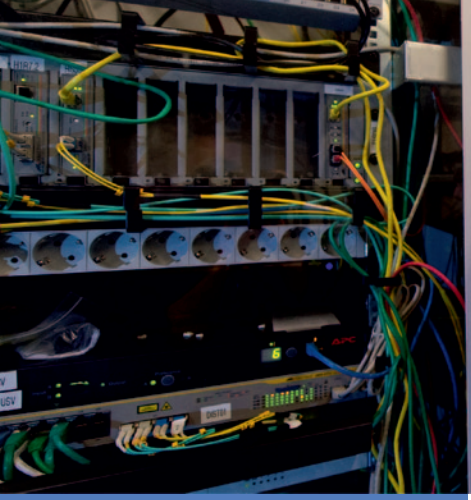
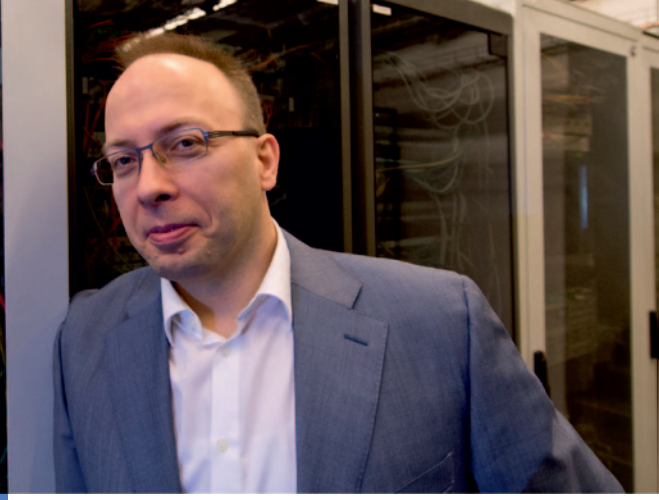
ispa
Internet Service Providers Austria

Internet sicher nutzen

Ein Leitfaden im Rahmen der Saferinternet.at-Initiative.

JUSTIZ
BUNDESKANZLERAMT ÖSTERREICH
Saferinternet.at
Das Internet sicher nutzen!
LIWEST
Ein Kabel. Alle Medien.



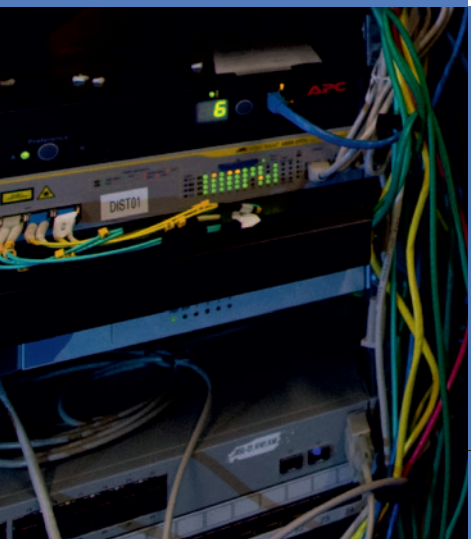


- Datendienste
- vISP
- Housing & Hosting
- SafeMail
- Cloudlösungen
- Media-Streaming
- Backuplösungen
- Remote Storage
- Softwarelösungen
- VoIP Telefonie
- Sicherheitslösungen
- Domains
- Datenschutz

Netzneutral.
Sicher. Zuverlässig.
Persönlich betreut.
Internet aus Österreich.

kapper.net

internet | communications | solutions



kapper.net betreibt seine Server und sein Netzwerk seit über 20 Jahren in Österreich. Hier gilt das Privileg, das Unternehmensdaten gleich schutzwürdig sieht, wie sonst nur Personendaten. kapper.net kann daher gesetzlichen Datenschutz für alle Informationen seiner Kunden garantieren.

kapper network-communications GmbH
Alserbachstr. 11/6 | 1090 Wien

Tel: +43 5 9080-0 | Fax: +43 1 3195502
https://kapper.net | office@kapper.net

Vorwort

von Dr. Wolfgang Brandstetter

Bundesminister für Justiz

Liebe Leserinnen und Leser,

das Internet hat sich in den vergangenen Jahren ohne Zweifel zu einem fixen Bestandteil unserer Gesellschaft entwickelt und ist aus unser aller Leben kaum mehr wegzudenken. Die Abwicklung von Bankgeschäften, die Erledigung von Behördengängen oder die Möglichkeit, sich zu jedem beliebigen Thema zu informieren – das alles ist nur einen Mausklick weit entfernt.

Millionen von Menschen weltweit sind täglich über das Internet miteinander verbunden – egal ob über Computer, Tablet oder Handy – und die Nutzung diverser Netzwerke ist spielend leicht und von fast überall aus möglich.

So positiv die vielen Errungenschaften des Internets auch sind, so müssen wir aber auch ein Bewusstsein für die damit verbundenen Gefahren schaffen. Denn mit der fortschreitenden Digitalisierung steigt leider auch die Anzahl der Delikte im Internet. Besonders der höchstpersönliche Lebensbereich wird oft zum Ziel von kriminellen Cyberattacken. Bei der vor dem Sommer beschlossenen Reform des Strafgesetzbuches haben wir daher nicht nur die bereits bestehenden gesetzlichen Regelungen modernisiert, sondern auch neue Tatbestände, wie beispielsweise „Cybermobbing“ oder „Skimming“, eingeführt. Damit haben wir auf die aktuellen gesellschaftlichen Bedürfnisse reagiert.

Doch viel wichtiger als Strafen zu verhängen, muss uns die Prävention sein. Mit dieser Broschüre werden Userinnen und User bereits im Vorfeld auf mögliche Gefahren im Netz hingewiesen, was zu einem verantwortungsvollen Umgang mit dem Internet beiträgt. Denn eines sollten wir bei der fortschreitenden Digitalisierung nicht vergessen: Hinter jedem Bildschirm sitzt immer auch ein Mensch.

Ich wünsche Ihnen viel Vergnügen und hilfreiche Informationen mit dieser Lektüre.

Vorwort

von Dr. Josef Ostermayer

Bundesminister für Kunst und Kultur, Verfassung und Medien

Informations- und Kommunikationstechnologien sind in Österreich und international ein bedeutender Faktor für das Funktionieren der Gesellschaft, der Wirtschaft und des Staates. Die Vorteile der digitalen Gesellschaft, in der wir leben und arbeiten, sind heutzutage nicht mehr wegzudenken.

Obwohl in den vergangenen Jahren die Zahl jener Menschen, die über einen Internetanschluss verfügen, enorm gestiegen ist, verfügt noch rund ein Fünftel der österreichischen Bevölkerung über keinen Zugang zum Internet. Durch entsprechende Maßnahmen, wie z. B. den weiteren Ausbau im Breitbandinternet-Bereich oder Schulungen, soll jeder Österreicherin und jedem Österreicher die Möglichkeit geboten werden, von der digitalen Vernetzung zu profitieren.

Viele der bisherigen Offliner nutzen das Netz auch deshalb nicht, weil sie es für nicht „sicher genug" erachten. Ein Befund, der von vielen aktiven Nutzerinnen und Nutzern geteilt wird. Eines der zentralen Probleme besteht 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 und Nutzer mehr Wissen erhalten, um sich etwa vor Betrugsfallen beim Onlineshopping oder Phishing-Mails besser zu schützen oder ihre Computer besser gegen Schadsoftware abzusichern. All diese Informationen bietet die vorliegende Broschüre der ISPA. Hier findet nicht nur der Internetlaie, 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.

Vorwort

von Dr. Andreas Koman

ISPA Präsident

Liebe Leserinnen und Leser!

Bereits 100.000 Exemplare dieses Ratgebers haben wir in den vergangenen Jahren vor allem an Bildungseinrichtungen verteilt. Dies spricht nicht nur Bände über die Beliebtheit dieser ISPA Publikation, sondern zeigt auch den großen Bedarf an verständlich aufbereitetem und kompaktem Informationsmaterial zum Thema Onlinesicherheit und Medienkompetenz auf. Als Interessenvertretung der österreichischen Internetwirtschaft war und ist es unser Ziel, das Internet in Österreich zu fördern. Es ist der ISPA aber ebenso ein Anliegen, dazu beizutragen, die Nutzung des Internets für alle Userinnen und User zu einem positiven und sicheren Erlebnis zu machen.

In diesem Zusammenhang freut es uns, Ihnen die neue, aktualisierte Ausgabe unseres Ratgebers „Internet sicher nutzen" präsentieren zu können. Beispielsweise haben wir die notwendigen Änderungen, die sich durch die Novellierung des Strafgesetzbuches und des Urheberrechts ergeben haben, eingearbeitet und ergänzt. Wie in den vergangenen Auflagen bieten wir auch Informationen zu den Themenbereichen Onlinekauf und -bezahlung, zu sozialen Netzwerken, Kontaktbörsen sowie zur Unterstützung der sicheren Internetnutzung von Kindern und Jugendlichen. Zudem gibt es Ratschläge für konkrete Herausforderungen in der Praxis, beispielsweise die Erstellung eigener Webseiten, Tipps zur ungebrochen aktuellen Netiquette, zur Vorsorge beim digitalen Nachlass oder zum Schutz vor Viren, Trojanern und Phishing-Mails.

Bedanken möchten wir uns an dieser Stelle auch für die Unterstützung durch das Bundeskanzleramt, das Bundesministerium für Justiz, die Europäische Union sowie unsere Projektpartner von Saferinternet.at.
Ich wünsche Ihnen eine interessante Lektüre und hoffe, dass Sie unsere Anregungen und Tipps gut nützen und umsetzen können.

Community

Abkürzungen

Emoticons

Netzjargon

Anhänge

HTML

E-Mail-Adressen

Meme

Netiquette

Seit 25 Jahren ist das Internet in Österreich verfügbar. 2013 hatten 81 Prozent aller Haushalte einen Internetanschluss. Das Internet ist aus dem privaten und beruflichen Alltag nicht mehr wegzudenken.

Kommunikation im Netz

Netiquette

Netiquette bezeichnet den höflichen und respektvollen Umgangston im Internet. Viele Onlineforen und -communitys geben eigene Benimmregeln und Verhaltensrichtlinien vor. Unter anderem wird darin etwa darauf hingewiesen, welche Inhalte verboten sind, oder darauf, dass beim Posten von Bildern und Videos eine Quellenangabe notwendig ist.
Die grundlegenden Verhaltensregeln für das Internet sind dieselben wie im Offline-Leben. Es gilt, höflich zu bleiben und selbst bei hitzigen Diskussionen einen kühlen Kopf zu bewahren. Dazu gehört, erst zu lesen und dann zu schreiben und nicht aggressiv oder untergriffig zu antworten. Da Userinnen und User ihre Gegenüber nicht direkt sehen und die Kommunikation etwa durch den Gebrauch von Pseudonymen und die Darstellung auf dem Computer oder einem anderen internetfähigen Endgerät verfälscht wird, fällt es schwerer, Ruhe zu bewahren und höflich zu bleiben, wie auch wissenschaftliche Studien belegen. Das Fehlen der direkten Reaktion des Gegenübers zum Beispiel führt zu einer Enthemmung der Nutzerinnen und Nutzer, sodass selbst geübte Userinnen und User bei Diskussionen im Internet leichter und schneller überreagieren. Es ist also wichtig, sich in Erinnerung zu rufen, dass es bei schriftlicher (Online-)Kommunikation leichter zu Missverständnissen kommen kann, um derlei unverhältnismäßige Erwiderungen zu vermeiden.

