Gerade bei Foren und Chats ist es vom dort üblichen Umgangston abhängig, ab welchem Grad 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). 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 eigentlich immer von einer Öffentlichkeit ausgegangen werden.

Entschuldigt ist aber, wer sich zu einer Beleidigung hinreißen lässt, weil er auf eine Beleidigung eines anderen begreiflicherweise reagiert, also zurückschlägt. Der „Gegenschlag" muss aber rasch nach der ersten Beleidigung erfolgen; dies ist vor allem bei Chats bedeutsam. **Empfehlenswert ist diese Vorgangsweise aber jedenfalls nicht (s. o.).**

Der Strafrahmen für Ehrenbeleidigung beträgt bis zu drei Monaten, 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 ihre Wahrheit bewiesen werden. Straffrei bleiben Sie auch, wenn Sie eine fremde Äußerung zitieren, solange Sie sich nicht mit dem Inhalt identifizieren („In der Zeitung hab ich gelesen, dass …").

Wird die üble Nachrede einer breiten Öffentlichkeit zugänglich gemacht (z.B. im Internet), kann der Strafrahmen bis zu einem Jahr umfassen.

Verleumdung

Eine Verleumdung liegt vor, wenn Sie jemandem die Begehung einer Straftat vorwerfen, obwohl Sie wissen, dass der Vorwurf nicht zutrifft. Der Vorwurf muss aber so konkret sein, dass die betroffene Person eine behördliche Verfolgung (durch Polizei, Staatsanwaltschaft) zu erwarten hat („Der X hat gestern bei der Gumpendorfer Straße mit Heroin gedealt").

Die Strafe für Verleumdung kann je nach Schwere der vorgeworfenen Straftat entweder bis zu einem Jahr, oder bis zu 5 Jahren betragen.

Kreditschädigung

Auch die Behauptung von unrichtigen Tatsachen kann strafbar sein, wenn dadurch der Kredit, der Erwerb oder das berufliche Fortkommen anderer geschädigt oder gefährdet wird. Eine Freiheitsstrafe bis zu sechs Monaten kann verhängt werden.

Illegale Foren und Chats

In manchen Foren und Chats wird keineswegs nur über harmlose Themen diskutiert. Statt von Modellbau ist von Bombenbasteln, Drogenanbau etc. 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. So ist z. B. das Posting von Missbrauchsdarstellungen im Internet als Zugänglichmachen von Kinderpornografie strafbar (Strafrahmen: drei Jahre). Auch das Veröffentlichen einer Anleitung zur Herstellung von Drogen kann als Beihilfe zur Erzeugung strafbar sein (Strafrahmen: 6 Monate). Weiters ist die Mitwirkung an einem Selbstmord in Österreich strafbar. Es wäre z. B. denkbar, jemanden durch Bestärkung zum Selbstmord zu verleiten.

Eigene Homepage & Weblog

Ein Blog oder auch Weblog (Wortkreuzung aus World Wide Web und Log im Sinne von Logbuch) ist ein auf einer Website geführtes, meist öffentlich einsehbares Tagebuch oder Journal. Häufig ist ein Blog „endlos“, das heißt eine lange, abwärts chronologisch sortierte Liste von Einträgen. Die Bloggerin oder der Blogger ist für den Inhalt selbst verantwortlich, oft sind die Beiträge in der Ich-Perspektive geschrieben. Ein Blog bietet ein einfach zu handhabendes Medium zur Darstellung von Aspekten des eigenen Lebens und von Meinungen zu spezifischen Themen.

Quelle: de.wikipedia.org

Dürfen Sie Bilder oder Musik auf Ihrer Homepage/in Ihrem Blog verwenden?

Domain-Grabbing

Dürfen Sie auf illegale Seiten verlinken?

Welche Angaben müssen Sie auf Ihrer Website machen?

Die Impressumspflicht

§ 5 ECG – Informationen

Eine eigene Website zu haben ist nicht schwer, sie mit Inhalten zu füllen hingegen sehr.

Dürfen Sie Bilder oder Musik auf Ihrer Homepage/in Ihrem Blog verwenden?

Auch Fotos oder Grafiken sind – wie Musikstücke und Programme – **urheberrechtlich geschützt.** Wenn Sie ein fremdes Foto auf Ihre Homepage stellen wollen, dürfen Sie dies daher nur mit Zustimmung der Herstellerin oder des Herstellers. Bei Fotos, die Sie selbst hergestellt haben, worauf aber andere Personen abgebildet sind, müssen Sie auch die Abgebildeten fragen, ob Sie das Foto veröffentlichen dürfen (so genannter „Bildnisschutz").

Prinzipiell ist es nicht erlaubt, Musikstücke von Anderen auf die eigene Website zu stellen oder dort abspielen zu lassen, ohne eine Einwilligung dafür zu besitzen.

Wollen Sie aber ein bestimmtes Musikstück unbedingt verwenden, können Sie sich 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 die AKM einerseits durch Gewährung von Lizenzen, andererseits aber auch durch Kontrollen und Klagen bei Verstößen.

→ www.akm.or.at

Domain-Grabbing

Immer wieder gibt es Leute, die einen Internet-Domain-Namen nur aus dem Grund registrieren lassen, um diese später an Dritte, die ein begründetes Interesse an der Nutzung dieser ☛ *Domain* haben, möglichst gewinnbringend weiter zu verkaufen. **Geschieht die Registrierung nur, um z. B. die Konkurrenz in ihrer Tätigkeit zu behindern, liegt nach der Rechtsprechung des OGH eine unlautere Handlung vor,** und es ist mit Unterlassungs- und Schadenersatzansprüchen zu rechnen. Dieses Vorgehen wird als Domain-Grabbing bezeichnet und hat für denjenigen, der sich den Domainnamen unberechtigterweise sichert, in den letzten Jahren keinerlei Vorteile mehr gebracht.

☛ Domain:
Ist ein „Namensraum", der bei dafür verantwortlichen Registrierungsstellen beantragt werden kann. Für die Vergabe der „Top-Level"-Domain „.at" (die oberste Hierarchie-Ebene) ist die Firma nic.at verantwortlich. Unterhalb einer Domain können Namen von Services definiert werden, die auf verschiedene Rechner zeigen (z. B. ist www.xyz.at ein Rechnername der Domain xyz.at).

Wollen Sie also eine eigene Domain haben, so ist es ratsam, den eigenen Namen als Domain anzumelden (z. B. karli-meier.at) oder einen Fantasienamen zu suchen, den garantiert noch niemand anderer hat. Dies können Sie zum Beispiel mit einiger Sicherheit durch eine Google-Abfrage herausfinden. Domains können Sie übrigens bei einem Provider anmelden (eine Übersicht der österreichischen Provider findet sich auf der → ISPA-Webseite). Die meisten ☛ *Provider* haben auch eine Abfragemöglichkeit, mit der festgestellt werden kann, ob der gewünschte Domainname noch frei ist. Ob eine .at Domain noch frei ist, können Sie bequem auch auf der Webseite der Österreichischen Domain-Registry → nic.at nachschauen.

→ www.ispa.at

☛ Provider: Unternehmen, über das Sie Zugang zum Internet bekommen.

→ www.nic.at

Dürfen Sie auf illegale Seiten verlinken?

Problematisch wird Verlinken, wenn es sich um Seiten mit rechtswidrigen oder strafbaren Inhalten (wie z. B. Kinderpornografie) handelt. Eine Erklärung auf der eigenen Website, in der eine Distanzierung vom Inhalt der gelinkten Seiten ausgedrückt wird (so genannter „Disclaimer"), ist unwirksam!

Die Haftung für Fremdinhalte kann auf diese Weise nicht umgangen werden. Immerhin wird ja auf diese fremden Inhalte verwiesen. Jedoch haften Sie nicht, wenn Sie eine Website betreiben und Sie von den rechtswidrigen Inhalten tatsächlich keine Kenntnis hatten bzw. wenn Sie, sobald Sie davon Kenntnis erlangen, den Link entfernen.

Strafrechtlich bedenkliche Websites mit kinderpornografischen oder nationalsozialistischen Inhalten können bei der anonymen Meldestelle der ISPA → Stopline oder beim Bundesministerium für Inneres (BMI) unter der Rubrik „Meldestellen" gemeldet werden.

→ www.stopline.at

Welche Angaben müssen Sie auf Ihrer Website machen?

Welche Daten müssen Sie offen legen?

Auch bei Webseiten muss nachvollziehbar sein, wer für die dargestellten Inhalte verantwortlich ist. Dies dient einerseits der Transparenz und an-

dererseits ermöglicht es Betroffenen durch Berichterstattung herauszufinden, wer hinter einer möglicherweise negativen Berichterstattung steht. Aus diesem Grund sehen Gesetze Informationsverpflichtungen vor, welche sich nach der Art der Webseite richten.

Vielfach wird umgangssprachlich für jegliche Informationen über die Inhaberin oder den Inhaber einer Webseite der Begriff „Impressum" verwendet. Dies ist nicht korrekt und kann zu Missverständnissen und im schlimmsten Fall zu rechtlichen Problemen führen. Aus diesem Grund sollte sich jede Inhaberin und jeder Inhaber einer Webseite beim Erstellen seines Web-Auftritts zumindest einmal kurz mit diesem Thema befassen.

Es kann grob zwischen der Offenlegungspflicht für Webseiten, der Impressumspflicht für (vor allem) Newsletter und der (sehr detaillierten) Informationsverpflichtung für kommerzielle Webseiten unterschieden werden.

Die Offenlegungspflicht:

Von der Offenlegungspflicht nach dem Mediengesetz sind primär Newsletter, Websites und Blogs erfasst. Es wird hierbei vom Gesetz zwischen „großen" und „kleinen" Websites unterschieden:

1. „Kleine Webseiten": Für rein private Websites oder einfache Firmenhomepages, ohne meinungsbildenden Charakter gilt (§ 25 Abs. 5 MedienG): Auf einer Website, die keinen Informationsgehalt aufweist, der über die Darstellung des persönlichen Lebensbereichs oder die Präsentation der Medieninhaberin oder des Medieninhabers hinausgeht und der geeignet ist, die öffentliche Meinungsbildung zu beeinflussen, sind folgende Angaben offen zu legen:

- Name oder Name der Firma,
- gegebenenfalls der Unternehmensgegenstand,
- Wohnort, Sitz oder Niederlassung (nicht die komplette Adresse!),

2. „Große Webseiten" Auf allen anderen Websites, Blogs und in Newslettern, sind folgende Angaben zu machen (§ 25 Abs. 2 MedienG):

- Name oder Name der Firma,
- Unternehmensgegenstand,

- Wohnort, Sitz oder Niederlassung (nicht die komplette Adresse!),
- bestimmte Beteiligungsverhältnisse,
- Geschäftsführung,
- die Mitglieder des Vorstandes und Aufsichtsrates und die Gesellschafterinnen oder Gesellschafter, deren Einlage oder Stammeinlage 25 % übersteigt,
- grundlegende Richtung des Mediums.

Es muss bei der Offenlegungspflicht für Webseiten also nicht die vollständige Adresse angegeben werden. Die Angabe des Wohnortes reicht (anders als bei der Impressumspflicht oder der Informationsverpflichtung für kommerzielle Webseiten) aus. Die Angabe von Straße und Hausnummer ist somit nicht erforderlich.

Die Offenlegungspflicht trifft die Medieninhaberin oder den Medieninhaber, also die- oder denjenigen, die oder der die inhaltliche Gestaltung besorgt und die Abrufbarkeit der Website oder die Verbreitung des Newsletters entweder besorgt oder veranlasst.

In Newslettern ist, zusätzlich zu der unten dargelegten Impressumspflicht, entweder anzugeben, unter welcher Web-Adresse die vom Gesetz vorgeschriebenen Angaben ständig, leicht und unmittelbar auffindbar sind, oder es sind diese Angaben jeweils dem Medium anzufügen. Auch auf einer Website müssen diese Angaben ständig leicht und unmittelbar auffindbar zur Verfügung stehen.

Sofern Unklarheiten bestehen, ob es sich bei einer Webseite um eine „kleine“ oder um eine „große“ Webseite handelt, ist es besser die (strengeren) Bestimmungen für sog. „große Webseiten“ einzuhalten.

Die Impressumspflicht

Die Impressumspflicht wird nicht auf Websites angewendet. Sie gilt nämlich nur für **so genannte wiederkehrende elektronische Medien (§ 24 MedienG).** Dies ist nach dem Mediengesetz ein Medium, das auf elektronischem Wege wenigstens viermal im Kalenderjahr in vergleichbarer Gestaltung verbreitet wird, wie etwa ein Newsletter.
Solche wiederkehrenden elektronischen Medien müssen enthalten:

- Name oder Firma,
- komplette Anschrift der Medieninhaberin oder des Medieninhabers und der Herausgeberin oder des Herausgebers.

Die Pflicht zur Veröffentlichung trifft jene Person, die für die inhaltliche Gestaltung des Newsletters verantwortlich ist und die Verbreitung entweder besorgt oder veranlasst. Für Newsletter gelten die Bestimmungen der Impressumspflicht ebenso wie die Offenlegungspflicht für „große Webseiten". Bieten Sie als Medieninhaberin oder Medieninhaber Dienste im Sinne des E-Commerce-Gesetzes (ECG) an, können die Angaben nach § 5 ECG gemeinsam mit den Angaben zum Impressum bzw. zur Offenlegung zur Verfügung gestellt werden.