Nutzerinnen und Nutzer sollten bedenken, dass ihre Postings im Internet erhalten bleiben. In Foren, die moderiert werden, werden unflätige oder angriffige Postings teilweise erst gar nicht veröffentlicht oder bald gelöscht. Schlimmstenfalls können derartige Postings auch ein Ausschlussgrund sein oder zu einer Anzeige führen.

Gleichzeitig ist zu berücksichtigen, dass nicht alle Teilnehmerinnen und Teilnehmer der Netzkultur an einem konstruktiven Austausch interessiert sind. Sogenannte ***TROLLE*** versuchen, Internetdiskussionen durch destruktive oder provozierende Kommentare zu behindern. Sie sind nicht an sachlichen Gesprächen interessiert, sondern möchten andere Userinnen und User verärgern und deren Online-Unterhaltungen stören.

Netiquette:
(Kombination aus „net", Engl. für Netz, und „étiquette", Franz. für Verhaltensregeln.) Der angemessene und achtsame Umgang mit anderen Userinnen und Usern im Internet.

Siehe Kapitel:
Strafbare Postings
S. 68

(Internet-)Troll:
Person, die im Internet absichtlich Diskussionen anheizt und meist andere Userinnen und User provoziert.

E-Mails

Das Versenden und Empfangen von E-Mails war eine der ersten Anwendungen im Internet – und ist bis heute eine der wichtigsten. Die Kommunikation per E-Mail ist mittlerweile in fast jedem Beruf ein fixer Bestandteil der professionellen Kommunikation, aber zum Beispiel auch Behördenerledigungen werden per E-Mail abgewickelt. Prinzipiell gilt das Gleiche wie für Briefe: Alle E-Mails, die nicht ausschließlich privater Natur sind, sollten förmlich gehalten sein. Dazu gehören korrekte Rechtschreibung, Groß- und Kleinschreibung und die richtige Anrede der Empfängerin oder des Empfängers. Inhaltlich sollten sich Nutzerinnen und Nutzer auf das Wesentliche beschränken, da unnötig lange E-Mails auf den ersten Blick abschreckend wirken. Auf ***EMOTICONS*** (z. B. :-)), Abkürzungen (z. B. „IDK" für „I don't know"), ***MEMES*** oder spezielle Redewendungen aus der Netzkultur sollte ebenso verzichtet werden, diese bleiben besser der privaten Online-Kommunikation vorbehalten.

Emoticon:
(Kombination aus „emotion", Engl. für Gefühl, und „icon", Engl. für Zeichen.) Zeichenfolge, die Smileys nachbildet, um in schriftlicher (Online-)Kommunikation Gefühle und Stimmungen auszudrücken.

Mem bzw. Meme:
(„mimema", Altgr. für etwas Nachgemachtes.) Internetphänomen, meistens Bild-Text-Kombinationen, die von Userinnen und Usern eingesetzt werden, um bestimmte Stimmungen bzw. Gedanken zu transportieren oder etwas zu kommentieren.

Domain:
Das ist ein „Namensraum" im Internet, der eine weltweit im Internet einmalige und eindeutige Adresse darstellt.

Zusätzlich gilt eine neutrale Absenderadresse als angemessen, etabliert hat sich hierbei beispielsweise das Format vorname.nachname@mail-dienst.at. Besonders im Berufsleben wird es als unprofessionell erachtet, „private" E-Mail-Adressen eher legerer Natur zu verwenden (z. B. Susi23@mail-dienst.at). Auch der Hinweis auf die ***DOMAIN*** in der E-Mail-Adresse, also jener Teil, der nach dem @-Zeichen folgt, sollte möglichst neutral sein. Die Namen der großen E-Mail-Provider wie etwa GMX oder Gmail oder die Mail-Adresse des eigenen Internetproviders sind hierbei empfehlenswert. Eher unprofessionell wirken E-Mail-Adressen von anderen Quellen (z. B. toni@cabrioliebhaber.at), es sei denn, die Userin oder der User möchte dadurch etwas ganz Bestimmtes, im beruflichen Kontext Relevantes ausdrücken.

Viele E-Mail-Programme unterstützen eine HTML-Darstellung, ermöglichen also die Verwendung von verschiedenen Farben, Schriftarten oder Formatierungen. Ganz grundsätzlich sollten Nutzerinnen und Nutzer beim Versand von E-Mails bedenken, dass nicht alle Empfängerinnen und Empfänger E-Mail-Programme verwenden, die HTML-Nachrichten unterstützen; diese E-Mail-Programme können also HTML-Elemente nicht anzeigen, es wird somit lediglich der unformatierte Text übermittelt. Ein schön und aufwendig gestaltetes HTML-E-Mail kann unter Umständen bei der Empfängerin oder dem Empfänger als (nicht besonders ansehnlicher) Textsalat ankommen. Beispielsweise ist dies bei E-Mail-Diensten der Fall, die Verschlüsselungen anwenden. Hier werden HTML-Nachrichten in textbasierte Nachrichten

umgewandelt. Zusätzlich verbraucht eine ***HTML***-Nachricht mehr Datenvolumen, das heißt, die E-Mail-Datenpakete sind größer. Der Einsatz von HTML-Elementen sollte also auf spezielle Anlässe wie etwa Einladungen beschränkt werden.

Sollen Anhänge mitgeschickt werden, empfiehlt es sich, bei Textdokumenten das Dateiformat ***PDF*** zu verwenden. Dieses Dateiformat kann auf fast allen Geräten angezeigt werden und zeichnet sich dadurch aus, dass es den Inhalt originalgetreu wiedergibt. Bei Word-Dokumenten, die als Anhang verschickt werden, kann es nämlich durchaus vorkommen, dass die Formatierung beim Versand „verrutscht" und bei der Empfängerin oder dem Empfänger anders aussieht als bei der Absenderin oder dem Absender.

HTML bzw. Hypertext Markup Language:

Textbasierte Auszeichnungssprache zur Strukturierung von digitalen Inhalten wie Texten, Bildern und Hyperlinks in elektronischen Dokumenten.

PDF bzw. Portable Document Format:

Plattformunabhängiges Dateiformat, das sich dadurch auszeichnet, den Inhalt originalgetreu wiederzugeben.

Foren & Chats

Im Internet gibt es eine schier unendliche Anzahl von Foren und ***COMMUNITYS*** zu den verschiedensten Themen. Sie werden von Userinnen und Usern genutzt, um sich mit Gleichgesinnten auszutauschen, sich zu informieren oder auch nur, um sich auf kurzweilige Art die Zeit zu vertreiben.

(Online-)Community:
(Engl. für Gemeinschaft.) Gruppe im Internet, deren Mitglieder miteinander (mit Bezug zu einem bestimmten Thema) kommunizieren und interagieren.

Es gilt jedoch zu bedenken, dass Community nicht gleich Community ist. Im Forum einer seriösen Tageszeitung ist der Ton unter Umständen höflicher und das Niveau der Postings höher als zum Beispiel in einer Community, in der Sportergebnisse diskutiert werden. Zusätzlich gibt es einige Foren, in denen ein sehr rauer Wind herrscht und manchmal sogar eine spezielle Sprache verwendet wird, die auf Außenstehende im ersten Moment wie eine Fremdsprache wirken kann.

Chats und die beliebten Instant Messenger werden überwiegend für private Zwecke genutzt, zur Kommunikation mit Freundinnen und Freunden oder etwa der Familie. Hier ist kein förmlicher Umgangston notwendig; beispielsweise ist die Verwendung von Emoticons oder das Weglassen von Interpunktionszeichen in Ordnung.

Abkürzungen des Netzjargons

Im Internet und vor allem bei Online-Kommunikation werden häufig Abkürzungen für gängige Redewendungen verwendet. Im beruflichen Umfeld können Nutzerinnen und Nutzer beispielsweise auf die Kürzel ASAP („as soon as possible“, Engl. für „so schnell wie möglich“), FYI („for your information“, Engl. für „zu deiner/Ihrer Information“) oder IMHO („in my humble opinion“, Engl. für „meiner bescheidenen Meinung nach“) stoßen. Im privaten Online-Austausch wiederum kursieren sehr oft die Abkürzungen GIYF („Google is your friend“, Engl. für „Google ist dein Freund“), WTF („what the fuck?“, Engl. für „Was zur Hölle?“) und IDK („I don’t know“, Engl. für „Weiß ich nicht“). Auf Wikipedia gibt es eine Liste der gängigsten Abkürzungen aus dem Netzjargon.

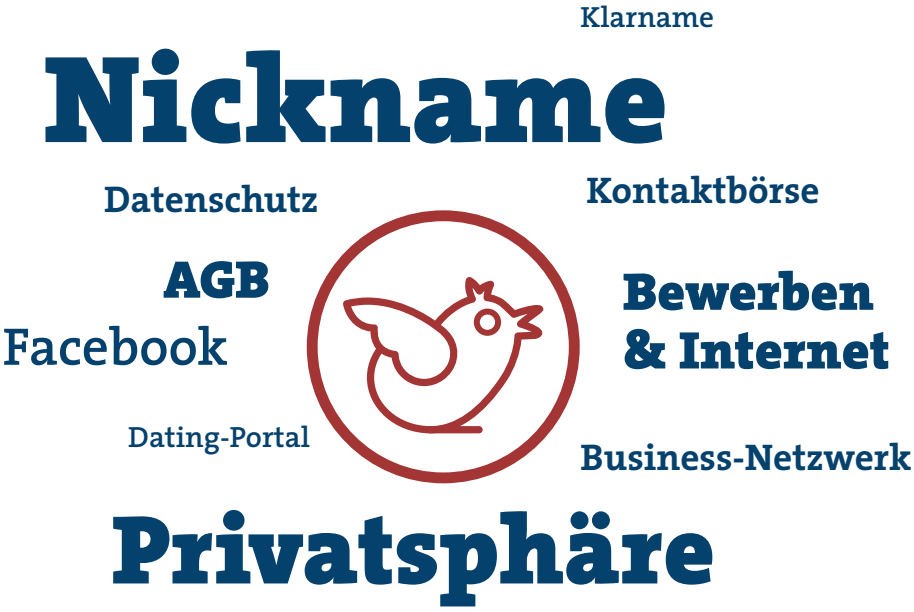
Liste der Abkürzungen:
goo.gl/zBCMU9

Meme

Ebenso häufig wie Abkürzungen kommen in gewissen Foren und Chats sogenannte Memes zum Einsatz. Das sind Bild-Text-Kombinationen, die von Userinnen und Usern eingesetzt werden, um satirisch einen bestimmten

Gedanken auf den Punkt zu bringen. Hierbei werden oftmals Bildausschnitte aus beliebten Sendungen oder Filmen verwendet, die Textkomponente basiert in vielen Fällen auf Zitaten von Filmfiguren oder Personen des öffentlichen Lebens. Die eingesetzten Zitate können von den Userinnen und Usern nach Belieben abgewandelt werden, ohne dass das Meme seinen Wiedererkennungswert verliert (z. B. „Brace yourself, winter/exams/new taxes etc. is/are coming“).