§ 5 ECG – Informationen

Dient die Website kommerziellen Zwecken, so haben Sie als Diensteanbieterin oder Diensteanbieter folgende Angaben zu machen, welche aber gemeinsam mit den Angaben zum Impressum bzw. zur Offenlegung zur Verfügung gestellt werden können:

- Name oder Name der Firma,
- die geografische Anschrift der Niederlassung (kein Postfach!),
- Angaben, die gewährleisten, dass die Nutzerinnen und Nutzer rasch und unmittelbar mit Ihnen in Verbindung treten können, einschließlich Ihrer E-Mail-Adresse,
- sofern vorhanden: Firmenbuchnummer und Firmenbuchgericht,
- soweit die Tätigkeit einer behördlichen Aufsicht unterliegt, die für Sie zuständige Aufsichtsbehörde,
- diverse gewerbe- oder berufsrechtliche Informationen (z. B. Kammerangehörigkeit, Berufsbezeichnung usw.),
- sofern vorhanden: die Umsatzsteuer-Identifikationsnummer.

Das Fehlen dieser Informationen kann im Übrigen ganz schön teuer werden. Fühlen sich die Konkurrenz, Konsumentenschutzorganisationen oder eine betroffene Person gestört, können diese mit einer Unterlassungsklage drohen.

E-Mail: Spam, Phishing, Viren

Der Intelligence Quarterly Report der Anti-Viren-Firma Symantec registrierte im dritten Quartal 2010 14,6 Millionen Spam-Nachrichten. Ihr Anteil an der Gesamtzahl aller versendeten E-Mail Nachrichten betrug 91%. 73% und damit die größte Zahl der bei Phishing Angriffen in diesem Quartal verwendeten Marken, gehörten zu Unternehmen im Finanzdienstleistungssektor.

Quelle: www.symantec.com

Verschicken von Mails
Was können Sie gegen Spam tun?
Wie kommen Spammer zu den Adressen?
Gibt es auch legale E-Mail-Werbung?
Phishing: Woran erkennen Sie Phishing Mails?
Vorsicht vor zweifelhaften Jobs!
Viren, Trojaner und Konsorten
Wie können Sie sich vor Viren schützen?
Wie werden Sie einen Computervirus wieder los?
Hoaxes
419 Scams
Wie sorgen Sie dafür, dass Ihre Passwörter sicher sind?

Das Versenden von E-Mails war eine der ersten Anwendungen im Internet, und sie ist bis heute auch eine der Wichtigsten. Hier eine kurze Übersicht, worauf Sie achten sollten:

Verschicken von Mails

In den Anfangstagen des Netzes wurden Neulinge oft darauf hingewiesen, doch vor dem Versenden von E-Mails oder dem Mitdiskutieren in Newsgroups erst die so genannte ☛ *„Netiquette"* zu lesen. In dieser Sammlung von Benimmregeln stand unter anderem noch zu lesen, dass Sie bei Postings auf Umlaute verzichten sollen, da diese nicht von allen PCs darstellbar sind.

☛ Netiquette:
Ein Kompendium an Höflichkeitsregeln, welches das gute Benehmen im Rahmen der technischen (elektronischen) Kommunikation regelt.

So streng sind die Regeln heute zum Glück nicht mehr. Trotzdem können Sie sich und anderen das Leben erleichtern:

Es ist z.B. ganz schlechter Stil, ein leeres Mail zu versenden und den eigentlichen Text in eine angehängte Word-Datei zu packen, obwohl das viele Menschen gerade im beruflichen Verkehr gerne tun. Weiters sollten Sie darauf achten, dass der Dateianhang einem universellen Format entspricht und somit für alle lesbar ist.

Das Dateiformat „.pdf" hat sich zu diesem Zweck als allgemeines Austauschformat für formatierten Text und Bilder etabliert. Diese Dateien können auf praktisch allen Computern angezeigt werden und lassen sich hervorragend ausdrucken. Das Erstellen von .pdf-Dateien ist heute nicht mehr schwierig, meist genügt der Aufruf der entsprechenden Funktion in dem Programm mit dem man den Inhalt erstellt hat.

☛ *HTML*-Mails (Nachrichten mit Bildern, Farben, verschiedenen Schriftstilen etc.) können heutzutage zwar von den meisten E-Mail-Programmen dargestellt werden, sind aber größer als reine Text-E-Mails. Außerdem ist die Darstellung in den verschiedenen Programmen durchaus unterschiedlich. Als Faustregel gilt: Nur dann HTML-Mails versenden, wenn es notwendig und passend ist (z. B. bei einer schön gestalteten Einladung), ansonsten ist normaler Text ausreichend. Niemand benötigt zum Verständnis der Nachricht „Ich komme heute etwas später" einen Blümchenhintergrund aus dem Outlook-Repertoire. Solche Mails wirken oft eher peinlich.

☛ Hyper Text Markup Language (HTML):
Ist jene Sprache, die zur Erstellung von Websites verwendet wird.

Noch ein Tipp zum Thema HTML-Mails: Viele Leute lesen heutzutage ihre E-Mails unterwegs auf dem Handy, und diese können HTML normalerweise schlecht bis gar nicht darstellen. Es ist daher zu empfehlen, HTML-Mails zusätzlich auch als reinen Text zu verschicken. Viele E-Mail-Programme verfügen über die entsprechende Einstellung.

Die Einstellungen **„Wichtig"** und **„Dringend"** sollten Sie nur verwenden, wenn der Inhalt auch entsprechend ist. Leute, die diese Optionen routinemäßig anklicken, sagen damit mehr über sich selbst aus, als über ihre E-Mails.

Möchten Sie Mails an viele verschiedene Empfängerinnen und Empfänger senden, sollten diese als **BCC** (Blind Carbon Copy) verschickt werden. Diese Einstellung bewirkt, dass die Personen 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.

Um anzuzeigen, dass es auch noch andere BCC-Empfängerinnen und -Empfänger gibt, hat es sich eingebürgert, im „To:"- Feld (in das ohnehin mindestens eine Empfängerin oder ein Empfänger eingetragen werden muss) die eigene Adresse anzugeben. Das Mail wird also unter anderem an Sie selbst adressiert.

Was den „Ton" der Mails betrifft, so gilt im Prinzip dasselbe wie für den guten alten Brief:

Das **geschäftliche E-Mail** sollte eher förmlich sein (korrekte Gross- und Kleinschreibung beachten und keinesfalls irgendwelche Smileys :-) beinhalten), in der privaten Post ist dagegen erlaubt, was gefällt.

In beiden Fällen sollten Sie auf korrekte Rechtschreibung achten; glücklicherweise verfügen die meisten E-Mail-Programme heutzutage bereits über Rechtschreib-Korrektur-Funktionen.

Weiters hat es sich in geschäftlichen E-Mails eingebürgert, eine Art **Visitenkarte (Signature** – nicht zu verwechseln mit der digitalen Signatur) **mitzuschicken.** Die meisten E-Mail-Programme bieten Ihnen die Möglichkeit, diese Signature quasi als Absender anzulegen. Darin können Sie

alle Ihre Kontaktinformationen (Firma, Abteilung, Adresse, Telefon, Fax etc.) automatisch mit jeder Mail mitschicken. Eine Signature erleichtert Ihrem Gegenüber die Kontaktaufnahme und wirkt professionell.

Noch ein wichtiger Tipp zum Schluss:
Achten Sie darauf, dass Ihr **E-Mail-Programm** mit Ihren E-Mails **korrekte Absenderinformationen** mitschickt. Diese sollten zumindest Vorname und Nachname (in dieser Reihenfolge) sowie die korrekte E-Mail-Adresse beinhalten. Es zahlt sich aus, diese Informationen in den Voreinstellungen des E-Mail Programms zu überprüfen!

Was können Sie gegen Spam tun?

☛ *Spam* ist für viele mittlerweile die größte Plage im Internet. Fast jede E-Mail-Adresse, die länger als ein paar Monate in Verwendung ist, erhält täglich Dutzende unerwünschte Massenzusendungen, in denen von Potenzmitteln bis zu Gartenleuchten so ziemlich alles beworben wird.

☛ Spam:
Ein Sammelbegriff für jede Art von unerwünschten E-Mails, insbesondere für Massenaussendungen zur Bewerbung scheinbar günstiger Angebote.

Was können Sie dagegen tun?

Die alte medizinische Grundregel, dass Vorbeugen besser als Heilen sei, hat sich auch in der Spam-Bekämpfung bewährt, allerdings mit Einschränkungen. Denn die Methoden, mit denen Spammer die E-Mail-Adressen ihrer Opfer aufspüren, verbessern sich ständig (s. S. 69).

Trotzdem ist es eine gute Idee, **mindestens zwei E-Mail-Adressen** zu verwenden: eine für berufliche oder „seriöse" Zwecke und eine, mit der Sie sich in ☛ *Communitys* registrieren, an Gewinnspielen teilnehmen, in Gästebücher schreiben etc. Die Idee dahinter ist einfach: Eine Adresse, die nirgends öffentlich aufscheint, ist für Spammer viel schwerer zu bekommen als eine, die inflationär im Web zu finden ist. Die zweite Adresse kann bei Bedarf leicht gewechselt werden, bei einer beruflich genutzten E-Mail-Adresse ist das kaum möglich.

☛ Community:
Gemeinschaft, die sich aufgrund gemeinsamer Interessen zusammengefunden hat und Austausch über Diskussionsforen, Chats oder auch Linksammlungen pflegt.

Die Zweitadresse sollten Sie übrigens bei einem der großen Webmail-Anbieter wie zum Beispiel → GMX, Yahoo oder Google Mail registrieren, denn diese verfügen auch über gute Spamfilter.

→ www.gmx.at
→ mail.yahoo.de
→ mail.google.com
→ home.live.com

Noch ein Wort zur Vorbeugung: Wenn Sie bereits Spam bekommen, sollten Sie die Mails nach Möglichkeit nicht öffnen und **auf keinen Fall auf so genannte Remove-Links klicken.** Beides kann vom Spammer dazu verwendet werden, Ihre E-Mail-Adresse zu verifizieren. Sie steigt dadurch im Wert, weil dann bewiesen ist, dass die Mails an diese Adresse tatsächlich gelesen werden.

Beim Öffnen des Mails kann beispielweise automatisch eine Grafik vom Server des Spammers angefordert werden. In dieser Anforderung ist ein Code enthalten, der dem Spammer mitteilt, wer das Mail gelesen hat.

Damit wäre auch schon die zweite Möglichkeit der Spam-Bekämpfung genannt, nämlich der **Spamfilter** beim ☛ *Provider*. Die meisten Provider bieten einen solchen mittlerweile kostenlos an. Gute Spamfilter tun nichts hinter dem Rücken der Kundinnen und Kunden, sondern kennzeichnen den Spam (z. B. im Betreff) und/oder sortieren ihn in einen eigenen Ordner (Spam oder Junk) ein.

☛ Provider: Unternehmen, über das Sie Zugang zum Internet bekommen. Eine Liste der österreichischen Provider finden Sie unter www.ispa.at.

Letzteres funktioniert dann am besten, wenn der Provider die E-Mail-Funktion über so genannte ☛ *IMAP*-Accounts anbietet, denn IMAP ist (im Unterschied zum verbreiteten ☛ *POP*) in der Lage, mehrere Ordner zu verwalten.

☛ IMAP: „Internet Message Access Protocol" ist ein Mailprotokoll, bei dem die Nachrichten auf einem zentralen Server verbleiben und nur bei Bedarf auf den lokalen Rechner übertragen werden. IMAP ist komfortabler als POP, da es mehrere Ordner unabhängig voneinander verwalten kann.

Die dritte Abwehrmöglichkeit ist ein **Spamfilter auf Ihrem Computer.** Alle modernen E-Mail-Programme bieten sehr gute selbstlernende Spamfilter an. Mit diesem Filter sind Sie in der Lage, auch jenen Spam zu filtern, der beim Provider durchgerutscht ist (der Spamfilter des Providers – mit dem tausende Personen bedient werden – muss notgedrungen grobmaschiger sein als einer, der vom Verhalten einer einzelnen Person lernt).

Wichtig ist, dass Sie **nach Installation eines neuen E-Mail-Programms** ein paar Wochen lang den **Spamfilter des Programms „anlernen",** damit sich der Filter Ihren Bedürfnissen anpassen kann. Andernfalls wird er nicht zu Ihrer Zufriedenheit funktionieren. Wie Sie das genau machen, entnehmen Sie bitte der Anleitung Ihres E-Mail-Programms.

☛ POP: „Post Office Protocol", das übliche Verfahren zur Zustellung von E-Mails. E-Mails werden auf einem Server so lange gespeichert, bis das Mail-Programm sie herunterlädt.

Wie kommen Spammer zu den Adressen?

Ursprünglich wurde von Spam-Versendern lediglich das ☛ *Usenet* (die alten Diskussionsforen des Internets) nach E-Mail-Adressen durchgekämmt.

Dann entstanden so genannte Spiders, die – ähnlich wie Suchmaschinen – das ganze WWW absuchen und alles, was nach einer E-Mail-Adresse aussieht, in ihren Datenbanken abspeichern. Gegen diese beiden Arten des „E-Mail-Harvestings“ (der „Ernte“ von E-Mail-Adressen) konnten sich Nutzerinnen und Nutzer früher wehren, indem Sie ihre Adresse nirgends öffentlich hinterließen.

Mit dem Aufkommen von E-Mail-Viren entstand aber die Möglichkeit, einen von einem ☛ *Virus* befallenen Computer nach E-Mail-Adressen zu durchsuchen. Das Virus hat unter anderem die Aufgabe, „nach Hause zu telefonieren“, also mit seinem ursprünglichen Versandort Kontakt aufzunehmen.

Auf diese Weise werden auf dem Rechner gefundene E-Mail-Adressen an den Spammer zurückgeschickt. Dagegen können Sie überhaupt nichts tun, denn wie sollen Sie verhindern, dass einer Ihrer E-Mail-Kontakte einen Virus bekommt? Trotzdem ist es sinnvoll, darauf aufzupassen, denn schließlich macht es einen Unterschied, ob Sie pro Tag 10, 100 oder mehr Spam-Mails bekommen.

☛ Usenet:
Jenes Netz, in dem die klassischen Diskussionsforen des Internets (Newsgroups) zu Hause sind. Diese entstanden bereits in den achtziger Jahren des vorigen Jahrhunderts. Newsgroups können entweder mit E-Mail-Programmen oder mit so genannten Newsreadern gelesen werden.

☛ Virus:
Ein Programm, das sich selbstständig verbreiten kann und meist auch irgendeine Art von Schaden anrichtet.

Gibt es auch legale E-Mail-Werbung?

Die Zusendung von Werbemails ist ohne Ihre vorherige Einwilligung grundsätzlich nicht erlaubt. Erlaubt wäre eine Zusendung von Werbemails aber im folgenden Fall:

Sie haben Ihre Mailadresse bei einer Bestellung dem Online-Shop bekannt gegeben und hatten bei der Bestellung Gelegenheit, die Zusendung von Werbemails abzulehnen (z. B. Ankreuzen eines Kästchens mit dem Text „Ich wünsche keine weiteren Informationen per E-Mail“). Falls Sie die Zusendung von Werbemails nicht aktiv ablehnen und Ihnen das Unternehmen weitere Werbemails sendet, darf das Unternehmen darin nur eigene Produkte bewerben und muss Ihnen Gelegenheit geben, weitere Werbemails abzulehnen.

Dieselben Regelungen gelten natürlich auch, wenn Sie selbst Werbung per E-Mail versenden wollen. Sie sollten darauf achten, niemanden mit häufigen E-Mail-Aussendungen zu belästigen.

Die Menschen erhalten heutzutage bereits viel zu viel Spam, und im Zweifelsfalle ist es jemandem egal, ob sie oder er einmal vor Jahren einer Aussendung zugestimmt hat. Spam ist das, was die Kundin oder der Kunde als solchen empfindet ...

Phishing

☛ *Phishing* ist eine Betrugsvariante. In den meisten Fällen geht es den Kriminellen darum, an die **Bankkonto-Zugangsdaten von ahnungslosen Internetbenutzerinnen und -benutzern zu gelangen.** Aber auch eBay und andere große Online-Shops sind von Phishing betroffen.

Sie erhalten ein Mail, das vorgeblich von der eigenen Bank stammt und mehr oder minder gut gefälscht ist. Durch Klicken auf die ☛ *URL* in diesem Mail, landen Sie auf einer gefälschten Website der Bank, auf der Sie unter irgendeinem Vorwand aufgefordert werden, sich mit User-ID und Passwort einzuloggen und einen oder mehrere ☛ *TANs* einzugeben. Sobald Sie das getan haben, müssen Sie damit rechnen, dass Ihr Konto ziemlich schnell leer geräumt wird. In anderen Varianten wird versucht, einen ☛ *Trojaner* auf Ihrem Computer zu platzieren, der mit der Versenderin oder dem Versender Kontakt aufnimmt, sobald Sie wertvolle Daten (z. B. TANs) auf der Tastatur eingegeben haben. Deshalb sollten Sie nie die in den Mails angegebenen Web-Adressen anklicken, auch nicht aus reiner Neugier.

Woran erkennen Sie Phishing Mails?

Oft sind Mails dieser Art leicht zu erkennen, z. B. auf Grund von Tippfehlern, schlechtem Deutsch, seltsamen Absenderadressen oder ungewöhnlichem Inhalt. In letzter Zeit wurden die Phishing Attacken immer professioneller, deshalb sind viele gefälschte Mails heute nicht mehr ganz so leicht zu identifizieren. **Wenn Sie auch nur den leisesten Zweifel haben, ob das Mail tatsächlich von Ihrer Bank ist, dann ist es das in**

☛ Phishing: Kunstwort aus „password“ und „fishing“. Kriminelle Methode, um Logins und Passwörter herauszufinden und z. B. Bankkonten zu plündern.

☛ URL: „Uniform Resource Locator“ ist der allgemeine Ausdruck für eine Adresse im Netz, die z. B.

☛ TAN: „TransaktionsAutorisierungs-Nummer“ ist eine hauptsächlich von Banken verwendete Möglichkeit, Online-Zahlungen zu verifizieren. TANs sind Zahlenfolgen und werden als Listen oder per SMS (mobile TAN oder TAC-SMS) verschickt und können jeweils nur einmal verwendet werden. TANs sind bei Phishing-Attacken das eigentliche Ziel der Betrüger, da sie zwingend für Überweisungen benötigt werden.

☛ Trojaner: Ein Programm, das vorgibt, etwas anderes zu sein, als es tatsächlich ist. Die Grenze zwischen Trojanern und Viren ist heute nur noch schwer zu ziehen, da die meisten derartigen Schädlinge beide Funktionen beinhalten.

den allermeisten Fällen nicht. Bevor Sie in diesem Mail irgendetwas anklicken, besuchen Sie lieber die Website Ihrer Bank. Gebem Sie die Adresse händisch in Ihren Browser ein und sehen Sie dort nach, ob Ihnen nicht vielleicht eine entsprechende Warnung ins Auge springt. Sofern Ihre Bank wirklich Daten von Ihnen benötigt, werden Sie wohl gleich nach dem Einloggen um diese Daten gebeten werden. Ihre Bank wird Sie nie bitten, Daten via E-Mail einzugeben oder sie zu bestätigen. Ebenso wird Sie Ihre Bank, sofern diese eine neuen Web-Adresse hat, nicht via E-Mail darüber informieren.

Am einfachsten und sichersten ist es, wenn Sie die Website Ihrer Bank immer nur händisch in den Browser eingeben oder von einem Bookmark (Favoriten, Lesezeichen) abrufen, die Sie selbst angelegt haben. Dann kann Ihnen nichts passieren. **Ihre Bank wird Sie übrigens nie auffordern, einen TAN für irgendeine Umstellung oder sonstige Eingaben zu verbrauchen. Dieser ist wirklich nur für Überweisungen gedacht.**

TIPPS:

Wie Sie sich gegen Phishing Betrug schützen können

Da Fälschungen oft schwer als solche zu erkennen sind, sollten Sie besonders sensibel mit Ihren Account-Daten umgehen.

- Fragen Sie sich zuerst, ob die Bekanntgabe der gewünschten Daten einen Sinn ergibt. Es gehört NICHT zum üblichen Verfahren von Banken oder Online-Shops, von Auktionshäusern o. Ä., sensible Daten via E-Mail abzufragen!
- Oft hilft ein Anruf bei der Hotline des jeweiligen Unternehmens, um herauszufinden, ob das Mail echt ist oder nicht.
- Bei der Passwortwahl sollten leicht zu erratende Kennwörter wie regelmäßige oder bekannte Zahlen (z. B. 12345, 4711, 0815) ebenso wie Geburtstage, Telefonnummern etc. vermieden werden. Am besten ist eine Kombination von Buchstaben und Zahlen (siehe dazu „Wie sorgen Sie dafür, dass Ihre Passwörter sicher sind?“ S. 76).
- Ihre Passwörter sollten Sie – wenn möglich – regelmäßig ändern.
- Achten Sie bei der Eingabe Ihrer Daten immer darauf, dass

diese über eine SSL-verschlüsselte Internetverbindung eingegeben werden. Die SSL-Verschlüsselung erkennen Sie daran, dass die Website mit https://www beginnt und im Browser das Schlosssymbol geschlossen aufscheint ( ). Wenn die angebliche Verbindung zum Server der Bank (zumindest auf der Seite mit der Passworteingabe) nicht verschlüsselt ist, dann ist sicher etwas faul. Allerdings können auch gefälschte Seiten über verschlüsselte Verbindungen verfügen. Vorsicht ist daher immer geboten!

- Sollten Sie dennoch einmal eine zweifelhafte Internetseite besucht und Ihre Daten preisgegeben haben, ändern Sie sofort Ihr Passwort und veranlassen Sie die Sperre der TANs bei Ihrem Online-Bankkonto.
- Für das Online-Banking werden von den Banken neben dem üblichen PIN/TAN-Verfahren zusätzliche Sicherheitsmaßnahmen wie die TAN-Übermittlung mittels SMS (auch mobile TAN oder TAC-SMS genannt) oder die Nutzung der digitalen Signaturkarte angeboten. Erkundigen Sie sich bei Ihrem Institut über diese Möglichkeiten.
- Sehen Sie doch gelegentlich auf den → Websites von Mozilla, Microsoft oder Apple nach, was die Herstellerfirmen der Browser Firefox, Internet Explorer und Safari in Sachen Phishing-Bekämpfung an neuen Features zu bieten haben.

→ www.mozilla.com
→ www.microsoft.at
→ www.apple.at

Vorsicht vor zweifelhaften Jobs!

Phishing-Betrügerinnen oder Betrüger wollen nicht nur an das Geld der Opfer gelangen, sondern müssen es anschließend auch noch außer Landes schaffen. Dazu bedienen sich die Kriminellen mehr oder minder ahnungsloser Mittelspersonen, die über Spam-Aussendungen angeworben werden.

Der Job als „Geldkurier", „Finanzmanager" o. Ä. besteht meist darin, das eigene Bankkonto für Transaktionen zur Verfügung zu stellen bzw. eingehendes Geld (abzüglich einer üppigen Provision) auf ein anderes Konto im Ausland zu überweisen, um dadurch die Fahndung nach den Betrügerinnen oder Betrügern zu erschweren. Der erhoffte Geldsegen ist aber – wenn überhaupt – nicht von langer Dauer, da Sie in diesem Fall selbst

das schwächste Glied in der Kette sind und mit Anzeigen und Rückforderungen zu rechnen haben. Derlei Tätigkeiten sind nämlich ganz und gar illegal und die Strafandrohungen für Betrug, Geldwäsche etc. sind nicht gerade gering. Kurz und gut: Finger weg von derartigen Angeboten. Wenn es zu schön klingt, um wahr zu sein, dann ist praktisch immer etwas faul.

Viren, Trojaner und Konsorten

Etwa zur Jahrtausendwende brachen die ersten großen Virenepidemien über das Internet herein. MyDoom, Sobig und Slammer waren in aller Munde. In den letzten Jahren hat nur der Virus Conficker es geschafft, durch das Blockieren der IT-Infrastruktur der Kärntner Krankenanstalten traurige Berühmtheit zu erlangen.

Mittlerweile ist es um Computerviren etwas ruhiger geworden, aber die großen und medienwirksamen Epidemien wurden lediglich durch chronische Gefahren ersetzt. Die Virenprogramme sind heute auch nicht mehr das Produkt irgendwelcher aufgeweckter Computerkids, sondern von Profis der organisierten Kriminalität.

Die neueste Generation von Viren (korrekt ausgedrückt, ☛ *Trojanern*) schadet nämlich nicht mehr (ausschließlich) der- oder demjenigen, die oder der das ☛ *Virus* hat. Frühere Virengenerationen löschten einfach die Festplatte oder gewisse Arten von Files auf dem verseuchten Rechner. **Hinter vielen aktuellen Viren stehen heute handfeste ökonomische Interessen:** Einerseits das **Sammeln von E-Mail-Adressen** (die auf den verseuchten Computern zu finden sind), andererseits werden diese Computer in ☛ *Botnetzen* als **so genannte** ☛ *Zombies* missbraucht. Über diese verseuchten Computer werden später zigtausende Spam-E-Mails versendet.

Viele andere Missbrauchsmöglichkeiten sind ebenfalls denkbar, da die verseuchten Computer (Zombies) von außen ferngesteuert werden können (was den Benutzerinnen und Benutzern oft nicht einmal auffällt).

Eine lästige Variante von Computerviren hat sich in den letzten Jahren auch in das Soziale Netzwerk Facebook eingeschlichen: immer wieder wird man dort mit manipulierten Bildern oder Videos auf eine externe

☛ Trojaner:
Ein Programm, das vorgibt, etwas anderes zu sein, als es tatsächlich ist. Die Grenze zwischen Trojanern und Viren ist heute nur noch schwer zu ziehen, da die meisten derartigen Schädlinge beide Funktionen beinhalten.

☛ Virus:
Ein Programm, das sich selbstständig verbreiten kann und meist auch irgendeine Art von Schaden anrichtet.

☛ Botnetz:
Ein Netzwerk aus lauter ☛ Zombies, das ohne Wissen der Inhaberinnen und Inhaber z. B. für Versand von Spam-Mails (Phishing Mails) missbraucht wird

☛ Zombie:
Ein Computer, der ohne Kenntniss der Besitzerin oder des Besitzers von aussen ferngesteuert wird.