Solche Memes erlangen in der Populär- bzw. Netzkultur rasch Beliebtheit und werden in gewissen Kreisen flächendeckend eingesetzt.



Das größte und gleichzeitig bekannteste soziale Netzwerk ist mit über einer Milliarde Mitgliedern zweifelsohne Facebook. So viele Vorteile die verschiedenen Online-Communitys bieten – Vernetzung, Ablenkung, Informationen –, so viele problematische Aspekte kann es bei ihrer Nutzung geben. Die meisten davon betreffen den Bereich des Datenschutzes oder der Cyberkriminalität (z. B. Identitätsdiebstahl, Cybermobbing). Die gute Nachricht ist aber, dass die Plattformen immer mehr dem Wunsch und dem Bedürfnis der Nutzerinnen und Nutzer nach mehr Privatsphäre und Kontrolle über ihre eigenen Daten folgen.

Soziale Netzwerke & Dating-Plattformen

Soziale Netzwerke gibt es in allen Farben und Formen und alle funktionieren sie nach einem ähnlichen Prinzip: Bei der Registrierung wird ein – unterschiedlich umfangreiches – Profil erstellt, mit welchem das Netzwerk genutzt wird. Die wichtigsten Angaben sind ein selbst gewählter ***NICKNAME***, ein Foto und weitere persönliche Informationen: Für die Registrierung ist üblicherweise die Angabe des ***KLARNAMENS***, des Geburtsdatums, des Geschlechts und einer gültigen E-Mail-Adresse notwendig. Ist schließlich ein Profil erstellt, gibt es die Möglichkeit, sich auf unterschiedliche Arten mit anderen Userinnen und Usern zu vernetzen. Dies fällt von Netzwerk zu Netzwerk verschieden aus: Bei Facebook können Freundinnen und Freunde hinzugefügt werden („geaddet"), bei Instagram werden selbst geschossene Fotos mit verschiedenen Fotofiltern belegt und geteilt, bei Tumblr werden die Blogs von ausgewählten Mitgliedern verfolgt („gefollowet").

Nutzerinnen und Nutzer sollten sich aber bewusst sein, dass viele dieser Social-Media-Plattformen werbefinanziert sind. Die Nutzung der verschiedenen Netzwerke und anderer Dienste ist nur auf den ersten Blick kostenlos, gezahlt wird mit den eigenen Daten.

Die meisten sozialen Netzwerke können grob in zwei Kategorien unterteilt werden: die eher öffentlichen Netzwerke und die eher privaten Netzwerke. Während bei den Netzwerken der ersten Kategorie (Twitter, Instagram, Tumblr oder Vine) alle Inhalte mehr oder minder komplett öffentlich verbreitet werden, geht es bei Netzwerken der zweiten Kategorie (Snapchat, Messenger-Apps wie WhatsApp, Telegram oder Line) darum, Inhalte nur mit ausgewählten Mitgliedern (friends, followern etc.) zu teilen. Der große Unterschied liegt somit in der Öffentlichkeit des geposteten Inhalts und der Möglichkeit des Zugriffs durch Userinnen und User, die nicht registrierte Mitglieder dieses Online-Dienstes sind. Bei öffentlichen Netzwerken müssen sich die Nutzerinnen und Nutzer bewusst sein, dass die geposteten Inhalte grundsätzlich allen zugänglich sind, außer sie verschicken diese als Privatnachrichten. Facebook ist beispielsweise ein Hybrid-Dienst, der von privaten Nachrichten über komplett öffentliche Postings alles anbietet.

?

Klarname:

Auch Engl. „Realname", ist der tatsächliche Name einer Person, der auch in amtlichen Dokumenten geführt wird.

Nickname:

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

Datenschutz & Privatsphäre

Ob die Teilnahme an sozialen Netzwerken empfehlenswert ist oder nicht, müssen Userinnen und User für sich selbst entscheiden. Manche Menschen verweigern sich Online-Communitys, oftmals, weil sie ihre Daten nicht an die Unternehmen weitergeben wollen oder Angst haben, dass diese missbraucht werden. Auf der anderen Seite gibt es Menschen, die ihr ganzes Leben öffentlich führen: einen Blog über ihre Weltreise betreiben, Fotos von Partys teilen oder aktiv Content posten – und das alles unter ihrem echten Namen. Zwischen Verweigerung und Online-Exhibitionismus gibt es aber auch die Möglichkeit, soziale Netzwerke zu nutzen, ohne das komplette Leben offenzulegen. Viele Nutzerinnen und Nutzer machen von den Communitys Gebrauch, um sich mit anderen zu vernetzen und sich zu informieren, ohne selbst allzu viel preiszugeben. Gemeinhin werden Nutzerinnen und Nutzer, die überwiegend passiv – also nur lesend – teilnehmen, als ***„LURKER“*** bezeichnet.

Besonders die etablierten sozialen Netzwerke erkennen die Datenschutzbedürfnisse ihrer Userinnen und User an und bessern auch regelmäßig nach. Diesbezüglich werden verschiedene Möglichkeiten zum Schutz der Privatsphäre geboten, beispielsweise die Einschränkung des Zugriffs auf ein Profil. Bei vielen sozialen Netzwerken sind die Profile standardmäßig auf „öffentlich“ gestellt, sodass sie über Suchmaschinen gefunden werden können. So können selbst nicht registrierte Userinnen und User ein Profil (oder Teile davon) finden und einsehen. Prinzipiell ist es daher zu empfehlen, das eigene Profil auf „nicht öffentlich“ umzustellen. Es ist dann nur für jene Mitglieder sichtbar, die vorher als Kontakt bestätigt wurden.

Trotz aller Sicherheitsvorkehrungen sollten sich Userinnen und User immer des Risikos bewusst sein, dass sie ihre Daten einem Online-Dienst anvertrauen. Nicht alle Dienste sind so privat, wie sie auf den ersten Blick erscheinen. In der Vergangenheit kamen bei einigen Dienstanbietern immer wieder Sicherheitslücken zutage, die Angriffsfläche für Hackings und Datenklau boten. Ebenso sollten Nutzerinnen und Nutzer berücksichtigen, dass auch bei Postings mit illegalen Inhalten rechtliche Schritte folgen können. Das Internet ist kein rechtsfreier Raum und Tatbestände wie Verhetzung, Rufschädigung, Erpressung oder Stalking sind auch online rechtswidrig. Gerade in jüngster Zeit häufen sich Verurteilungen in Zusammenhang mit rechtswidrigen Postings in sozialen Netzwerken.

Lurker:
(„to lurk“, Engl. lauern, schleichen.) Userinnen und User von sozialen Netzwerken, die nur passiv am Online-Geschehen teilnehmen und kaum aktiv Content produzieren.

Facebook:
Einstellungen > Privatsphäre

Twitter:
Sicherheit und Datenschutz > Privatsphäre

Ask.fm:
Datenschutz

Instagram:
Profil > Privatsphärenschutz

Hasspostings:
Postings mit Inhalten, die unter strafrechtliche Tatbestände wie Verhetzung, Rufschädigung, Ehrenbeleidigung oder üble Nachrede fallen.

Kapitel „Cybercrime“:
S. 68

Facebook

Facebook bietet seinen Userinnen und Usern verschiedene Vorkehrungen, um genau kontrollieren zu können, wer welche Daten einsehen und mitlesen kann. Eine neue Funktion, die Nutzerinnen und Nutzern dabei helfen soll, ist der „blaue Sicherheitsdinosaurier". Mit diesem Sicherheitscheck können die wichtigsten Einstellungen in drei kurzen Schritten vorgenommen werden.

Ganz grundlegend können Mitglieder selbst entscheiden, welche ihrer persönlichen Daten für andere sichtbar sind (Geburtsdatum, Kontaktinformation etc.), ebenso ihre Fotos und Postings. Diese sollten unbedingt auf den Freundeskreis eingeschränkt werden.

Zusätzlich können die Online-Freundinnen und -Freunde in Untergruppen sortiert werden; hier können Nutzerinnen und Nutzer für jeden angelegten Personenkreis („Liste") eigene Regeln erstellen und so zum Beispiel festlegen, dass die Arbeitskolleginnen und -kollegen nicht die Urlaubsfotos sehen, die Familienmitglieder aber schon. Auch gibt es mit der Profilvorschau die Möglichkeit zu überprüfen, wie das eigene Profil aus der Sicht eines anderen Mitglieds aussieht.

Facebook bietet viele verschiedene Anwendungen an (Spiele, Quiz etc.). Diese werden von Drittanbietern betrieben. Um diese Anwendungen nutzen zu können, wird der Zugriff auf die Nutzerdaten verlangt. Teilweise können Drittanbieter auch über Freundinnen und Freunde an die eigenen Daten gelangen. Es empfiehlt sich dringend, diese Option einzuschränken und auch bei den eigenen Anwendungen regelmäßig „auszumisten". Zuletzt sollten Nutzerinnen und Nutzer von Facebook die Markierungsfunktion deaktivieren, sodass sie nicht mehr in Fotos oder Beiträgen markiert – also verlinkt – werden können („getagget").
Zu guter Letzt ein Tipp, der nicht die Sicherheit, aber vielleicht die Nerven schützt: das Blockieren von Spielen und Anwendungen. Keine lästigen Spieleeinladungen von anderen Facebook-Userinnen und -Usern mehr!

Die wichtigsten fünf Tipps für mehr Privatsphäre auf Facebook:

- → ***Sichtbarkeit:*** *Postings und Fotos sollten nicht für die Öffentlichkeit freigeschaltet werden; Gruppen für verschiedene Inhalte verwenden (z. B. Familie, Arbeit etc.).*
- → ***Persönliche Informationen:*** *Möglichst wenige persönliche Informationen*

YouTube:
beim eigenen Kanal das hochgeladene Video auswählen, Upload bearbeiten > Datenschutzeinstellungen

Xing:
Einstellungen > Privatsphäre

Vine:
Profil bearbeiten > Einstellungen > Dein Content

Linkedin:
Konto & Einstellungen > Datenschutz & Einstellungen > Prüfen

Sicherheits-Check auf Facebook:
Privatsphäre-Verknüpfungen > Überprüfung der Privatsphäre

Facebook: Einstellungen > Chronik und Markierungen > Anzeigen aus der Sicht von > Person, aus deren Sicht das eigene Profil angezeigt werden soll, auswählen.

preisgeben, Adresse- und Kontaktdaten sollten tunlichst nicht veröffentlicht werden; zumindest eine leichte Abwandlung des eigenen Klarnamens sollte verwendet werden (z. B. Kathi Müller statt Katharina Müller).