Seite gelockt. Ist man erst einmal auf dieser Seite und versucht sich mit einem Klick das Bild oder Video anzuschauen, hat sich der Link schon verselbstständigt und eine Statusmeldung oder ein Mail an alle Freunde auf Facebook verschickt oder gesendet. Dadurch, dass man gleichzeitig bei Facebook eingeloggt ist, hat dieser Virus die Möglichkeit sich weiter zu verbreiten. Alle Freunde sehen, dass man den Link über seinen eigenen Status oder per Mail weiter schickt, klicken ihn an und der Kreislauf beginnt erneut.

Hier hilft nur, aufmerksam zu sein; wenn man in die Virus-Falle tappt sollte Facebook informiert werden („als Spam melden") und die Meldung von der Pinnwand gelöscht werden um zu verhindern, dass sich der Virus weiter verbreitet. Auch ein Mail oder eine Statusmeldung mit dem Hinweis, dass man selbst in die Virus-Falle getappt ist, informiert Betroffene und hält sie unter Umständen davon ab, den Virus weiter zu verbreiten.

Wie können Sie sich vor Viren schützen?

Die einfachste – aber leider nicht immer ausreichende – Regel zum Schutz vor Viren ist, **keine unbekannten Dateianhänge (Attachments) aus E-Mails herunterzuladen oder gar zu öffnen bzw. auszuführen.** Insbesondere Dateien mit den Endungen .vbs, .bat, .com, .cmd, .exe, .pif, .scr und auch .zip sind verdächtig. Solche Attachments können durchaus von bekannten Absenderadressen stammen, da sich viele Viren über die Adressbücher der befallenen Rechner selbstständig weiterversenden. Drehen Sie im Browser und im E-Mail-Programm sowie im ZIP-Programm auch unbedingt die Voreinstellung ab, dass heruntergeladene Dateien sofort ausgeführt werden sollen. Sollten Sie doch versehentlich einen Virus auf Ihrer Festplatte haben, so kann dieser erst aktiv werden, wenn er einmal aufgerufen wurde.

Viele Viren nutzen auch Eigenheiten und Sicherheitslücken von diversen E-Mail-Programmen aus. Egal ob Sie Microsoft Outlook, Eudora oder Thunderbird verwenden, wiegen Sie sich nicht in Sicherheit: Versuchen Sie mit Ihrem E-Mail Programm sorgfältig umzugehen und öffnen Sie keine E-Mails, deren Absender sie nicht kennen.

Generell ist es eine gute Idee, immer sofort die neuesten **Updates des**

verwendeten Mailprogramms, Browsers, Betriebssystems sowie der Antivirensoftware einzuspielen.

Achtung! E-Mail ist heutzutage nicht mehr die einzige Möglichkeit, sich einen Virus oder Trojaner einzufangen. Unter Umständen kann das auch über das bloße Ansehen von manipulierten Websites passieren (vor allem dann, wenn der verwendete Webbrowser nicht auf dem neuesten Stand ist), ebenso über ☛ *Messenger*-Dienste oder den Download kostenloser Programme von dubiosen Quellen (z. B. ☛ *File-Sharing*-Plattformen).

→ Instant Messaging Programme
Instant Messaging bezeichnet den sofortigen und unmittelbaren Versand einer Textnachricht. Meist erscheint die Nachricht in Echtzeit am Bildschirm der Empfängerin oder des Empfängers.

☛ File-Sharing:
Der Austausch von Dateien erfolgt auf File-Sharing-Plattformen. Die erste derartige Plattform war Napster. File-Sharing funktioniert normalerweise in Peer-to-Peer-Netzwerken.

Es wird daher immer wichtiger, auf den eigenen Hausverstand zu vertrauen und nicht auf eine aktuelle Antivirensoftware und Firewall zu verzichten. Die Firewall ist deshalb wichtig, weil viele Trojaner versuchen, sich direkt über das Netz auf dem Rechner zu installieren. Sie gut zu konfigurieren und zu warten ist daher unerlässlich.

Wie werden Sie einen Computervirus wieder los?

Zunächst müssen Sie feststellen, ob Sie wirklich ein Virus haben. Dabei hilft Ihnen ein Antivirusprogramm (z. B. → Norton AntiVirus oder McAfee) mit aktuellen Virusinformationen (Virus-Definitions).

→ www.symantec.de
→ de.mcafee.com

Sollten Sie kein oder ein bereits veraltetes Programm besitzen, so ist es in jedem Fall eine gute Idee, ein aktuelles zu kaufen. Zusätzliche Informationen und Hilfestellungen erhalten Sie auf den Websites verschiedener Spezialisten. In Österreich beispielsweise bei der Firma Ikarus. Kostenlose Alternativen dazu, d. h. → Gratis-Download von Antivirenprogrammen etc. bieten diverse Websites.

→ www.freeware.de

Hoaxes

Eine Hoax ist üblicherweise ein Mail, in dem Sie aufgefordert werden, es an viele andere Adressaten weiterzuschicken. Dafür werden oft – wie in den guten alten **Kettenbriefen** – haarsträubende Begründungen genannt, manche – wie z. B. Warnungen vor angeblich neuen Viren – scheinen auf

den ersten Blick plausibel. Was immer es aber ist, das Sie weiterschicken sollen: Tun Sie es nicht, Sie tragen damit nur zum ohnehin schon viel zu hohen Spam-Aufkommen bei.

→ www.tu-berlin.de/www/software/hoax.shtml

Und wenn Sie noch immer glauben, dass die Viruswarnung, die Sie gerade erhalten haben, echt ist, dann sehen Sie im → Hoax Info Service der TU Berlin nach oder geben Sie einen kurzen Textabschnitt des E-Mails in Google ein.

419 Scams

Eine Sammelbezeichnung für zum Teil besonders trickreichen Betrug sind die so genannten **419 Scams,** deren Bezeichnung sich aus dem entsprechenden **Paragrafen des nigerianischen Strafgesetzes ableitet.**

Üblicherweise erhalten Sie ein fantasievolles E-Mail, in dem Ihnen jemand ein Geschäft vorschlägt, das zu verlockend ist, um wahr zu sein (oft informiert es über einen angeblichen Lotteriegewinn). Wenn Sie darauf reagieren, erhalten Sie Instruktionen, wie Sie an das Geld gelangen. Diese Konversation geht oft über dutzende Mails. Irgendwann werden Sie dann aber aufgefordert, Geld zu überweisen (für entstandene Spesen, Steuern, Flugtickets, was auch immer). Sobald Sie dieses Geld dann überweisen, hören Sie von der anderen Seite nie wieder etwas (und das Geld ist natürlich weg).

→ www.nigeria-connection.de

Wenn Ihnen also jemand, von dem Sie noch nie gehört haben, ein unglaubliches Geschäft vorschlägt, dann ignorieren Sie dieses Mail am besten. Mehr Infos dazu finden Sie z. B. auf der Seite → Nigeria-Connection.

Wie sorgen Sie dafür, dass Ihre Passwörter sicher sind?

Passwörter sind der Schlüssel für den eigenen Computer und alle dort abgespeicherten Daten. Hat jemand Zugriff auf einen Computer, bekommt er oder sie einen guten Einblick in das Privatleben, die Bankverbindungen, Familienfotos und Musik-Sammlungen der Computerbesitzerin oder des Computerbesitzers. Umso wichtiger ist es, die eigenen **Passwörter verantwortungsvoll zu wählen** und zu versuchen, es potentiellen Pass-

wort-Crackern möglichst schwer zu machen. Dabei sollten einige Dinge beachtet werden:

1.) Ein **Passwort sollte immer aus 6 bis 8 Zeichen bestehen**, die sich idealerweise aus **Buchstaben, Sonderzeichen und Zahlen** zusammen setzen. Auch eine Kombination zwischen Groß- und Kleinschreibung ist empfehlenswert. Umso mehr Sie Sonderzeichen, Zahlen und Buchstaben kombinieren, umso sicherer wird das Passwort.

2.) **Verwenden Sie Sätze oder Wörter, die von anderen Personen nicht leicht zu erraten sind.** Ungeeignet sind Dinge wie das eigene Geburtsdatum, der eigene Name (oder der nahestehender Personen wie Kinder, Ehepartner oder Haustiere), Hobby, Lieblingsgericht, etc.

3.) Verwenden Sie für verschiedene Anwendungen oder Seiten immer unterschiedliche Passwörter. Vor allem für kritische Webseiten wie **Online-Banking, Online-Shops** oder das **hauseigene Drahtlosnetzwerk,** sollten **unbedingt verschiedene Passwörter gewählt werden,** um den Zugang für Unbefugte zu erschweren.

4.) Vermeiden Sie unbedingt Wörter die in Wörterbüchern vorkommen! Passwort Cracker verwenden oft Programme, die einfach stur alle existierenden Wörter durchprobieren. Am sichersten ist es, wenn sie irgendwelche sinnlosen Zeichenfolgen (gemischt mit Zahlen und Sonderzeichen) verwenden.

5.) Vermeiden Sie es, den Benutzernamen (oder Teile davon) als Passwort wieder zu verwenden.

6.) Vermeiden Sie eine Reihenfolge oder Wiederholungen von Zeichen. Wenn Sie Kombinationen wie „123456“, „0815“ oder „asdfghjklö“ verwenden, ist Ihr Kennwort nicht sicher.

7.) **Ändern Sie Ihre Kennwörter regelmäßig.** Eine nur marginale Änderung wie die Abwandlung des letzten Zeichens ist keine wirksame Änderung. Versuchen Sie, Ihre Kennwörter regelmäßig und komplett zu ändern.

8.) **Halten Sie Ihre Kennwörter auf alle Fälle geheim** und teilen Sie Ihre Kennwörter niemandem mit.

9.) Versenden Sie keine Passwörter per Mail, auch nicht wenn Sie dazu aufgefordert werden!

Aber wie erstelle ich ein sicheres Kennwort, das ich mir auch merken kann?

Dazu gibt es zwei sehr einfache Methoden:

1.) Denken Sie sich einen Satz aus, den Sie sich gut merken können. Geeignet sind Sätze wie „Ich bin seit 5 Jahren verheiratet“ oder „Mein Motorrad ist eine BMW und ich habe sie 2005 gekauft“. Nehmen jeweils den Anfangsbuchstaben eines jeden Wortes und bilden daraus ein eigenes Wort. Beim ersten Satz wäre das dann „Ibs5Jv“ oder beim zweiten „MMieBuihs2005g“. Diese Kombination können Sie dann noch um Zahlen oder Sonderzeichen ergänzen, bzw. absichtlich Rechtschreibfehler einbauen.

   Um sich nicht zusätzlich noch Sonderzeichen merken zu müssen, können Sie auch hier einen Trick anwenden, indem Sie verschiedene Buchstaben durch Zeichen ersetzen, die so ähnlich aussehen. Bei dem ersten Kennwort können Sie beispielsweise statt „Ich bin seit 5 Jahren verheiratet“ auch „Ich bin $eit 5 Jahren verheiratet“ („Ib$5Jv“) verwenden, oder im zweiten Beispiel können sie statt „Mein Motorrad ist 3ine BMW & ich habe $ie 2005 gekauft“ („MMi3B&ih$2005g“) einsetzen. Durch diese Methode ergeben sich Kombinationen, die ein sicheres Passwort ergeben.

2.) Die zweite Möglichkeit besteht darin, Zeichenfolgen die Sie sich leicht merken können (wie z.B. den Namen Ihres Kindes) methodisch durch Zahlen zu ersetzen, und diese dann mit Zeichen zu kombinieren. Das klingt verwirrend, ist aber ganz einfach. Nehmen Sie ihre Handytastatur und betrachten Sie den Ziffern- und Zeichenblock: Würden Sie ein SMS schreiben und beispielsweise den Namen „Daniela“ in ein SMS tippen, würden Sie die Zahlenkombination „3264352“ eintippen (da der Buchstabe „D“ bei der Zahl 3 ist, der Buchstabe „a“ bei 2, der Buchstabe „n“ bei 6, usw.). Auch hier empfiehlt es sich, zu kombi-

nieren, indem Sie beispielsweise jeden zweiten Buchstaben als Zahl machen oder durch ein Sonderzeichen ersetzen. D@643L2 wäre eine Kombination, die allen Sicherheitsanforderungen entsprechen würde.

Voll sicher surfen!

Mit Tele2 können Sie nicht nur voll **schnell** surfen, sondern sind auch **absolut sicher** im Internet unterwegs. Denn neben unseren Highspeed Internet-Anschlüssen bietet Ihnen Tele2 mit dem Sicherheitspaket auch einen **Komplettschutz für Ihren Computer** und Ihre persönlichen Daten. Damit sind alle Ihre Familienbilder, Urlaubsfotos, Musikdateien, Videos, Adressen und Bankdetails perfekt vor Viren, Trojanern, Würmern und sonstigen Schädlingen aus dem Internet geschützt.

Und auch was die Sicherheit Ihrer Kinder im Internet betrifft, können Sie voll auf Tele2 vertrauen. Sämtliche Seiten mit Inhalten, die nicht jugendfrei sind, können mit einer Kindersicherung blockiert werden.

Mehr Infos zum Sicherheitspaket von Tele2 auch unter www.tele2.at/sicherheit

TELE2

Kontakt-börsen

Eine von Parship veröffentlichte Studie aus dem Jahr 2010 kommt zu dem Ergebnis, dass jede vierte in Österreich lebende Person alleinstehend ist. Mehr als die Hälfte der Singles (53 %) ist länger als 3 Jahre allein stehend und somit Langzeit-Single. Die höchste Single-Quote findet sich in der Altersgruppe zwischen 18 und 29 Jahren (38 %), die 50- bis 59-Jährigen sind am seltensten alleine (16 %). Zwei Drittel der befragten Singles hätte gerne eine Partnerschaft, haben aber wegen dem Wunsch nach Unabhängigkeit, hohen Ansprüchen und arbeitsbedingtem Zeitmangel noch immer keine Partnerin oder keinen Partner gefunden.

Quelle: www.parship.at

Worauf sollten Sie achten, wenn Sie sich entschieden haben?

Persönliche Daten

Das erste Date

Dating im Internet ist mittlerweile eine weit verbreitete „Sportart". Viele tragen sich nur aus Neugier oder zum Spaß auf einer Kontaktbörse ein, viele sind aber auch ernsthaft auf der Suche nach einer neuen Partnerin oder einem neuen Partner. Immer öfter wird aber auch berichtet, dass die Eine oder der Andere die große Liebe auf einer dieser Plattformen gefunden hat.

Wichtig ist zunächst einmal, die richtige Website für die eigenen Bedürfnisse auszuwählen. Auf „Adult Friend Finder" beispielsweise, werden Sie eher schwer den Mann oder die Frau fürs Leben finden, umgekehrt werden Sie auf „Parship" kaum ein Date nur für eine Nacht vereinbaren können.

Abgesehen von diesen beiden Plattformen (und noch ein paar anderen Branchenriesen) gibt es viele kleinere Sites, die sich z. T. an ganz spezielle Zielgruppen wenden, wie etwa „Jewish Singles". Es zahlt sich daher aus, auch ein wenig Zeit in die Auswahl der richtigen Kontaktbörse zu investieren, bevor Sie sich – meist durch den Einsatz kleiner bis mittlerer Scheine – „auf ewig binden". Beispiele für beliebte Singlebörsen in Österreich sind unter anderem → Websingles, love.at, Parship, Elite Partner oder friendscout24.

→ www.love.at
→ www.parhip.at
→ www.websingles.at
→ www.elitepartner.at
→ www.friendscout24.at

Worauf sollten Sie achten, wenn Sie sich entschieden haben?

Achtung vor versteckten langen Laufzeiten

Oftmals finden sich in den Geschäftsbedingungen der Sites lange Laufzeiten für das kostenpflichtige Abo oder Regelungen über die **automatische Verlängerung des Abos.**

Sie sollten also sowohl die Geschäftsbedingungen als auch jegliche Mails, die Sie in der Folge von Dating-Plattformen erhalten, genau lesen, um keine unerwünschten Abo-Verlängerungen zu riskieren!

Vorsicht vor Betrug!

Besonders als Mann bekommen Sie häufig verlockenden Angebote von jungen Damen, die vorgeben, zu Ihrer eigenen „Sicherheit" eine **besondere Telefonnummer** zu haben (deren Vorwahl mit 0900, 0930 oder 00 beginnt).

Der Anruf bei einer solchen Nummer führt mit Sicherheit dazu, dass Ihre Telefonrechnung schwindelnde Höhen erreicht (oft kosten diese Konversationen € 3,– pro Minute oder mehr). Ein Date mit diesen Damen kommt aber praktisch nie zu Stande, denn merke: Seriöse Damen haben keine Mehrwertnummern.

419 Scams auch in Kontaktbörsen

Die bereits an anderer Stelle beschriebenen 419 Scams (siehe Kapitel „E-Mail: Spam, Phishing, Viren“, S. 64) gibt es in unterschiedlichen Varianten auch auf Kontaktbörsen. Meist erhalten Sie sehr verlockende Angebote von hübschen und heiratswilligen Damen aus Russland oder Afrika, und nach längerem E-Mail-Kontakt werden Sie dann ersucht, Geld für eine neue Webcam zu schicken. Grund: Die alte Webcam ist kaputtgegangen, und die Dame möchte sich dem Gegenüber ja auch zeigen. Dumm ist nur, dass die Webcam € 1.000,– kostet und die Dame mit ziemlicher Sicherheit ein Herr ist. Die Betreiberinnen und Betreiber der jeweiligen Dating-Plattformen sind übrigens sehr dankbar, wenn Sie ihnen solche „Damen“ möglichst schnell melden, damit sie aus dem System gelöscht werden können.

Persönliche Daten

Es ist eine Grundregel im Netz, nur so viele persönliche Daten von sich zu veröffentlichen wie unbedingt nötig. Das ist auf Kontaktbörsen naturgemäß nicht so einfach, denn Sie wollen sich ja in einem vorteilhaften Licht darstellen und von anderen gefunden werden.

Auf **keinen Fall sollten Sie Daten veröffentlichen, die auf Ihren richtigen Namen oder Ihre Wohnadresse schließen lassen.** Seriöse Kontaktbörsen erkennen Sie auch daran, dass E-Mail-Adressen der Mitglieder geheim gehalten und keine Profile mit Telefonnummern zugelassen werden.

→ mail.google.com
→ mail.yahoo.de
→ home.live.com
→ www.gmx.at

Am besten, Sie legen sich für diese Zwecke eine eigene E-Mail- Adresse zu, die nicht mit Ihrem Namen oder in Nick Verbindung steht (z. B. → Yahoo, Windows Live, GMX oder Google Mail). Doch auch hier ist Vorsicht geboten: Oftmals registriert man sich eine E-Mail-Adresse (z.B. 0815@gmx.at) und muss dann den eigenen Namen angeben. Einige Mailprogramme tragen dann diesen (oft richtig angegebenen) Namen in den

Absender mit ein und bei versendeten E-Mails steht dann „0815@gmx.at [Robert Meier]“. Somit ist der richtige Name für die Empfängerin oder den Empfänger klar ersichtlich, was im Falle einer Kontaktbörse meist nicht wünschenswert ist.

TIPP

Ein Beispiel

Sie registrieren sich auf einer Single-Börse unter angel-for-u@gmx.at. Wenn andere Personen auf Google nach dieser Adresse suchen, finden sie Ihre Homepage, denn dort steht die Adresse auch. Auf Ihrer Homepage steht auch Ihr richtiger Name. Eine Nachfrage im elektronischen Telefonbuch genügt, und Ihre Postadresse und Ihre Handynummer sind ebenfalls bekannt.

Fazit

In weniger als zehn Minuten sind die persönlichen Details aus Ihrem Single- Börsen-Profil mit Ihren realen Daten verknüpfbar – was durch die Wahl eines anderen Namens leicht vermieden werden kann.

Das erste Date

Bitte bedenken Sie, dass die Person, die Sie auf Grund des E-Mail-Kontakts zu treffen glauben, unter Umständen nicht jene ist, die dann zum Date kommt.

Wie im realen Leben gibt es auch im Internet jede Menge „verrückte“ Menschen; es ist daher vor allem für Frauen gut und wichtig, gewisse **Vorsichtsmaßnahmen** zu ergreifen. Treffen Sie sich beim ersten Date auf öffentlichen Plätzen oder in Lokalen und schauen Sie sich die Menschen gut an, mit denen Sie sich treffen. Es ist nicht ratsam, jemanden sofort nach Hause einzuladen oder zu jemandem, den Sie über eine Single-Börse kennen gelernt und zuvor noch nie gesehen haben, in die Wohnung zu gehen.

Wenn Sie besonders misstrauisch sind oder sonst Grund zur Besorgnis haben, können Sie zusätzlich auch noch regelmäßigen Telefonkontakt mit einer Freundin oder einem Freund vereinbaren.

Filesharing, BitTorrent & Streaming

Unter Filesharing (gemeinsamer Dateizugriff) wird die direkte Weitergabe von Dateien im Internet unter Verwendung eines Peer-to-Peer Netzwerkes bezeichnet. Dabei finden sich die Daten auf dem Computer aller teilnehmenden Personen oder Servern und werden von dort aus weltweit verteilt. Üblicherweise werden die Daten von fremden Rechnern kopiert (Download), während gleichzeitig andere Daten versendet werden (Upload). Große Peer-to-Peer Netzwerke haben mehrere Millionen Teilnehmerinnen und Teilnehmer und bieten eine Vielfalt an Dateien an.

Quelle: de.wikipedia.org

Dürfen Sie Musik oder Videos aus dem Internet downloaden?
Dürfen Sie Musik oder Videos zum Download anbieten?
Streaming

Online-Tauschbörsen, in denen Musik, Videos oder auch Software getauscht bzw. heruntergeladen werden können, sind so beliebt wie umstritten.

Täglich werden verschiedene ☛ *BitTorrent*-Clients oder ähnliche Filesharing-Programme, die einen Download ermöglichen, millionenfach verwendet.

☛ BitTorrent:
Ein Protokoll, das den Datenaustausch über ein großes Netzwerk ermöglicht.
Im Vergleich zum herkömmlichen Herunterladen einer Datei mittels HTTP oder FTP werden bei der BitTorrent-Technik die (ansonsten ungenutzten) Upload-Kapazitäten der Downloader mitgenutzt, auch wenn sie die Datei erst unvollständig heruntergeladen haben.

Durch das Herunterladen eines Werks von einer derartigen Tauschbörse verstoßen Sie in der Regel gegen das Urheberrecht. Ein Werk ist eine individuelle geistige Schöpfung im Bereich der Musik, der Literatur, der bildenden Kunst oder der Filmkunst. Diese Schöpfung muss sich vom Alltäglichen abheben. Computerprogramme (Software) gelten nach österreichischem Urheberrecht als Sprachwerke, also als Werke der Literatur. Auch Computerspiele sind daher als Sprachwerke anzusehen.

Die Urheberin oder der Urheber hat das alleinige Recht, ihr oder sein Werk öffentlich zugänglich zu machen, zu vervielfältigen, zu verbreiten, zu senden, zu vermieten und öffentlich wiederzugeben. Auf Tauschbörsen und auch Websites werden vor allem zwei Rechte verletzt: Einerseits wird das Werk Anderen öffentlich zugänglich gemacht, andererseits spätestens durch die Abspeicherung von unerlaubten Kopien vervielfältigt.

Dürfen Sie Musik oder Videos aus dem Internet downloaden?

Ob der reine Download von Musik oder Videos aus dem Internet (also ohne die Datei zum Upload freigeschaltet zu haben, wie dies allerdings typischerweise beim ☛ *File-Sharing* der Fall ist) erlaubt ist, ist auch in der juristischen Fachwelt umstritten. Die Einen sehen darin eine erlaubte Vervielfältigung zum privaten Gebrauch, die Anderen meinen, auch diese Vervielfältigung zum privaten Gebrauch sei nicht erlaubt, wenn bereits die Vorlage selbst unrechtmäßig hergestellt oder erlangt wurde. Eine eindeutige Antwort auf diese Frage ist leider derzeit nicht möglich, **auf der sicheren Seite sind Sie nur, wenn Sie von zweifelhaften Quellen nichts herunterladen.**

☛ File-Sharing:
Der Austausch von Dateien erfolgt auf File-Sharing-Plattformen. Die erste derartige Plattform war Napster. File-Sharing funktioniert normalerweise in Peer-to-Peer-Netzwerken.

Unproblematisch ist hingegen, wenn Sie Musik und andere Dateien

(z.B. Videoclips) von Portalen beziehen, die die erforderlichen Verwertungsrechte erworben haben, wie z. B. Apples iTunes Music Store oder MP3 Downloadstore auf Amazon.

Zu beachten ist weiters, dass auch Software urheberrechtlich geschützt ist und nicht einmal eine Vervielfältigung zum eigenen oder privaten Gebrauch erlaubt ist. Ohne urheberrechtliche Zustimmung ist ein Download von derartigen Programmen somit immer illegal. Software darf nur zum Zweck der Erstellung einer „Sicherheitskopie" vervielfältigt werden. Eine Sicherheitskopie darf nicht parallel zur Originalsoftware betrieben oder verbreitet werden.

Einfacher ist es Bilder zu nutzen, welche unter eine „Creative Commons Lizenz" gestellt wurden. Diese dürfen im nicht-kommerziellen Bereich überwiegend gratis genutzt werden. Nähere Informationen darüber findet man unter: → http://www.creativecommons.at

→ www.creativecommons.at

Das illegale Besorgen von Entsperrcodes für Demoversionen oder Shareware ist genauso unzulässig. Wird ein Programm hingegen von Berechtigten als Freeware zur Verfügung gestellt, dann ist der Download erlaubt.

Dürfen Sie Musik oder Videos zum Download anbieten?

Hier gibt es eine einheitliche juristische Meinung: **Ohne Erlaubnis der Rechteinhaberin oder des Rechteinhabers darf nichts zum Download angeboten werden.**

Besondere Vorsicht ist bei Downloads über Bittorrent (File-Sharing-Protokoll) geboten: Sobald Sie einen Download starten, können andere ebenfalls auf diese Datei zugreifen und sie wiederum von Ihrem Computer herunterladen. Auch wenn Sie selbst erst Bruchstücke eines Files auf der Festplatte haben, bieten Sie dieses dadurch wieder zum Download an!

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 privaten Gebrauch scheidet somit aus. Es ist daher ratsam, den Upload zu deaktivieren oder selbst nur Material anzubieten, das urheberrechtlich unbedenklich ist.