- → ***Anwendungen blockieren:*** *Drittanbieter verlangen Zugriff auf persönliche Daten und können diese auch über die eigenen Freundinnen und Freunde sammeln – diese Möglichkeit sollte unbedingt deaktiviert werden.*
- → ***Suchmaschinen:*** *Das Profil auf „privat" schalten, sodass es nicht in den Ergebnissen von Suchmaschinen auftaucht.*
- → ***Profilvorschau nutzen:*** *Das Profil aus der Sicht von befreundeten Nutzerinnen und Nutzern ansehen, um sicherzugehen, dass nur die gewünschten Informationen einsehbar sind.*

Facebook: Einstellungen > Apps > Von anderen Nutzern verwendete Apps > alle Optionen abwählen

Facebook: Einstellungen > Chronik und Markierungen

Anwendungen blockieren: Einstellungen > Blockieren > Anwendungen blockieren

Kontaktbörsen & Dating-Portale

„Drum prüfe, wer sich ewig bindet": Online-Dating-Plattformen sind die Kontaktanzeigen der digitalen Welt. Hatten sie früher ein negatives Image und waren lediglich ein Nischenprodukt, so sind sie heute in der breiten Öffentlichkeit angelangt und werden stark genutzt. Online-Dating scheint in unserer vernetzten Welt immer mehr die Partnersuche der Zukunft zu sein. Mittlerweile sind Dating-Plattformen ein umsatzstarkes Geschäft, so verzeichnete beispielsweise das größte Portal im deutschsprachigen Raum, Parship, im Jahr 2013 über 50 Mio. Euro Umsatz.

Weitere Tipps für Sicherheitseinstellungen auf Facebook und in anderen Netzwerken:

www.saferinternet.at/privatsphaere-leitfaeden

Besonders mobile Dating-Apps boomen derzeit. Die bekanntesten Beispiele sind Tinder und Lovoo. Diese basieren auf dem Prinzip der standortbezogenen Dienste, die unter Zuhilfenahme von positionsabhängigen Daten arbeiten ***(„GEOSOCIAL NETWORKING")*** – also beispielsweise Singles in geografischer Nähe anzeigen.

Geosocial Networking:

Soziale Netzwerke, die mit standortbezogenen Daten arbeiten.

Im (Online-)Geschäft mit der Liebe gibt es spezialisierte Plattformen für besondere Zielgruppen. So können zum Beispiel Singles in geografischer Nähe, für Seitensprünge oder speziell Singles mit hohem Bildungshintergrund gesucht werden. Auch Plattformen, die sich an Minderjährige richten, gibt es mittlerweile nicht wenige.
Beim Online-Dating gilt wie im echten Leben: lieber Vorsicht als Nachsicht. Denn viele Dating-Plattformen locken mit Gratismitgliedschaften (***„FREEMIUM"***), jedoch sind nur sehr wenige Funktionen bei diesen Gratisprofilen inkludiert (beispielsweise ist die Kontaktaufnahme mit anderen Mitgliedern blockiert). Dadurch wollen die Plattformen Userinnen und User zu den vollen und oftmals kostenpflichtigen Mitgliedschaften drängen. Nicht

Teenager & Dating-Plattformen:

Siehe Kapitel „Kinder und Medien", S. 91

selten finden sich in den Geschäftsbedingungen solcher Plattformen lange Laufzeiten für die Mitgliedschaft, kostenpflichtige Abos oder Klauseln zur automatischen Verlängerung. Daher sollten unbedingt die AGB, aber speziell die E-Mails, die im Zuge der Registrierung von den Plattformen versandt werden, aufmerksam gelesen werden. Oftmals sind in diesen Hinweise auf Laufzeiten oder Kosten enthalten.

Immer wieder werden die undurchsichtigen Vertragsbedingungen bei Online-Partnerbörsen oder deren zweifelhafte Praxis im Hinblick auf Widerruf und Kündigung von Verbraucher- und Konsumentenschutz kritisiert. So ist bei manchen Plattformen eine Kündigung auch dann nicht möglich, wenn die Userinnen und User bereits die „große Liebe" über die Plattform gefunden haben.

Manche Plattformen arbeiten auch mit „Köderkontakten". Hier werden neue Mitglieder von fiktiven oder eigens für solche Dienste engagierten Mitgliedern kontaktiert (sogenannten ***„DATE-BAITS"***), die sie in ein Abo locken oder zu einer Verlängerung der Mitgliedschaft motivieren sollen.

Versteckte AGB

Einige wenige Social-Media- und Dating-Plattformen machen sich durch extremere Werbemaßnahmen unbeliebt: Userinnen und User erhalten E-Mail-Einladungen zum Plattform-Beitritt von ihren eigenen Bekannten oder bekommen Benachrichtigungen, dass ihnen eben jene Bekannte über diese Plattform Nachrichten geschickt hätten. Geübte Nutzerinnen und Nutzer erkennen diese E-Mails auf den ersten Blick als Spam und Ködernachricht, doch nicht wenige fallen auf diesen Trick herein und melden sich bei der Plattform an, um die angeblich dort abrufbaren Nachrichten lesen zu können – und hier beginnt der Teufelskreis.

Denn in den AGB zum Datenschutz schreibt eine dieser Plattformen, dass ein Tool zum Import der privaten Kontakte angeboten wird. Dieses Tool ist fixer Bestandteil des Anmeldeprozederes, allerdings nicht sehr benutzerfreundlich, sodass viele unbeabsichtigt dem Import ihrer Adressbücher zustimmen. Daraufhin beginnt die Plattform, an alle Kontakte aus den Adressbüchern E-Mails mit Einladungen und Erinnerungen zu schicken. Die AGB enthalten zusätzlich eine Klausel, in der festgehalten ist, dass das Mitglied durch den – wenn auch unbeabsichtigten – Import der Kontakte zustimmt, dass das Netzwerk diesen Kontakten Einladungen und anderes zuschicken darf.

?

Freemium:

(Kombination aus „free", Engl. gratis, und „premium", Engl. Belohnung.) Geschäftsmodell, bei dem Basisprodukte oder -funktionen kostenlos sind, die Vollversion bzw. deren Freischaltung ist jedoch kostenpflichtig.

?

Date-Baits:

(Engl. Date-Köder.) Von Dating-Plattformen engagierte Personen, die Mitglieder in eine (kostenpflichtige) Mitgliedschaft locken sollen.

Ausstieg & digitale Leichen

www.justdelete.me:
Informiert über die Möglichkeiten, Konten bei verschiedenen Online-Diensten zu löschen.

Irgendwann kommt der Punkt, an dem Userinnen und User die sozialen Netzwerke oder Online-Communitys verlassen möchten oder diese einfach nicht mehr nutzen. Ist das der Fall, sollte unbedingt der Account deaktiviert und gelöscht werden. Somit werden nicht nur unnötige „digitale Leichen" verhindert, sondern auch die Daten beim jeweiligen Dienst gelöscht.
Ein angelegtes Profil oder Konto zu löschen, ist von Plattform zu Plattform unterschiedlich einfach oder kompliziert. Manche der Online-Dienste stellen Kontaktformulare bereit, andere haben „Lösch-Buttons". Wiederum andere machen es registrierten Userinnen und Usern möglichst schwer, indem sie die Kontolöschfunktionen gut verstecken und auf den ersten Blick nicht auffindbar machen. Die Absicht hierbei ist, die Userinnen und User zum Aufgeben zu bewegen. Schließlich werben die Online-Dienste mit ihren hohen Mitgliederzahlen nicht nur neue Mitglieder an, sondern können dadurch auch die Werbeeinnahmen erhöhen. Üblicherweise können die Informationen über die Löschung aber in den FAQ oder in den AGB gefunden werden. Ist dies nicht der Fall, kann eine kurze Internetsuche nach dem Namen des Online-Dienstes und den Begriffen „Konto" und „löschen" gut weiterhelfen. Die Wahrscheinlichkeit ist groß, dass viele andere Mitglieder diese Frage bereits gestellt und beantwortet bekommen haben. Ansonsten ist die Webseite justdelete.me eine gute Anlaufstelle. Hier werden Informationen über die verschiedenen Löschabläufe der beliebtesten Online-Dienste gesammelt.

Manche Dienste haben keine standardisierten Verfahren und auch keine Informationen zur Kontolöschung, führen sie aber auf Anfrage beim Kundensupport durch (z. B. Ask.fm). Registrierungen bei Diensten wie Picasa oder YouTube, die über das zentrale Google-Konto laufen, können oftmals nicht einzeln gelöscht werden, da hierfür das Hauptkonto von Google gelöscht werden müsste. Bei Facebook ist der Löschvorgang etwas komplizierter. In einem ersten Schritt muss der Account unter den Kontoeinstellungen deaktiviert werden. Soll das Konto dauerhaft gelöscht werden, muss im Menüpunkt „Hilfe" nach „Wie kann ich mein Konto dauerhaft löschen?" gesucht werden. In der Erklärung findet sich ein Link, der zum Netzwerk-Ausgang führt. Allerdings wird das Konto vorerst für 14 Tage stillgelegt, sodass die Userinnen und User wiederkehren können. Erst nach dieser zweiwöchigen Frist wird das Konto dauerhaft gelöscht. Der Löschvorgang der Daten dauert anschließend noch 90 Tage.

Facebook-Konto löschen:
Account deaktivieren > unter „Hilfe" nach „Konto löschen" suchen > Link folgen

Reißen alle Stricke, gibt es noch die Möglichkeit, die eigenen Daten manuell zu löschen und die Benutzerdaten dahingehend zu ändern, dass die eigene Identität nicht mehr nachvollziehbar ist. So können nicht löschbare Daten verschleiert und unkenntlich gemacht werden.