Streaming

Als ☛ *Streaming* bezeichnet man den Vorgang der Datenübertragung, bei dem Audio- oder Videodateien am Rechner des Nutzers wiedergegeben werden können. Auf manchen Plattformen können beispielsweise ganze Filme über dieses **„On Demand Streaming"** angeschaut werden. Es gibt aber auch die Möglichkeit des Livestreams, bei dem die Übertragung nicht vom Benutzer oder von der Benutzerin zeitversetzt abgerufen wird, sondern die Übertragung „live" zu der Veranstaltung oder zu der ausgestrahlten Sendung läuft. Viele Radiosender bieten beispielsweise mittlerweile einen Livestream ihrer ausgestrahlten Sendungen über die eigene Webseite an. Aber auch **punktuelle Livestreams bei Veranstaltungen, Podiumsdiskussionen oder Konzerten** erfreuen sich immer größerer Beliebtheit.

☛ Streaming: Datenübertragung, bei der gleichzeitig Audio- oder Videodateien downgeloadet und abgespielt werden können.

Plattformen, die Server verlinken auf denen urheberrechtlich geschütztes Material illegal zur Verfügung gestellt wird, sind mit Vorsicht zu genießen. Einerseits ist die juristische Fachmeinung nicht eindeutig, ob das Betrachten eines gestreamten Filmes legal ist oder nicht: die **Server die derartiges Material zum Streaming anbieten, begehen mit Sicherheit eine Copyrightverletzung.** Andererseits besteht bei derartigen Streaming Webseiten oft die Gefahr, dass Sie in eine Abzocke oder Phishing-Falle tappen: oft werden hier Abos, die einen schnelleren Download versprechen angeboten, bzw. wird versucht Ihnen über Links auf andere Seiten persönliche Daten oder Passwörter heraus zu locken. Wollen Sie sich also keiner derartigen Gefahr aussetzen und auch beim Urheberrecht auf Nummer sicher gehen, sollten Sie derartige Angebote lieber meiden.

Unbedenklich hingegen ist die Lage zumeist bei Livestreams: die übertragene Veranstaltung kann unbedenklich und ohne Rechts- oder Urheberrechtsverletzungen live konsumiert werden. Völlig legal ist außerdem, wenn Sie sich Sendungen auf der Internetseite eines Radio- oder Fernsehsenders anhören oder ansehen.

Cybercrime

Im Jahr 2010 gingen bei der österreichischen Meldestelle für Kinderpornografie und nationalsozialistische Wiederbetätigung (Stopline) 5.021 Meldungen ein, von denen 1.005 zutrafen und zur weiteren Untersuchung an die Polizei weitergeleitet wurden. Von den zutreffenden Meldungen fielen 65% in den Bereich Kinderpornografie, 7% entsprachen dem Tatbestand der NS-Wiederbetätigung. Die meisten Meldungen hatten ihren Ursprung in den USA, gefolgt von Russland, Deutschland und den Niederlanden.

Quelle: Stopline

Was ist im Netz erlaubt und was nicht?

Ab welchem Alter können Sie sich strafbar machen?

Pornografie im Internet

Nationalsozialistische Wiederbetätigung

Hacking

Stalking

Strafbare Postings

Was ist im Netz erlaubt und was nicht?

Wie schon gesagt, im Großen und Ganzen ist es wie in der nichtvirtuellen Welt: was dort verboten ist, ist auch im Internet verboten.

Ab welchem Alter können Sie sich strafbar machen?

Sobald Sie das 14. Lebensjahr vollendet haben, können Sie für strafbare Handlungen zur Verantwortung gezogen werden. Bis zur Vollendung des 18. Lebensjahres gilt allerdings das Jugendstrafrecht, das geringere Strafausmaße (meist die Hälfte der Erwachsenenstrafe) vorsieht.

Das heißt aber nicht, dass Kinder unter 14 Jahren tun und lassen können, was sie wollen. In ernsten Fällen sind Maßnahmen nach dem Jugendwohlfahrtsgesetz zu verhängen.

Auch das Pflegschaftsgericht kann tätig werden, wenn sich Eltern nicht hinreichend um ihr Kind kümmern. Das Kind kann unter Aufsicht des Jugendamtes gestellt werden, und im äußersten Fall, kann den Eltern das Erziehungsrecht entzogen werden.

Pornografie im Internet

In Österreich hat das Konsumieren von „legalen" pornografischen Inhalten auf Websites für Personen, die diese Inhalte konsumieren, grundsätzlich keine rechtlichen Folgen.

Anders ist es, wenn sich auf einer solchen Seite illegale Bilder befinden, in erster Linie Missbrauchsdarstellungen von Kindern. Hier ist seit dem 1.6.2009 **neben dem Besitz auch die wissentliche Betrachtung strafbar.**

Besitz liegt dann vor, wenn eine solche Darstellung auf dem eigenen Computer gespeichert wird. In der Regel werden die Elemente einer Website schon beim bloßen Ansehen temporär auf der Festplatte gespeichert. Bereits das kann als Besitz eines Bildes gelten!

Eine wissentliche Betrachtung kann z. B. dann angenommen werden,

wenn auf eine Seite mit eindeutigem Material wiederholt zugegriffen wird.

Als Kinderpornografie gilt die Darstellung sexueller Handlungen an Personen unter 18 Jahren oder von Personen unter 18 Jahren an sich selbst, anderen oder Tieren.

Missbrauchsdarstellungen von Kindern unter 14 Jahren sind immer strafbar. Es reicht bereits der Eindruck, dass es zu einer sexuellen Handlung gekommen ist (z. B. eine Fotomontage).

Bei Betrachten oder bloßem Besitz von solchen Darstellungen gilt ein Strafrahmen von bis zu einem Jahr; handelt es sich um Aufnahmen Unmündiger (unter 14), beträgt der Strafrahmen bis zu zwei Jahre Gefängnis (für Erwachsene).

Diese Strafe kann sich auf bis zu fünf Jahre erhöhen, wenn Kinder zwecks Aufnahmen missbraucht werden oder derartiges Material auch nur anderen zugänglich gemacht wird. Jemand, der sich z. B. ein Missbrauchs-Video über eine Tauschbörse herunterlädt und dieses Video anderen zum Download bereitstellt, fällt unter den höheren Strafsatz.

→ www.stopline.at
→ www.bmi.gv.at

Wenn Sie auf Missbrauchsdarstellungen im Internet aufmerksam werden, können Sie sich anonym an die → Stopline (die Meldestelle der ISPA) oder an die → Meldestelle des Bundesministeriums für Inneres wenden.

Nationalsozialistische Wiederbetätigung

Es ist strafbar, in einem Medium (z.B. im Internet) **nationalsozialistische Verbrechen zu leugnen, zu verharmlosen oder gutzuheißen;** dazu zählt z. B. die Auschwitz-Lüge. Der Strafrahmen beträgt bis zu zehn Jahren Haft.

Noch empfindlichere Strafen gibt es für die Gründung von nationalsozialistischen Verbindungen, das Anwerben von Mitgliedern für eine solche Verbindung, oder auch für die bloße Beteiligung daran. All diese Handlungen sind alle auch im Internet möglich.
Sollten Sie im Netz auf Material stoßen, dass Ihrer Meinung nach unter

nationalsozialistische Wiederbetätigung fällt, gibt es auch hier die Möglichkeit, sich an die → Stopline, die österreichische Meldestelle für Kinderpornografie und NS Wiederbetätigung, zu wenden.

→ www.stopline.at

Hacking

Beim Begriff Hacking handelt es sich um **unerlaubtes Eindringen in ein fremdes Computersystem.** Dieses ist allerdings nur dann strafbar, wenn Sicherheitsvorkehrungen des Systems verletzt bzw. überwunden werden und sich die Täterin oder der Täter zusätzlich einen Vermögensvorteil verschaffen, oder die Betreiberin oder den Betreiber des Systems schädigen will (z. B. durch Auskundschaften vom Betriebsgeheimnissen).

Aber auch die Störung der Funktionsfähigkeit eines Computersystems ist (wenn nicht schon als Datenbeschädigung) strafbar, ebenso wie das Umgehen von Zugangsbeschränkungen oder technischer Sperren. Eine Freiheitsstrafe bis zu 6 Monaten ist zu erwarten.

Stalking

2006 ist in Österreich das so genannte „Anti-Stalking Gesetz“ (Tatbestand der „beharrlichen Verfolgung“) in Kraft getreten. Dabei geht es darum, die Opfer von Stalking vor weiterer Verfolgung zu schützen, indem die beharrliche Verfolgung und die damit verbundene Unzumutbarkeit für die Opfer unterbrochen wird. Unter Stalking fallen folgende Verhaltensweisen durch die Täterin oder den Täter über einen längeren Zeitraum:

Der Stalker oder die Stalkerin

- sucht die räumliche Nähe des Opfers
- stellt mithilfe von Telekommunikation oder durch sonstige Kommunikationsmittel oder über Dritte den Kontakt zum Opfer her
- bestellt unter Verwendung der persönlichen Daten des Opfers Waren oder Dienstleistungen in dessen Namen
- bewegt unter Verwendung der persönlichen Daten des Opfers Dritte dazu, mit dem Opfer Kontakt aufzunehmen

Wird die Lebensführung des Opfers also unzumutbar beeinträchtigt, reichen die Konsequenzen von Wegweisung über Betretungsverbote bis hin zur Festnahme. Der Strafrahmen bei einer Verurteilung wegen Stalkings beträgt bis zu einem Jahr Haft.

Strafbare Postings

Üble Nachrede

Unter übler Nachrede wird der Vorwurf einer verächtlichen Gesinnung oder Eigenschaft oder eines unehrenhaften Verhaltens (z. B. Faschist, Rechtsextremist etc.) oder eines Verhaltens gegen die guten Sitten in der Öffentlichkeit verstanden.

Für das Kriterium „Öffentlichkeit" reicht schon die Anwesenheit einer einzigen weiteren Person neben der betroffenen Person. Handelt es sich um eine wahre Behauptung, ist dies nicht strafbar, sofern das Zutreffen der Behauptung bewiesen werden kann. Die Strafe kann bis zu sechs Monate betragen. Werden die Behauptungen jedoch einer breiten Öffentlichkeit zugänglich gemacht, was bei übler Nachrede im Internet zutreffen kann, gilt ein Strafrahmen bis zu einem Jahr (siehe dazu auch Kapitel"Communities, Foren, Chats", S. 52).

Ehrenbeleidigung

Eine Beleidigung liegt vor, wenn Sie eine **andere Person öffentlich** oder vor mehreren (mindestens zwei zusätzlichen) Personen **beschimpfen oder verspotten.** Greift jemand eine andere Person unter Angabe Ihres Namens auf seiner eigenen Homepage, in Chatrooms oder Foren auf diese Weise an, kann er oder sie sich leicht (bei einem Strafrahmen von bis zu drei Monaten) strafbar machen.

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

Selbst wenn es sich um anonyme Beteiligte in einem Chatroom handelt, kann eine Beleidigung vorliegen, z. B. wenn die beleidigte Person regelmäßig unter dem gleichen ☛ *Nicknamen* auftritt und auf Grund des Imageverlustes diesen Nicknamen nicht mehr verwenden kann (siehe dazu auch Kapitel"Communities, Foren, Chats", S. 52).

Verleumdung

Wird jemand einer strafbaren Handlung verdächtigt, obwohl klar ist, dass

der Vorwurf nicht zutrifft, und besteht dabei die Gefahr, dass die oder der Betroffene auf Grund dieser Verdächtigung durch die Polizei oder die Staatsanwaltschaft verfolgt wird, kann die Freiheitsstrafe je nach Schwere der vorgeworfenen Straftat bis zu einem Jahr oder bis zu fünf Jahren betragen.

Kreditschädigung

Auch die Behauptung von unrichtigen Tatsachen kann strafbar sein, wenn dadurch der Kredit, der Erwerb oder das berufliche Fortkommen anderer geschädigt oder gefährdet wird. Eine Freiheitsstrafe bis zu sechs Monaten oder eine Geldstrafe bis zu 360 Tagessätzen kann verhängt werden.

Internet am Arbeitsplatz

In Österreich haben 97% aller Unternehmen einen Internetzugang. 82% dieser Unternehmen verfügen über einen Breitbandzugang, davon wählen sich 76% mittles Breitbandverbindung über eine fixe Leitung und 46% über eine mobile Breitbandverbindung ein. Über eine eigene Webseite verfügen 81% der Unternehmen, 51% haben schon im Internet eingekauft und 18% haben aktiv über das Internet Waren verkauft.

Quelle: Statistik Austria, Zahlen aus 2010

Mittlerweile ist es Standard, dass Büroarbeitsplätze mit einem Internetzugang ausgestattet sind. Wie schon vor Jahrzehnten beim Telefonanschluss stellt sich auch hier die Frage, wie weit Sie als Arbeitnehmerin oder Arbeitnehmer diesen Anschluss privat nutzen dürfen. **Es ist auch unklar, ob die Arbeitgeberin oder der Arbeitgeber kontrollieren darf, welche Websites von Ihnen angeschaut wurden, und ob Ihre privaten E-Mails gelesen werden dürfen.**

Es kommt auf die vertragliche Regelung zwischen Arbeitgeberin oder Arbeitgeber und Arbeitnehmerin oder Arbeitnehmer an. Grundsätzlich können drei Szenarios unterschieden werden, die die Nutzung des Internets am Arbeitsplatz beeinflussen können:

1.) Die Arbeitgeberin oder der Arbeitgeber hat jegliche Privatnutzung des Internets (und damit auch private E-Mails) untersagt.
2.) Die Arbeitgeberin oder der Arbeitgeber hat die Privatnutzung erlaubt (wenngleich nur in einem bestimmten Umfang).
3.) Es gibt keinerlei Abmachung über die Nutzung des Internets.

Zu Punkt 1 ist anzumerken, dass ein dermaßen umfassendes Verbot tatsächlich ausgesprochen werden darf. Eine Ausnahme stellen hier bloß Notsituationen dar: Ein privates Nottelefonat und das vorherige Suchen der richtigen Telefonnummer im Internet oder das Lesen eines E-Mails, mit dem Sie z. B. über eine Notsituation informiert werden, ist (trotz Verbots der Privatnutzung) als zulässig anzusehen.

Surfen Sie trotz Verbots privat im Netz oder schreiben und lesen private E-Mails, so stellt dies einen Entlassungsgrund dar, wenn Sie trotz Ermahnung beharrlich weiter privat surfen oder mailen.

In Punkt 2 stellt sich nur mehr die Frage, inwieweit die Internetnutzung kontrolliert werden darf. Darüber hinaus ist ein so genanntes „Exzessverbot“ zu beachten, was bedeutet, dass die Nutzung nicht übertrieben werden darf.

Punkt 3 ist am schwierigsten klar zu beantworten. Gibt es keinerlei offizielle Abmachung, so ist, was die Internetnutzung betrifft, der betriebliche Usus, die Betriebssitte (= Übung) ausschlaggebend. Hier kommt es ohne eine schriftliche oder explizite mündliche Vereinbarung zu einer Ergän-

zung des Arbeitsvertrages durch die so genannte Übung. Es gilt aber natürlich auch hier ein „Exzessverbot“.

Darf Internetnutzung am Arbeitsplatz kontrolliert werden?

Wurde die private Internetnutzung in einem Unternehmen verboten und die Mitarbeiterinnen und Mitarbeiter darauf hingewiesen, dass das Verbot kontrolliert wird, **so ist dies auch gesetzlich erlaubt.**

Er darf vom Unternehmen jedoch nur kontrolliert werden, ob die Arbeitsaufträge sorgfältig und zur Zufriedenheit ausgeführt wurden. Die Arbeitgeberin oder der Arbeitgeber muss sich bei ihrer oder seiner Kontrolle des gelindesten Mittels bedienen. Um Arbeitsaufträge zu überprüfen, ist beispielsweise das Lesen der E-Mails erlaubt.

Schwieriger wird es, wenn die Internetnutzung entweder explizit erlaubt ist oder es der Betriebssitte entspricht, dass das Internet zu einem gewissen Umfang privat genutzt wird. In diesem Fall dürfen Ihre E-Mails nur (inhaltlich) kontrolliert werden, solange nicht erkannt wird, dass es sich um eine private Nutzung handelt.

Haben Sie also nur eine E-Mail-Adresse für berufliche und private Mails, dann müssen Sie damit rechnen, dass auch Ihre privaten E-Mails von Zweiten gelesen werden.

Besitzen Sie jedoch am Arbeitsplatz einen eigenen Ordner für private Mails oder gar einen eigenen Account, so ist für die Arbeitgeberin oder den Arbeitgeber die Trennung erkennbar, und Ihre private Post darf von ihr oder ihm nicht durchgesehen werden.

Elektronische Signatur und E-Government

In Österreich können mit der Bürgerkarte schon viele Amtswege online erledigt werden. Als Bürgerkarte werden zum Beispiel das eigene Handy oder die E-Card eingesetzt. Beide Möglichkeiten müssen jedoch vorher aktiviert werden, um als elektronische Signatur zu fungieren. Ist das Handy erst einmal aktiviert, reicht ein Internetzugang um rund um die Uhr Amtswege erledigen zu können. Um mit der E-Card aktiv zu werden, benötigt man ein Kartenlesegerät und die dazugehörigen Programme.

Quelle: www.buergerkarte.at

Die elektronische (oder digitale) Signatur soll dazu dienen, einen erheblichen Nachteil des elektronischen Alltags zu beheben, den es in der normalen Papierwelt nicht gibt: Sie können elektronische Dokumente nicht mit Ihrer handschriftlichen Unterschrift versehen. Es ist daher nicht eindeutig feststellbar, ob eine bestimmte Person mit etwas einverstanden ist oder etwas erhalten hat, weil diese sich nicht selbst identifizieren kann.

Die elektronische Signatur ist die elektronische Unterschrift einer Person, die all das, was eine handschriftliche Unterschrift leistet, in der elektronischen Welt bietet. Um Einheitlichkeit und Sicherheit vor Missbrauch, Fälschung usw. zu gewährleisten, wurden ein eigenes Gesetz und eine Ausführungsverordnung geschaffen und außerdem eine Behörde (die → RTR) mit der Aufsicht über elektronische Signaturen beauftragt. In Österreich stellt z.B. die → A-Trust elektronische Signaturen aus.

→ www.rtr.at
→ www.a-trust.at

Technisch gesehen besteht eine digitale Signatur aus einem Code, der durch ein kompliziertes mathematisches Verfahren aus mehreren Komponenten errechnet wird. Dadurch kann sichergestellt werden, dass ein signiertes Dokument (z. B. ein E-Mail) tatsächlich von der Person stammt, die es signiert hat, und dass es seit dem Signaturvorgang auch nicht verändert (gefälscht) wurde.

Als Empfängerin oder Empfänger einer Rechnung sind Sie nicht dazu verpflichtet, eine Rechnung elektronisch entgegenzunehmen oder zu akzeptieren. Egal ob Sie eine Privatperson oder ein Unternehmen sind, das Unternehmen oder die Person, die Ihnen eine elektronische Rechnung ausstellt, muss Ihre Einwilligung dazu einholen (Achtung: Sehr oft ist Ihre Zustimmungserklärung schon im Bestellformular oder in den AGB enthalten). Diese Einwilligung ist an keinerlei Formvorschriften gebunden. Ein Unternehmen sollte sich diese Einwilligung jedoch bereits zu Beginn der Geschäftsbeziehung einholen, um sich Ärger und Aufwand im Nachhinein zu ersparen.

Beachten Sie: Die Erfordernisse an elektronische Rechnungen sind in diesem Leitfaden nicht umfassend dargelegt! Sollten Sie als Unternehmerin oder Unternehmer elektronische Rechnungen empfangen oder senden, ist es jedenfalls ratsam, sich zuvor eingehend steuerrechtlich oder juristisch beraten zu lassen.

Aber auch als Privatperson bietet Ihnen die elektronische Signatur in Verbindung mit dem Internet wesentliche Erleichterungen, vor allem bei der Erledigung von Behördenwegen: Auf → help.gv.at finden Sie schon zahlreiche Anwendungen der elektronischen Signatur. So können Sie sich viele Behördenwege ersparen. Um die elektronische Signatur verwenden zu können müssen Sie eine → „Bürgerkarte“ (elektronischer Ausweis am Handy oder auf der e-card) aktivieren lassen und können alle Funktionen der Bürgerkarte nützen.

→ www.help.gv.at

→ www.buergerkarte.at

Es ist nunmehr möglich, auch außerhalb der normalen Arbeitszeit (und vor allem außerhalb von Amtszeiten) z.B. Strafregisterauszüge zu beantragen, sich eine Meldebestätigung zu holen und vieles mehr.

Ziel des E-Governments ist es, dass die Bürgerinnen und Bürger nur mehr in Ausnahmefällen persönlich zum Amt kommen müssen. Eine der derzeit meistgenutzten E-Government-Anwendungen ist → „FinanzOnline“. Damit ist es möglich, auf sehr einfache Weise seine Arbeitnehmerveranlagung zu erledigen und sich eventuell zu viel bezahlte Lohnsteuer vom Finanzamt zurückholen.

→ finanzonline.bmf.gv.at

Anonymität & Identität

Anonymität ist die Geheimhaltung der Identität einer Person, einer Gruppe, einer Institution oder einer agierenden Struktur.

Identität ist die den Menschen kennzeichnende und als Individuum von anderen Menschen unterscheidende Eigentümlichkeiten seines Wesens. Häufig wird darunter auch die Summe der Merkmale verstanden, anhand derer sich ein Individuum von anderen unterscheiden lässt.

Quelle: de.wikipedia.org

Anonymität

Identität

Was können Sie tun, um Ihre Identität im Netz zu schützen?

Normalerweise sind Sie im Netz „unsichtbar“. Niemand weiß, wie Sie aussehen, welche Kleidung Sie tragen, oft bleibt auch Ihr Name ungenannt. Sind Sie deshalb anonym? Die kurze Antwort ist „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 oder vom ☛ *Provider* dynamisch vergeben wird.

Wann immer Sie im Internet agieren (z. B. chatten, eine E-Mail schreiben, eine Website besuchen), wird die IP-Adresse Ihres Rechners in einem ☛ *Logfile* gespeichert bzw. zusätzlich auch noch im ☛ *Header* des E-Mails verewigt.

Sie hinterlassen also Spuren, wenn Sie sich im Internet bewegen. 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 entsprechenden Computer bzw. zur entsprechenden Telefonnummer. Die meisten Internet-Straftaten können also relativ schnell und problemlos aufgeklärt werden.

Auch Personen, die nach Ihnen denselben PC benutzen, können sich einfach ansehen, welche Websites Sie besucht oder welche Programme Sie aufgerufen haben. Mit etwas technischem Sachverstand lässt sich so sehr viel über andere herausfinden.

Natürlich gibt es Tools, um sich gegen diese Art von Schnüffelei zu wehren. Diese setzen aber meist ein gewisses Maß an technischem Wissen voraus und sind trotzdem nicht unfehlbar. Ist eine genügend große Anzahl an Daten (Logfiles, verwendete Nicknames, Passwörter etc.) vorhanden, können meistens trotz Tool Ihre Aktivitäten im Netz nachvollzogen werden.

So genannte **Anonymisierungsprogramme** funktionieren technisch unterschiedlich, haben aber gemeinsam, dass sie die Internetverbindung

☛ Provider:
Unternehmen, über das Sie Zugang zum Internet bekommen. Eine Liste der österreichischen Provider finden Sie unter www.ispa.at.

☛ Logfile:
Textdatei, in der ein Server automatisch gewisse Ereignisse mitschreibt (z. B. Aufruf einer Website, herunterladen eines E-Mails). Logfiles sind für Statistiken, Ressourcenplanung und Fehlersuche von Providern unerlässlich, dienen aber oft auch als Basis für Strafverfolgung.

☛ Header:
Der „Kopf“ eines E-Mails, wo verschiedene technische Informationen zu dem jeweiligen Mail gespeichert sind (z. B. über welchen Server es verschickt wurde).

Ihres PCs über einen Anonymisierungsserver lenken. Dadurch wird die wahre Herkunft (= IP-Adresse) gegenüber dem Zielserver verschleiert. Sie müssen allerdings darauf vertrauen, dass die Anbieterin oder der Anbieter des Services selbst vertrauenswürdig ist, denn dieser kann (zumindest theoretisch) feststellen, welche IP-Adresse wohin gelenkt wird. Lediglich bei einigen wenigen Programmen werden Sie durch mehrere Server hintereinander gelenkt. Deshalb ist es mathematisch beinahe unmöglich, herauszufinden, wer sich was angesehen hat (das wird zumindest behauptet).

Anonymisierung kann in manchen Fällen sinnvoll oder notwendig sein, aber verlassen Sie sich nicht darauf!

Identität

Oft ist es aber nicht von Interesse, seine Anonymität zu schützen, sondern das genaue Gegenteil soll erreicht werden: Die eigene Identität soll geschützt werden. **Identitätsdiebstahl** war lange Zeit nur ein Thema für Science-Fiction-Filme. Nun wird es zunehmend Realität.

Der einfachste Fall ist ganz simpel, aber trotzdem vielen nicht bekannt: Sie können unter jedem beliebigen Namen E-Mails schreiben. Sie müssen dazu nur den Namen und die Absenderadresse in Ihrem eigenen E-Mail-Programm ändern, und schon können Sie als jemand anderer im Netz auftreten – freilich nicht sehr lange, denn im Netz gibt es ja keine Anonymität, wie bereits ausgeführt wurde. Sie sollten sich daher vor Augen führen, dass im Netz nicht immer alles so ist, wie es zunächst den Anschein hat.

Ein gutes Beispiel dafür sind die Absenderadressen der Spam-Mails, die Tag für Tag in unseren Mailboxen landen.

Kompliziertere Fälle von **Identitätsdiebstahl** funktionieren oft über **gestohlene Passwörter, elektronische Signaturen oder Kreditkarteninformationen.** Die Palette möglicher Schäden reicht vom Plündern des Bankkontos bis zum Ersteigern von Luxus-Limousinen, die dann an die Adresse des ahnungslosen Opfers geliefert werden.

Was können Sie tun, um Ihre Identität im Netz zu schützen?

Leider nicht sehr viel. Am besten ist es, wenn Sie einen (möglichen oder vermuteten) Identitätsdiebstahl nicht auf sich sitzen lassen und sich umgehend bei der jeweiligen Anbieterin oder beim jeweiligen Anbieter beschweren und ihn ersuchen, **Beweismaterial zu sichern.** Gegebenenfalls sollten Sie auch vor einer Anzeige nicht zurückschrecken. Wichtig ist es, immer möglichst schnell zu handeln, da oftmals Daten im Netz nicht sehr lange gespeichert werden und dann die Gefahr besteht, dass Beweise vernichtet werden.