Berufswelt und soziale Netzwerke

Das Privat- und das Berufsleben verschmelzen immer mehr, die Übergänge sind oftmals fließend. Auch nach Ende des regulären Arbeitstages beantworten Berufstätige ihre E-Mails, genauso wie während der Arbeitszeit das eine oder andere Mal etwas auf Facebook gepostet oder ein Flug für den nächsten Urlaub gebucht wird. Umso wichtiger ist es aber, den beruflichen und den privaten Internetauftritt voneinander zu trennen. Unprofessionelles Online-Verhalten kann für die berufliche Zukunft ein nicht geringes Hindernis sein, schlimmstenfalls kann es einen den zukünftigen genauso wie den aktuellen Job kosten. In diesem Zusammenhang sollten sich Arbeitnehmerinnen und -nehmer über die Richtlinien bezüglich der Verwendung des Internets am Arbeitsplatz in ihrem Unternehmen informieren. Diese Richtlinien legen genau fest, was im Unternehmen erlaubt und was ein No-Go ist.
Viele Unternehmen haben außerdem auch ***SOCIAL-MEDIA-RICHTLINIEN***. Je nach Branche und Unternehmenskultur ist es beispielsweise angebracht oder unangebracht, mit der Chefin auf Facebook befreundet zu sein oder während der Arbeitszeit den Kollegen mit der Frage anzutwittern, ob er was vom Bäcker haben will. Besonders das „Ventilieren" im Internet, also das Schimpfen über Chefs oder die werte Kollegenschaft, kann gefährlich werden und im schlimmsten Fall zu einer Verwarnung oder auch zur Kündigung führen. Arbeitnehmerinnen und Arbeitnehmer sollten sich besonders mit negativen Äußerungen oder dem Preisgeben von – durch das Geschäftsgeheimnis geschützten – internen Abläufen zurückhalten. Für Internetnutzerinnen und -nutzer in Österreich gilt österreichisches Recht, ein strafrechtlicher Tatbestand wie Ehrenbeleidigung oder ein zivilrechtlicher Tatbestand wie Kreditschädigung kann auch durch Postings in Social Media erfüllt werden.

Social-Media-Richtlinien:

Von Unternehmen erstellte Richtlinien für die Angestellten, die das Verhalten in und die Nutzung von sozialen Netzwerken während der Arbeitszeit festlegen.

Strafbare Postings:

Siehe Kapitel „Cybercrime", S.65

Bewerben & Internet

ISPA Studie „Mein Ruf im Netz“:
www.ispa.at/studien

In der ISPA Studie „Mein Ruf im Netz – Auswirkungen auf die berufliche Zukunft“ aus dem Jahr 2014 gaben die knapp 300 befragten Personalverantwortlichen an, dass sie in 47 Prozent der Fälle das Internet im Verlauf eines Bewerbungsverfahrens zur Recherche verwenden. Besonders oft kommt das in der IT-, Kommunikations- und der Finanzbranche vor. Zusätzlich gaben 81 Prozent der befragten Personalverantwortlichen an, dass die Online-Präsenz von Bewerberinnen und Bewerbern in Zukunft noch an Bedeutung gewinnen wird. In diesem Sinne ist es wichtig, auf den eigenen Online-Auftritt zu achten und das Internet gezielt als Jobmotor zu nutzen.

Business-Netzwerke:
Dienen der beruflichen Vernetzung und der Präsentation der eigenen Person als Fachkraft; funktionieren wie soziale Netzwerke.

www.xing.at
www.linkedin.com

Eine aktuelle und gepflegte Webpräsenz – ob eine eigene Webseite oder „nur“ ein Profil in ***BUSINESS-NETZWERKEN*** – kann gezielt als Unterstützung für die Bewerbung und die Repräsentation nach außen gesehen werden. Jedoch sollten die Daten regelmäßig aktualisiert werden, da ein vernachlässigter Webauftritt keinen professionellen Eindruck hinterlässt. Profile in Business-Netzwerken bieten die Möglichkeit, sich geschäftlich zu vernetzen, nach interessanten Stellen Ausschau zu halten oder selbst als potenzielle Arbeitskraft gefunden zu werden.

Alert-Dienst:
Der wohl bekannteste Alert-Dienst ist der Google-Alert. Ein Alert-Dienst ist ein Informationsdienst, der per E-Mail-Benachrichtigung oder RSS informiert, wenn neue Ergebnisse zu einem vorher festgelegten Schlagwort, Namen oder sonstigen Abfragekriterien auftauchen.

Es empfiehlt sich außerdem, regelmäßig eine Suche nach sich selbst im Internet durchzuführen. Somit können rechtzeitig Schritte eingeleitet werden, falls etwas Nachteiliges im Internet zu finden ist, beispielsweise (unvorteilhafte) Fotos der eigenen Person, die ohne Zustimmung veröffentlicht wurden. Eine weitere Möglichkeit ist, einen ***ALERT-DIENST*** für den eigenen Namen einzurichten. Er informiert, wenn der eigene Name im Internet auftaucht. Somit können böse Überraschungen – beispielsweise beim Bewerbungsgespräch – vermieden werden.

Bei einem Bewerbungsgespräch sollte heutzutage damit gerechnet werden, dass sich die Personalverantwortlichen unter Umständen im Internet schlau gemacht haben und Fragen zum Online-Auftritt stellen, vor allem, wenn die Profile in Online-Netzwerken öffentlich sind oder der eigene Klarname statt eines Pseudonyms oder Nicknames verwendet wird. Die Personalverantwortlichen wollen sich oftmals nur einen allgemeinen Eindruck von den Bewerberinnen und Bewerbern, ihrer Persönlichkeit, ihrem Internetverhalten oder auch der Internetkompetenz verschaffen.

Das berühmte „Partyfoto“ kann potenzielle Arbeitgeber abschrecken und Postings über den ehemaligen „dummen Chef“ zeigen nicht nur unprofessionelles Verhalten, sondern auch fehlendes Bewusstsein für den eigenen Online-Auftritt – und beide können im Internet weite Kreise ziehen. Die geringste Konsequenz ist die eines negativen Ersteindruckes. Umso wichtiger ist es, über das eigene Auftreten im Internet informiert zu sein und es aktiv zu gestalten!

Tipps für einen professionellen Internetauftritt:

- → ***Suche nach sich selbst:*** *Mittels Suchmaschinen regelmäßig nach sich selbst zu suchen hilft, den Überblick über den eigenen Online-Auftritt zu behalten, und gibt die Möglichkeit, sofort entsprechende Maßnahmen zu setzen, wenn „überraschende“ Einträge auftauchen.*
- → ***Alert-Dienst:*** *Online-Dienst, der Benachrichtigungen schickt, wenn der zuvor eingestellte Suchbegriff (z. B. der eigene Name) im Internet auftaucht.*
- → ***Pseudonyme:*** *Bei sozialen Netzwerken, die überwiegend privat genutzt werden, empfiehlt es sich nicht, den eigenen Klarnamen zu verwenden, sondern ein Pseudonym oder einen Nickname.*
- → ***Privatsphäre-Einstellungen:*** *Möchten Bewerberinnen und Bewerber verhindern, dass ihre privaten Fotos oder Postings von potenziellen Chefs gefunden werden, sollten sie unbedingt ihre Profile und Fotos auf „privat“ schalten.*
- → ***Business-Netzwerke:*** *Ein Profil in einem Business-Netzwerk ist die wichtigste Plattform zur Präsentation der eigenen Person als qualifizierter Fachkraft, zusätzlich gibt es Möglichkeiten, Networking zu betreiben und sich mit anderen auf professioneller Ebene zu vernetzen.*

Achtung:

Es gibt vereinzelte Erfahrungsberichte von Bewerberinnen und Bewerbern, die beim Bewerbungsgespräch gezielt nach ihrem Auftritt in sozialen Netzwerken befragt wurden, teilweise sollten sie sogar den Nutzernamen preisgeben, unter dem sie beispielsweise auf Facebook zu finden sind. Derartige Praktiken sind fragwürdig. In einem extremen Fall wurden sogar die Zugangsdaten zu den Social-Media-Konten verlangt, damit diese während des Bewerbungsgesprächs live „überprüft“ werden konnten. Solche Fragen sind unzulässig, da die Informationen dem privaten Bereich der Bewerberinnen und Bewerber angehören und zudem nicht mit der Arbeitsstelle in direktem Zusammenhang stehen.

Domain

Recht am eigenen Bild

Impressum

fremde Inhalte

Disclaimer

Weblog

Urheberrecht

Offenlegungspflicht

Vlog

Creative Commons

Eine eigene Webseite, ein Blog oder ein Vlog bieten eine einfache Möglichkeit, sich selbst, die eigene Meinung oder die eigenen Interessen im Internet zu präsentieren. So gibt es mittlerweile anscheinend zu fast jedem Thema Webseiten und Blogs, die zur professionellen Meinungsbildung beitragen, über Trends informieren, Detailinformationen zu Spezialthemen oder auch nur Kurzweiliges bieten.

Webseite & Blog

Domains

Eine Domain ist ein einmaliger und eindeutiger Name, der hierarchisch unter einer Top-Level-Domain (TLD) angesiedelt ist. Eine TLD wird unterteilt in allgemeine gTLDs wie .com oder .org und in Länder-TLDs wie .at oder .de. Vereinfacht gesagt ist eine Domain also eine Internetadresse. In Österreich ist die Registrierungsstelle nic.at für die Top-Level-Domain .at zuständig. Eine Domain kann auch bei einem Internet ***PROVIDER*** angemeldet werden, die meisten Provider haben auch eine Abfragemöglichkeit, mit der festgestellt werden kann, ob der gewünschte Domainname noch frei ist. Auch, ob eine .at-Domain noch frei ist, kann bei nic.at abgefragt werden.

Achtung: Die absichtliche Registrierung von Domainnamen mit dem Vorsatz, diese später gewinnbringend an Dritte, die ein berechtigtes Interesse an dieser Domain haben, zu verkaufen, wird Domaingrabbing genannt. Domaingrabbing ist nach der Rechtsprechung des OGH eine unlautere Handlung, in einem solchen Fall können Unterlassungs- und Schadenersatzklagen drohen. Ein Beispiel für ***DOMAINGRABBING*** wäre es, wenn die Domainregistrierung vorgenommen wird, um die Konkurrenz in ihrer Tätigkeit zu behindern.

Blogs

Mittlerweile gibt es zahlreiche Online-Dienste, die Platz für private oder auch berufliche ***BLOGS*** und eigene Webseiten zur Verfügung stellen („Blogging-Dienste"). Hierbei können Nutzerinnen und Nutzer ein Konto oder Profil anlegen und bekommen, basierend auf ihrem Nutzernamen, eine Subdomain zugewiesen; dort können sie eigene Inhalte uploaden und posten. Essenzieller Bestandteil beim Blogging-Dienst Tumblr ist beispielsweise die Vernetzung mit anderen Userinnen und Usern; über die Reblog-Funktion können sehr leicht die Inhalte anderer auf dem eigenen Blog geteilt werden. Ebenso können andere Blogs gefollowet werden, sodass deren neueste Beiträge auf dem eigenen Dashboard aufscheinen.

Provider:
Unternehmen, die den Zugang zum Internet gewährleisten.

Domaingrabbing:
Missbräuchliche Registrierung eines oder mehrerer Domainnamen.

Blog bzw. Weblog:
(Kombination aus Engl. „web" und „log" für Logbuch.), ist ein auf einer Webseite geführtes, periodisches und meist öffentliches Journal zu einem bestimmten Thema.

Vlog:
(Kombination aus „Video“ und „Blog“.) Blog, dessen Einträge aus Videos bestehen.

Subdomain:
Eine Domain, die in der Hierarchie unter einer anderen liegt; meistens sind damit Domains der dritten oder vierten Ebene gemeint (die Top-Level-Domain ist .at, die Second-Level-Domain ist beispiel.at und eine Subdomain davon wäre irgendein.beispiel.at).

Reblog bzw. Reblogging:
Das Posten von fremden Inhalten, genauer gesagt, das Posten von bereits veröffentlichten Inhalten anderer Nutzerinnen und Nutzer auf dem eigenen Blog.

Dashboard:
(Engl. für Armaturenbrett.) Es ist je nach Onlinedienst unterschiedlich ausgestaltet, meistens jedoch die persönliche Start- oder Admin-Seite, auf der Information zusammengetragen wird.

Blogging-Dienste:
www.tumblr.com
www.wordpress.com
www.blogger.com

Eine neue Entwicklung des Blogs ist der ***VLOG***. Hierbei werden die einzelnen Beiträge in Form von Videos veröffentlicht. Speziell die Plattform YouTube wird dafür genutzt. Auch hier können Nutzerinnen und Nutzer eigenständig auf ihrem Kanal Inhalte hochladen und posten. Doch wie bei jeder Form der Veröffentlichung im Internet gilt es, das Urheberrecht zu berücksichtigen. Das Teilen oder Veröffentlichen von urheberrechtlich geschütztem Material ist auch im Internet verboten – beispielsweise, dass ohne Nutzungserlaubnis ein Lied als Hintergrundmusik für eine Webseite verwendet wird –, da es das geistige Eigentum anderer verletzt.

Impressum

Auch bei Webseiten und anderen Formen der selbst erstellten Internetpräsenz muss nachvollziehbar sein, wer für die dargestellten Inhalte verantwortlich ist. Das dient einerseits der Transparenz und ermöglicht andererseits Userinnen und Usern herauszufinden, wer die Webseite betreibt und für die Berichterstattung zuständig ist. Aus diesem Grund sieht das österreichische Mediengesetz Informationsverpflichtungen vor, die je nach Art der Webseite variieren.

Vielfach wird umgangssprachlich für jegliche Informationen über die Inhaberin oder den Inhaber einer Webseite der Begriff „Impressum“ verwendet. Das ist allerdings kein allgemein gültiger Begriff und ist nicht (immer) korrekt. Im schlimmsten Fall kann das zu rechtlichen Problemen führen. Prinzipiell kann die Informationspflicht in drei Kategorien eingeteilt werden: Offenlegungspflicht (§ 25 MedienG), Impressumspflicht (§ 24 MedienG) und Informationspflicht für kommerzielle Anbieter (§ 3 ECG).

Die Offenlegungspflicht

Die Offenlegungspflicht nach §25 MedienG unterscheidet, vereinfacht ausgedrückt, zwischen „kleinen Webseiten“ und „großen Webseiten“.

Kleine Webseiten

Kleine Webseiten, die zur Darstellung des persönlichen Lebensbereiches dienen, oder einfache Firmenwebseiten, die nicht die öffentliche Meinungsbildung beeinflussen, müssen lediglich diese Informationen bereitstellen:

- → *Name oder Firmenname,*
- → *gegebenenfalls Unternehmensgegenstand,*
- → *Wohnort oder Sitz der Niederlassung (nicht die komplette Adresse).*

Ob eine Webseite „geeignet ist, die öffentliche Meinungsbildung zu beeinflussen“, muss jeweils im Einzelfall bestimmt werden. Beispiele für Webseiten, die nicht geeignet sind, die öffentliche Meinungsbildung zu beeinflussen, sind etwa Unternehmenswebseiten, die bloß das Unternehmen und seine Produkte oder Dienstleistungen vorstellen. Ein weiteres Beispiel wären Vereinswebseiten, die den Verein und seine Aktivitäten präsentieren. Wird bei der Darstellung der Ziele auf gesellschafts- oder kulturpolitische Themen Bezug genommen, liegt keine privilegierte „kleine“ Webseite mehr vor. Ein Beispiel hierfür wäre es, wenn auf der Webseite eines Gärtnereiunternehmens im zugehörigen Blog auch umweltpolitische Themen diskutiert werden, sodass diese Webseite geeignet ist, die öffentliche Meinungsbildung zu beeinflussen.

Große Webseiten

Große Webseiten, also Webseiten, die der Beeinflussung der öffentlichen Meinung dienen, beispielsweise Newsletter oder politische Blogs, müssen diese Informationen bereitstellen:

- → *Name oder Firmenname,*
- → *Unternehmensgegenstand,*
- → *Wohnort oder Sitz der Niederlassung (nicht die komplette Adresse),*
- → *Geschäftsführung,*
- → *Beteiligungsverhältnisse,*
- → *Mitglieder des Vorstandes und Aufsichtsrates und die Gesellschafterinnen oder Gesellschafter,*
- → *grundlegende Richtung des Mediums.*

Entsprechend der Offenlegungspflicht für Webseiten muss nicht die vollständige Adresse angegeben werden. Die Angabe des Wohnortes reicht aus, die Angabe von Straße und Hausnummer ist nicht notwendig.

Sind sich Inhaberinnen und Inhaber von Webseiten nicht sicher, in welche der Kategorien ihre Webseite fällt, ist es zu empfehlen, die strengere Offenlegungspflicht für große Webseiten zu erfüllen.

Impressumspflicht

Die Impressumspflicht wird nicht auf Webseiten angewendet, sie gilt für wiederkehrende elektronische Medien (§ 24 MedienG). Das ist nach der Definition des Mediengesetzes ein Medium, das auf elektronischem Wege wenigstens viermal im Kalenderjahr in vergleichbarer Gestalt verbreitet wird (z. B. ein Newsletter).

Solche Medien müssen folgende Informationen enthalten:

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

Informationspflicht für kommerzielle Anbieter

Handelt es sich bei einer Webseite im weitesten Sinn um einen kommerziellen Dienst, muss laut dem ***E-COMMERCE-GESETZ*** (ECG) die Dienstanbieterin oder der -anbieter folgende Angaben leicht oder unmittelbar zugänglich machen:

§ 5 E-Commerce-Gesetz:
Gilt für Webseiten mit kommerziellem Zweck.

- → *den Namen oder Firmennamen,*
- → *die geografische Anschrift der Niederlassung,*
- → *Angaben, mithilfe derer die Nutzerinnen und Nutzer mit dem Diensteanbieter rasch und unmittelbar in Verbindung treten können, einschließlich der E-Mail-Adresse,*
- → *sofern vorhanden, die Firmenbuchnummer und das Firmenbuchgericht,*
- → *soweit die Tätigkeit einer behördlichen Aufsicht unterliegt, die für den Diensteanbieter zuständige Aufsichtsbehörde,*
- → *bei einem Diensteanbieter, der gewerbe- oder berufsrechtlichen Vorschriften unterliegt, die Kammer, den Berufsverband oder eine ähnliche Einrichtung, der er angehört, die Berufsbezeichnung und den Mitgliedstaat, in dem diese verliehen worden ist, sowie einen Hinweis auf die anwendbaren gewerbe- oder berufsrechtlichen Vorschriften und den Zugang zu diesen,*
- → *sofern vorhanden, die Umsatzsteuer-Identifikationsnummer.*

Verletzung der Offenlegungspflicht

Verletzungen der Offenlegungspflicht stellen eine Verwaltungsübertretung dar und können Geldstrafen von bis zu 20.000 Euro nach sich ziehen. Ein Verstoß gegen die Impressumspflicht kann bei der zuständigen Bezirksverwaltungsbehörde angezeigt werden.

Wird die Informationspflicht bei kommerziellen Diensten verletzt, kann vonseiten der Mitbewerberinnen und -bewerber sogar eine zivilrechtliche Unterlassungsklage nach dem Gesetz gegen unlauteren Wettbewerb (UWG) drohen.

Geistiges Eigentum und Urheberrecht

Egal, ob Userinnen und User eine eigene Webseite betreiben, oder „nur" eine Subdomain bei einem Blogging-Dienst nutzen – auch hier ist das Urheberrecht zu beachten.
Das Urheberrecht entsteht automatisch bei der Werkerschaffung. Daher sind Fotos, Videos und Grafiken urheberrechtlich geschützt und dürfen nur mit Zustimmung der ***URHEBERIN*** oder des ***URHEBERS*** verwendet, also veröffentlicht werden. Werden Werke ohne Zustimmung der ***RECHTEINHABERIN*** oder des ***RECHTEINHABERS*** verwendet, ist das eine Urheberrechtsverletzung; das kann zu einer Unterlassungs- und Schadenersatzklage führen. Es bestehen die Möglichkeiten, die Veröffentlichungsrechte zu erwerben oder auf Werke, die unter einer CC-Lizenz stehen, zurückzugreifen.

Doch auch bei selbst geschossenen Fotos oder Filmen, in denen andere Personen zu sehen sind, muss vor Veröffentlichung deren Einverständnis eingeholt werden (***„RECHT AM EIGENEN BILD"*** nach § 78 UrhG). Aufnahmen von Personen an öffentlichen Plätzen sind üblicherweise unbedenklich. Wenn jedoch die Situation für die Abgebildeten nachteilig ist oder diese bloßstellt (z. B. Oben-ohne-Foto am Strand), darf die Abbildung nicht veröffentlicht werden. Geschieht dies dennoch, haben die Abgebildeten das Recht auf Löschung und Entfernung, die Verletzung ihres Rechts nach § 78 UrhG ist auch ein Klagsgrund.

Sollen zum Beispiel die Veröffentlichungsrechte eines Werks erworben werden, ist dies bei der AKM (Gesellschaft der Autoren, Komponisten, Musikverleger) möglich. Sie sorgt für die Wahrnehmung von Urheberrechten im Bereich der öffentlichen Zurverfügungstellung, Aufführung und Sendung von Musik. Die AKM verwaltet und gewährt die Lizenzen aber nicht nur, sondern kontrolliert sie auch und klagt gegebenenfalls.

Creative-Commons-Lizenzen

Eine CC-Lizenz (Creative-Commons-Lizenz) ist ein Standardvertrag, der es der Autorin oder dem Autor auf einfache Art ermöglicht, die Nutzungsrechte an einem Werk mit der Öffentlichkeit zu teilen. Diese Lizenzen können auf verschiedene Werke angewendet werden (z. B. Videos, Musik, Text) und schaffen freie Inhalte bzw. frei nutzbare Inhalte. Sie können auf der Webseite von Creative Commons mit wenigen Klicks erstellt und für die eigenen Werke genutzt werden. Hierbei antworten Userinnen und User auf ein paar Fragen

Urheberin oder Urheber:

Eine Person, die durch eigene geistige Leistung ein Werk erschaffen hat.

Rechteinhaberin oder Rechteinhaber:

Jene Person, die die Rechte an einem bestimmten Werk hat; meint gemeinhin die Urheberin oder den Urheber.

Recht am eigenen Bild:

Bereits die Herstellung eines Bildes ohne Einwilligung der oder des Abgebildeten kann als Eingriff in die Persönlichkeitsrechte gelten. Fotos, Videos oder deren Begleittext dürfen die Abgebildeten nicht herabsetzen oder bloßstellen.