Eine weitere Möglichkeit, sich zu wehren, besteht darin, **nur noch digital signierte E-Mails zu verschicken.** Dadurch kann die Empfängerin oder der Empfänger sicher sein, dass es sich um die angegebene Absenderin oder den angegebenen Absender handelt.

Leider funktioniert diese Methode nur bei E-Mails, nicht aber auf Websites. Nähere Informationen zur digitalen Signatur finden Sie im vorhergehenden Kapitel „Elektronische Signatur und E-Government".

TIPP

Datenschutz, Beauskunftung persönlicher Daten und Überwachung

Die oft geäußerte Ansicht, dass Ihre Präsenz und Tätigkeit im Internet anonym seien, ist nicht ganz zutreffend.

Es bestehen in allen europäischen Ländern gesetzliche Regelungen, welche es den Sicherheitsbehörden (Polizei), Verwaltungsbehörden (z. B. Fernmeldebehörde) und unter Umständen auch Privaten ermöglichen, Ihre persönlichen Daten bei Ihrem Provider zu erfragen, um die Möglichkeit einer Rechtsdurchsetzung zu haben. Dies erfolgt in der Regel über die IP-Adresse, die Ihnen von Ihrem Provider zugewiesen wird und mit der Sie für andere im Internet sichtbar sind.

Ihre Verkehrsdaten für E-Mail und Telefonie (d.h. wann Sie mit wem kommuniziert haben) sowie ihre IP-Adresse müssen laut einer eu-

ropäischen Richtlinie in Zukunft von den Internetservice-Providern gespeichert werden, um den Strafverfolgungsbehörden Auskunft geben zu können („Vorratsdatenspeicherung").

Im Rahmen der Strafverfolgung besteht für die zuständigen Behörden auch die Möglichkeit, innerhalb ihrer gesetzlichen Aufgaben Ihre Kommunikation über das Internet mit zu verfolgen und bei dem Verdacht schwerer Delikete auch zu überwachen.

Wer hilft Ihnen weiter?

Die österreichische Informations- und Koordinierungsstelle Saferinternet.at unterstützt Internetnutzerinnen und –nutzer bei der sicheren Nutzung von Internet, Handy und Computerspielen. Saferinternet.at gibt Tipps und Hilfestellungen für den kompetenten Umgang mit Risiken und zeigt gleichzeitig die positiven Aspekte bei der Nutzung auf. Die Initiative wird vom Österreichischen Institut für Angewandte Telekommunikation (ÖIAT) in Kooperation mit dem Verband der österreichischen Internet Service Provider (ISPA) koordiniert und in enger Kooperation mit der öffentlichen Hand und der Wirtschaft umgesetzt.

Quelle: www.saferinternet.at

Beschwerden über Inhalte von Websites oder Communitys

Probleme beim Internet-Einkauf

Illegale Inhalte

Für die Beantwortung von weiterführenden Fragen zur sicheren Internetnutzung sowie für Hilfe und Beratungen steht Ihnen das Team von → Saferinternet per E-Mail zur Verfügung. Ferner bietet → „147 Rat auf Draht“ in Kooperation mit Saferinternet.at für Kinder und Jugendliche eine kostenlose und anonyme Telefonberatung rund um die Uhr an: Einfach 147 wählen!

→ www.saferinternet.at
→ Rat auf Draht: ☎ 147
→ www.rataufdraht.at
→ www.ispa.at

Beschwerden über Inhalte von Websites oder Communitys

Wenn Sie sich in Ihren Rechten verletzt fühlen, **so ist die erste Adresse für Beschwerden jene Person, die das direkt zu verantworten hat,** also die Autorin oder der Autor des jeweiligen Inhaltes. Dies trifft sowohl bei E-Mail-Kommunikation als auch auf Websites und in ☛ *Communitys* zu.

☛ Communitys:
Gemeinschaft, die sich aufgrund gemeinsamer Interessen zusammengefunden hat und Austausch über Diskussionsforen, Chats oder auch Linksammlungen pflegt.

Sollte die Person auf Ihre Beschwerde nicht reagieren, so kann es unter bestimmten Umständen sinnvoll sein, sich bei **der Betreiberin oder dem Betreiber der Site zu beschweren,** also dort, wo der beanstandete Inhalt eingebunden ist. Wenn also beispielsweise ein Video auf YouTube geladen wurde, das Sie in Ihren Persönlichkeits- oder Urheberrechten verletzt, dann ist es sehr wohl sinnvoll, das Unternehmen, das die Website betreibt, aufzufordern, das File zu löschen. Eine Beschwerde ist auch angebracht, wenn ein Provider (nachweislich) einen ☛ *Spammer* beherbergt. Der Provider wird den Spammer vermutlich ermahnen oder vom Netz nehmen. Fühlen Sie sich in Ihren Rechten verletzt, können Sie immer auch **vor Gericht gehen.**

☛ Spam:
Ein Sammelbegriff für jede Art von unerwünschten E-Mails, insbesondere für Massenaussendungen zur Bewerbung scheinbar günstiger Angebote.

Probleme beim Internet-Einkauf

Ähnlich verhält es sich, wenn Sie mit Ihrem Einkauf in einem Online-Shop oder Auktionshaus unzufrieden sind. Bitte wenden Sie sich zunächst an die Person, die Ihnen die Ware verkauft hat, erst dann an den betreibenden Online-Shop.
Sollten beim Internet-Einkauf Probleme aufgetreten sein, die Sie selbst nicht lösen können, unterstützt Sie beim →Internet-Ombudsmann ein Team von Expertinnen und Experten kostenlos als neutraler Vermittler.

→ www.ombudsmann.at

Illegale Inhalte

Sollten Sie bei Ihren Streifzügen durch das Web auf illegale Inhalte gestoßen sein (insbesondere Kinderpornografie oder nationalsozialistische Wiederbetätigung), so können Sie dies bei der → Stopline (Meldestelle der österreichischen Internet-Service-Provider) oder bei der → Meldestelle des Bundesministeriums für Inneres deponieren.

→ www.stopline.at
→ www.bmi.gv.at/meldestellen

Glossar

BitTorrent Ein Protokoll, das den Datenaustausch über ein großes Netzwerk ermöglicht. Im Vergleich zum herkömmlichen Herunterladen einer Datei mittels HTTP oder FTP werden bei der BitTorrent-Technik die (ansonsten ungenutzten) Upload-Kapazitäten der Downloader mitgenutzt, auch wenn sie die Datei erst unvollständig heruntergeladen haben.

Botnetz Ein Netzwerk aus lauter ☛ *Zombies,* das ohne Wissen der Inhaberinnen und Inhaber z. B. für Versand von Spam-Mails (Phishing Mails) missbraucht wird

Community Gemeinschaft, die sich aufgrund gemeinsamer Interessen zusammengefunden hat und Austausch über Diskussionsforen, Chats oder auch Linksammlungen pflegt.

Cyber-Mobbing Bloßstellung, permanente Belästigung oder Verbreitung falscher Behauptungen über eine Person im Internet.

Domain Ist ein „Namensraum", der bei dafür verantwortlichen Registrierungsstellen beantragt werden kann. Für die Vergabe der „Top-Level"-Domain „.at" (die oberste Hierarchie-Ebene) ist die Firma nic.at verantwortlich. Unterhalb einer Domain können Namen von Services definiert werden, die auf verschiedene Rechner zeigen (z. B. ist www.xyz.at ein Rechnername der Domain xyz.at).

FAQ „Frequently Asked Questions" sind eine Zusammenstellung häufig gestellter Fragen zu einem Themenbereich oder zu einer Website.

File-Sharing Der Austausch von Dateien erfolgt auf File-Sharing-Plattformen. Die erste derartige Plattform war Napster. File-Sharing funktioniert normalerweise in Peer-to-Peer-Netzwerken.

GPS Global Positioning System ist ein Satelitensystem das der Positionsbestimmung dient.

Header Der „Kopf" eines E-Mails, wo verschiedene technische Informationen zu dem jeweiligen Mail gespeichert sind (z. B. über welchen Server es verschickt wurde).

HTML „Hyper Text Markup Language" ist jene Sprache, die zur Erstellung von Websites verwendet wird.

IMAP „Internet Message Access Protocol“ ist ein Mailprotokoll, bei dem die Nachrichten auf einem zentralen Server verbleiben und nur bei Bedarf auf den lokalen Rechner übertragen werden. IMAP ist komfortabler als POP, da es mehrere Ordner unabhängig voneinander verwalten kann.

Instant Messaging Programme Instant Messaging bezeichnet den sofortigen und unmittelbaren Versand einer Textnachricht. Meist erscheint die Nachricht in Echtzeit am Bildschirm der Empfängerin oder des Empfängers.

Location Based Services Standortbezogene Dienste, die selektive positionsabhängige Informationen bereitstellen.

Logfile Textdatei, in der ein Server automatisch gewisse Ereignisse mitschreibt (z. B. Aufruf einer Website, herunterladen eines E-Mails). Logfiles sind für Statistiken, Ressourcenplanung und Fehlersuche von Providern unerlässlich, dienen aber oft auch als Basis für Strafverfolgung.

Netiquette Ein Kompendium an Höflichkeitsregeln, welches das gute Benehmen im Rahmen der technischen (elektronischen) Kommunikation regelt.

Netizen Ein bereits leicht veraltetes Kunstwort aus „Network“ und „Citizen“, also sozusagen „Netzbürgerinnen oder Netzbürger“ oder „Bewohnerin/Bewohner des Netzes“.

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

Phishing Kunstwort aus „password“ und „fishing“. Kriminelle Methode, um Logins und Passwörter herauszufinden und z. B. Bankkonten zu plündern.

POP „Post Office Protocol“, das übliche Verfahren zur Zustellung von E-Mails. E-Mails werden auf einem Server so lange gespeichert, bis das Mail-Programm sie herunterlädt.

Provider Unternehmen, über das Sie Zugang zum Internet bekommen. Eine Liste der österreichischen Provider finden Sie unter www.ispa.at.

Server Rechner, auf dem Dateien gespeichert sind, die von anderen Rechnern (Clients) gelesen oder verarbeitet werden können (z. B. Webserver, Mailserver, aber auch Fileserver in einem Unternehmensnetzwerk).

Spam Ein Sammelbegriff für jede Art von unerwünschten E-Mails, insbesondere für Massenaussendungen zur Bewerbung scheinbar günstiger Angebote.

Streaming Datenübertragung, bei der gleichzeitig Audio- oder Videodateien downgeloadet und abgespielt werden können.

Taggen Ist das Indexieren eines Fotos mit dem eigenen Namen. Bei einer Suchanfrage können Fotos so besser gefunden werden.

TAN „TransaktionsAutorisierungsNummer“ ist eine hauptsächlich von Banken verwendete Möglichkeit, Online-Zahlungen zu verifizieren. TANs sind Zahlenfolgen und werden als Listen oder per SMS (mobile TAN oder TAC-SMS) verschickt und können jeweils nur einmal verwendet werden. TANs sind bei Phishing-Attacken das eigentliche Ziel der Betrüger, da sie zwingend für Überweisungen benötigt werden.

Trojaner Ein Programm, das vorgibt, etwas anderes zu sein, als es tatsächlich ist. Die Grenze zwischen Trojanern und Viren ist heute nur noch schwer zu ziehen, da die meisten derartigen Schädlinge beide Funktionen beinhalten.

URL „Uniform Resource Locator“ ist der allgemeine Ausdruck für eine Adresse im Netz, die z. B. mit „http://“ beginnt.

Usenet Jenes Netz, in dem die klassischen Diskussionsforen des Internets (Newsgroups) zu Hause sind. Diese entstanden bereits in den achtziger Jahren des vorigen Jahrhunderts. Newsgroups können entweder mit E-Mail-Programmen oder mit so genannten Newsreadern gelesen werden.

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

Zombie Ein Computer, der ohne Kenntniss der Besitzerin oder des Besitzers von aussen ferngesteuert wird.

Impressum:

Medieninhaber, Herausgeber, Verleger: ISPA – Internet Service Providers Austria

Verband der österreichischen Internet-Anbieter, 1090 Wien, Währinger Straße 3/18

Redaktion: Romana Cravos und Maximilian Schubert

Layout: allesgrafik.at, 1200 Wien

Druck: Gutenberg Druck GmbH, 2700 Wr. Neustadt

Fotos: S. 6: Bundeskanzleramt, Fotograf: Johannes Zinner;
S. 5: Bundesministerium für Justiz

Gefördert durch die Europäische Union – Safer Internet Programm

Alle Angaben erfolgen ohen Gewähr. Eine Haftung der Autorinnen und Autoren oder von saferinternet.at / ISPA ist ausgeschlossen.

Notizen

Notizen

Einfach alles aus einer Hand.

Mobilfunk. Festnetz. Internet. Fernsehen. Einfach Alles.

Alles bekommen, was man braucht.
Aus einer Hand. Einfach Alles. Einfach A1.

Einfach A1.

A1.net

Stopline

Eine ISPA Initiative

Österreichs Meldestelle für Kinderpornografie und nationalsozialistische Wiederbetätigung im Internet

www.stopline.at

Unterstützen Sie die Stopline! Logo unter www.stopline.at/download downloaden und auf Ihrer Webseite platzieren!

Stopline ist Partner von INHOPE