Weitere Infos zum Urheberrecht:

Siehe Kapitel „Urheberrecht", S. 109; siehe ISPA Publikation „Ratgeber Urheberrecht" kostenloser Download unter www.ispa.at/urheberrecht

Staatlich genehmigte Gesellschaft der Autoren, Komponisten und Musikverleger (AKM):

www.akm.at

(z. B. „Möchten Sie die kommerzielle Nutzung Ihres Werkes erlauben?“) und auf Basis ihrer Antworten wird die entsprechende CC-Lizenz generiert.

www.creativecommons.at

Aber Achtung: Es gibt nicht ***„DIE CC-LIZENZ“***, sondern verschiedene Lizenzverträge, die unterschiedlich frei oder streng formuliert sind. Eine CC-Lizenz ist kein Freibrief, das Werk komplett frei nutzen zu können, die Lizenz formuliert genau, unter welchen Bedingungen das Werk verwendet werden darf. Um einfach und dennoch eindeutig anzuzeigen, welche Nutzungslizenz vorliegt, werden Symbole (Icons) verwendet. Sie schlüsseln die Bedingungen, unter denen das Werk genutzt werden darf, auf.

Suchmaschine für Werke, die unter CC-Lizenzen stehen:
www.letscc.net

Es gibt eigene Suchmaschinen, die nur Onlinedienste mit Werken, die unter einer CC-Lizenz stehen, durchsuchen (z. B. www.letscc.net). Beispielsweise verwendet Wikipedia nur Bilder mit einer CC-Lizenz. Plattformen für frei verwendbare Musik mit CC-Lizenz für den privaten Bereich sind etwa Jamendo oder Free Music Archive.

Plattformen für frei nutzbare Musik:
www.jamendo.com
www.freemusicarchive.org

Beispiele für CC-Lizenzen

Das ist die freieste CC-Lizenz, empfohlen für maximale Verbreitung und Nutzung des lizenzierten Werkes. Diese Lizenz erlaubt es, das Werk zu verbreiten, zu remixen und darauf aufzubauen, auch kommerziell, solange Urheberin oder Urheber des Originals genannt werden.

Diese Lizenz erlaubt es, das Werk zu bearbeiten oder zu remixen, auch kommerziell, solange Urheberin oder Urheber des Originals genannt werden und die auf diesem Werk basierenden neuen Werke unter denselben Bedingungen veröffentlicht werden.

Das ist die restriktivste der CC-Kernlizenzen. Sie erlaubt lediglich Download und Weiterverteilung des Werkes unter Nennung der Urheberin oder des Urhebers, jedoch keinerlei Bearbeitung oder kommerzielle Nutzung.

Fremde Inhalte und Disclaimer

Disclaimer:
(Engl. für Haftungsausschluss.) Ablehnung, für fremde Inhalte zu haften.

Auf der eigenen Webseite oder im eigenen Blog auf fremde Inhalte zu verlinken, ist möglich und auch grundsätzlich in Ordnung. Die Schwierigkeit dabei ist, dass es nicht möglich ist zu wissen, welche weiteren Inhalte auf den verlinkten Webseiten veröffentlicht sind. Oft bleiben rechtsverletzende Inhalte unbemerkt, da Nutzerinnen und Nutzer nicht jede einzelne Unterseite der verlinkten Webseite durchsehen oder kurzzeitige Änderungen

wahrnehmen können. Um die Haftung für fremde rechtswidrige Inhalte zu vermeiden, setzen Bloggerinnen und Blogger und Webseiten-Host-Unternehmen sogenannte Disclaimer, also Haftungsfreizeichnungen ein. In diesen wird beispielsweise erklärt, dass die verlinkten Webseiten Dritter nicht inhaltlich oder auf zwischenzeitige Änderungen geprüft werden. Da die verlinkte Seite nicht unter der eigenen Verwaltung steht, haben Nutzerinnen und Nutzer keinen Einfluss darauf, ob der verlinkte Inhalt nicht später rechtlich bedenkliche Textpassagen enthält. Häufig findet auch der E-Mail-***DISCLAIMER*** Verwendung: Er klärt die Empfängerin oder den Empfänger darüber auf, dass der Inhalt vertraulich ist und Nutzerinnen und Nutzer das E-Mail bei versehentlichem Erhalten ignorieren oder an die Absenderin oder den Absender retournieren sollen.

Problematisch werden Verlinkungen, sofern sie auf Seiten mit rechtswidrigen oder strafbaren Inhalten verweisen (z. B. Kinderpornografie oder nationalsozialistische Inhalte). Webseiten-Betreiberinnen und -Betreiber sind haftbar, wenn sie von den rechtswidrigen Inhalten Kenntnis hatten und dennoch auf diese Webseiten verlinkten. Wussten die Betreiberinnen und Betreiber davon nichts oder entfernten sofort die Links, sobald sie davon erfuhren, haften sie nicht für die Inhalte.

Beispiele für Nutzungsbedingungen bzw. einzelne CC-Lizenzen:

Der Name der Urheberin oder des Urhebers muss angegeben werden.

Das Werk darf nicht verändert werden.

Das Werk darf nicht für kommerzielle Zwecke verwendet werden.

Bearbeitungen des Werkes dürfen unter den gleichen Bedingungen bzw. mit derselben Lizenz verbreitet werden.

Onlineshop

Buttonlösung

Rücktrittsrecht

Impressum

Informationspflicht

AGB

Online-Auktion

E-Commerce

Vertrag

Zahlungsart

54 Prozent aller Österreicherinnen und Österreicher kaufen regelmäßig über das Internet ein, damit befinden sie sich im EU-Durchschnitt. Am aktivsten ist die Altersgruppe der 25- bis 34-Jährigen, am häufigsten werden Kleidung, Sportartikel, Bücher und E-Books gekauft sowie Flüge und Urlaube gebucht. Die Online-Beschwerdestelle des österreichischen Internet Ombudsmannes verzeichnete im Jahr 2013 rund 5000 Beschwerden, der Großteil betraf vermeintliche Gratisangebote.
Quelle: Statistik Austria, Jahresbericht Internet Ombudsmann 2013

Onlinekauf

Sichere Onlineshops

Shoppen über das Internet bietet viele Vorteile: eine große Auswahl und die Möglichkeit, jederzeit und überall einzukaufen. Doch gerade, weil der Onlinekauf aus der Ferne stattfindet, sollten Userinnen und User vorsichtig sein. Im Gegensatz zum normalen Einkauf kann die Ware nicht „live" begutachtet werden, stattdessen gibt es Fotos, Beschreibungen und Rezensionen von Kundinnen und Kunden. Viele Webshops bieten sehr viele verschiedene Produkte an und verlangen teilweise auch unterschiedliche Preise, dazu kommen noch Versandkosten. Wie schon ihr Name verrät, fassen Preisvergleichsportale Produkte von mehreren Onlineshops zusammen und bieten so einen Überblick über die unterschiedlichen Preise im Netz. Doch Achtung: Tests von Verbraucherschutzzentralen zeigten, dass die Preissuchmaschinen nicht immer vollständige oder richtige Ergebnisse lieferten. Es empfiehlt sich daher, die Informationen von mehreren Preisvergleichsportalen miteinander zu vergleichen.

Wenn ein paar einfache Regeln beachtet werden, kann dennoch auch im Internet sicher eingekauft werden.

- → ***Faustregel:*** *Internationale und vertrauenswürdige Unternehmen betreiben oft eigene europäische, wenn nicht sogar österreichische Webshops (z. B. H&M, Thalia). Bei Anbietern außerhalb der EU oder ohne europäische Verkaufsplattform sollten Nutzerinnen und Nutzer vorsichtig sein, da es hier unter Umständen schwierig sein kann, ihr Recht durchzusetzen. Jedoch ist nicht jede Webseite mit einer .at- oder .de-Domain vertrauenswürdig! Bei Domainnamen, die auffällige Schlagwörter wie „Outlet" und „Sale" enthalten, ist Vorsicht geboten.*
- → ***Sichere Verbindung:*** *Eingaben von Daten sollten nur über verschlüsselte* ***SSL****-Verbindungen erfolgen. Die SSL-Verschlüsselung ist am* ***Schlosssymbol*** *erkennbar, oder daran, dass der Webadresse ein https:// vorangestellt ist.*
- → ***Impressum und AGB:*** *Das Impressum kann Aufschluss darüber geben, wer die Eigentümerin bzw. der Eigentümer der jeweiligen Domain ist. Webshops, die keine entsprechenden Informationen offenlegen, sollten mit Vorsicht behandelt werden. Die allgemeinen Geschäftsbedingungen zu*

Preisvergleichsportale:

www.geizhals.at

www.idealo.at

SSL-Protokoll:

Ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet (SSL = Secure Sockets Layer), seit Version 3.0 wird das Protokoll unter TLS weiterentwickelt und standardisiert (TLS = Transport Layer Security).

lesen dauert lange und teilweise sind diese schwer verständlich, zumindest ein kurzer Blick auf die Abschnitte bezüglich des Rücktrittsrechts oder der Bezahlung empfiehlt sich aber sehr.

- → ***Rücktrittsrecht:*** *Vertrauenswürdige Unternehmen haben ordentliche AGB und erläutern darin das Rücktrittsrecht.*
- → ***Zahlungsart:*** *Vertrauenswürdige Onlineshops bieten mehrere Zahlungsarten an. Zahlungen im Voraus sollten tunlichst vermieden werden, auch Kreditkarten sind nicht immer die sicherste Methode. Mittlerweile gibt es verschiedene sichere Online-Zahlungsarten, die von den meisten Webshops unterstützt werden, beispielsweise die* ***EPS-ONLINE-ÜBERWEISUNG*** *oder die Nachnahme.*
- → ***Österreichisches E-Commerce-Gütezeichen:*** *Dieses Gütezeichen kennzeichnet seriöse Onlineshops, die zuvor auf Sicherheit und Kundenservice geprüft wurden.*

EPS-Online-Überweisung:
„Electronic Payment Standard" ist die Schnittstelle für Online-Zahlungssysteme österreichischer Banken.

Vertragsabschluss

Um einen Kaufvertrag abzuschließen, müssen sich Käuferin oder Käufer und Verkäuferin oder Verkäufer über die Ware und den Preis einigen. Das gilt offline genauso wie online. Denn Verträge können – mit wenigen, für Onlinekäufe nicht relevanten Ausnahmen – in jeder beliebigen Form abgeschlossen werden.

Möglich sind im Internet etwa Einigungen zwischen den Vertragspartnern per E-Mail oder durch das Klicken eines Bestellbuttons, sogar in einem Chatraum können wirksame Verträge abgeschlossen werden. Dank dem Grundsatz der Formfreiheit von Verträgen sind hier – von gesetzlichen Ausnahmen einmal abgesehen – der Fantasie kaum Grenzen gesetzt. Jedoch dürften Vertragsschlüsse auf exotischen Wegen wie in einem Chatroom eher die Ausnahme darstellen. Verbreitet und in der Geschäftspraxis üblich sind vielmehr folgende Möglichkeiten:

Download

Eine Vertragspartei stellt eine bestimmte Ware (z. B. Musik, Filme etc.) in einer Datenbank zur Verfügung. Interessierte können nun gegen ein Entgelt diese Ware erwerben. Durch das Klicken eines Bestellbuttons und das Herunterladen der Inhalte erklären sich die Käuferinnen und Käufer mit dem Angebot einverstanden und nehmen dieses automatisch durch den Klickprozess an.

Webseite

Das reine Ausstellen von Waren auf einer Webseite wird rechtlich noch nicht als konkretes Angebot verstanden, sondern vielmehr als ein Anpreisen. Dadurch kann die Verkäuferin oder der Verkäufer sichergehen, dass bei großer Nachfrage nicht mehr Verträge abgeschlossen werden, als bedient werden können. Es bedarf der konkreten Anfrage durch die Besucherin oder den Besucher der Webseite via Kontaktformular oder E-Mail. Dann entscheidet die Verkäuferin oder der Verkäufer, ob diese Anfrage beantwortet wird bzw. beantwortet werden kann. Entweder wird eine Rückantwort versendet, oder die Ware wird direkt an die Käuferin oder den Käufer geschickt.

Online-Auktion

Eine Besonderheit stellt der Vertragsschluss über eine Auktionsplattform wie etwa eBay dar. Der Vorteil für die Verkaufenden besteht darin, dass sie ihre Kapazitäten genau abschätzen können, da nur ein Vertrag mit der oder dem Höchstbietenden abgeschlossen wird. Somit gibt es nicht das Risiko, dass mehr Verträge abgeschlossen werden, als tatsächlich Waren vorhanden sind.

Vertragsabschluss durch Kinder

Nicht jeder kann einen Vertrag schließen. Voraussetzung für die Vertragsschließung ist die Geschäftsfähigkeit. Geschäftsfähig sind alle Personen, die das 18. Lebensjahr vollendet haben und nicht geschäftsunfähig sind. Prinzipiell geschäftsunfähig sind Kinder, die das 7. Lebensjahr noch nicht erreicht haben, oder Personen, die sich dauerhaft in einem geistigen Zustand befinden, der es ihnen nicht erlaubt, rechtliche Geschäfte zu erledigen (z. B. Demenz, psychische Erkrankung).
Zwischen 7 und 14 Jahren sind Kinder noch unmündig, aber bereits beschränkt geschäftsfähig. Über Geschäfte nach dem „Taschengeldparagrafen" hinaus können sie nun auch solche tätigen, die ihnen ausschließlich rechtliche Vorteile bringen. Alle anderen Geschäfte sind schwebend unwirksam, bis sie durch die Erziehungsberechtigten bestätigt werden.

Der Taschengeldparagraf besagt, dass Kinder altersgerechte Geschäfte des alltäglichen Lebens vornehmen können (beispielsweise eine Kinderzeitschrift oder etwas zu Essen kaufen). Hierbei ist das Geschäft mit der Erfüllung der das Kind treffenden Pflichten (z. B. Zahlung des Kaufpreises) rückwirkend rechtswirksam. So können 7- bis 14-Jährige zum Beispiel ein geschenktes ferngesteuertes Auto wirksam annehmen, nicht aber einen geschenkten Hund. Ein geschenkter Hund wäre kein Geschäft des alltägli-

Definition von Minderjährigkeit:
§ 21 ABGB Abs 2

Geschäftsfähigkeit von Minderjährigen:
§ 865 ABGB

chen Lebens und würde dem Kind auch Pflichten auferlegen, somit würde die Schenkung eines Hundes über den Taschengeldparagrafen hinausgehen. Um den Hund als Geschenk anzunehmen, würde es der Zustimmung der gesetzlichen Vertreter bedürfen.

Jugendliche im Alter von 14 bis 18 Jahren sind ebenfalls nur beschränkt geschäftsfähig. Sie dürfen Geschäfte mit ihrem Taschengeld oder aus ihrem eigenen Einkommen (sofern vorhanden) ohne Zustimmung der Erziehungsberechtigten tätigen. Sobald diese Geschäfte aber ihren Lebensunterhalt gefährden – beispielsweise dürfen keine Schulden aufgenommen oder Ratenzahlungen vereinbart werden –, ist auch hier eine Genehmigung der Erziehungsberechtigten notwendig. Ohne diese Zustimmung ist der Vertrag ungültig.

Geschäfte über das Internet können zwar mittlerweile als alltäglich angesehen werden. Die Onlinebezahlung findet jedoch meistens per Kreditkarte, Lastschrift, Online-Überweisung oder Ähnlichem statt. Das alles sind Zahlungsmittel, die per se die Zustimmung der Erziehungsberechtigten voraussetzen.

Informationspflichten

Verbraucherinnen und Verbraucher müssen bei Bestellungen im Internet die wesentlichen Vertragsinformationen unmittelbar vor Beendigung des Bestellvorgangs klar, verständlich und in hervorgehobener Weise erhalten, damit sie selbst erkennen können, ob sie einen kostenpflichtigen Vertrag abgeschlossen haben oder nicht.

Unter anderem sind folgende Informationen zwingend erforderlich:

- → *die wesentlichen Merkmale der Ware oder Dienstleistung*
- → *Name und Anschrift des Unternehmens*
- → *die Mindestlaufzeit des Vertrags, wenn dieser eine dauernde oder regelmäßig wiederkehrende Leistung zum Inhalt hat (z. B. Abos)*
- → *den Gesamtpreis der Ware oder Dienstleistung inklusive Steuern*
- → *allfällige Lieferkosten*
- → *Zahlungs-, Liefer- und Leistungsbedingungen*
- → *bei Bestehen eines Rücktrittsrechts die Bedingungen, die Fristen und die Vorgangsweise für die Ausübung dieses Rechts*
- → *die Kosten für den Einsatz des Kommunikationsmittels*
- → *Hinweise auf das gesetzliche Gewährleistungsrecht und Kündigungsbedingungen*

→ *bei digitalen Inhalten: Hinweise hinsichtlich der Funktionsweise digitaler Inhalte und Interoperabilität digitaler Inhalte mit Hard- und Software*

Darüber hinaus muss die Käuferin oder der Käufer mit der Bestellung eindeutig zum Ausdruck bringen, dass mit der Bestellung eine kostenpflichtige Transaktion getätigt wird. Erfolgt die Absendung der Bestellung über einen Bestellbutton, so muss eben dieser auf die Kostenpflichtigkeit hinweisen, beispielsweise mit der Beschriftung „zahlungspflichtig bestellen" oder „kaufen".

Exkurs: Buttonlösung

Die ***„BUTTONLÖSUNG"*** ist Teil der neuen Verbraucherrechte-Richtlinie der EU. Sie soll dafür sorgen, dass Konsumentinnen und Konsumenten bei Vertragsabschlüssen im Internet die wesentlichen Informationen über den Vertragsinhalt sehen. Somit soll garantiert werden, dass es den Käuferinnen und Käufern bewusst ist, wenn sie einen kostenpflichtigen Vertrag abschließen.

In erster Linie muss die Unternehmerin oder der Unternehmer über die wesentlichen Merkmale der Ware oder Dienstleistung, die Mindestlaufzeit des Vertrags und den Gesamtpreis aufklären. Diese Informationen müssen derart prominent auf der Webseite platziert sein, dass sie beim Bestellvorgang nicht überlesen werden können. Der Bestellbutton darf erst nach dieser Information sichtbar sein. Ist eine Anmeldemaske so gestaltet, dass zuerst der Bestellbutton erscheint und erst danach die Informationen über den Vertragsinhalt zu sehen sind, so widerspricht das dem Gesetz.
Zusätzlich kommt es aber auch auf die richtige Beschriftung des Buttons an. Damit Verbraucherinnen und Verbraucher klar erkennen, dass sie nun dabei sind, einen Vertrag abzuschließen, muss der Bestellbutton mit eindeutigen Wörtern wie „kostenpflichtig bestellen", „zahlungspflichtigen Vertrag abschließen" oder „kaufen" beschriftet sein. Begriffe wie „Anmeldung", „weiter" oder „bestellen" sind nicht ausreichend, da sie im Hinblick auf eine Zahlungspflicht zu unklar sind.

Gerade die Mehrdeutigkeit von allgemeinen Begriffen haben sich Abo-Betrügerinnen und -Betrüger in der Vergangenheit zunutze gemacht. Für Vertragsabschlüsse seit dem 13. 6. 2014 gilt: Erfüllt eine Unternehmerin oder ein Unternehmer eine dieser Vorschriften nicht korrekt, kommt kein Vertrag zustande. Somit muss auch kein Rücktritt erklärt werden.

Buttonlösung ab dem 13. 6. 2014:

Sie macht die klare Ausweisung des Vertragsinhalts und eindeutig beschriftete Bestellbuttons erforderlich.

KOSTENPFLICHTIG KAUFEN

Verletzung der Informationspflichten

Die Informationen, die Verbraucherinnen und Verbraucher erhalten, sind Vertragsbestandteile. Änderungen sind nur dann wirksam, wenn sie von den Vertragsparteien ausdrücklich vereinbart wurden. Werden die kaufenden Userinnen und User nicht über zusätzliche Kosten oder Kosten für die Rücksendung der Ware aufgeklärt, so haben sie diese auch nicht zu tragen.

Die AGB

Die Allgemeinen Geschäftsbedingungen sind vorformulierte Vertragsbedingungen, die bei einer Vielzahl von Verträgen gelten sollen. Die Anwendung von AGB auf eine bestimmte Bestellung muss zuvor zwischen der verkaufenden Partei und den Kundinnen oder Kunden vereinbart werden. Die Unternehmerin oder der Unternehmer muss zu diesem Zweck deutlich zu erkennen geben, dass gewisse AGB angewendet werden sollen. Diese müssen zum Lesen und Speichern zur Verfügung gestellt werden. Klassischerweise können Käuferinnen und Käufer erst dann den Bestell- oder Kaufvorgang abschließen, wenn sie einen Haken in das Kästchen „Ich habe die AGB gelesen und erkläre mich mit ihnen einverstanden“ gesetzt haben. Wenn keine Zustimmung erfolgt, also den AGB nicht durch einen Haken zugestimmt wird, kommt der Vertrag auch nicht zustande.

Gibt es nachteilige, ungewöhnliche oder überraschende Klauseln in den AGB oder Vertragsformblättern, müssen die Userinnen und User auf diese hingewiesen werden, da sie ansonsten nicht gelten. Das ist auch dann der Fall, wenn die Käuferinnen und Käufer aufgrund der Begleitumstände des Vertrags und des äußeren Erscheinungsbilds nicht mit etwaigen nachteiligen oder ungewöhnlichen Klauseln rechnen konnten. Ein Beispiel hierfür wäre, wenn sich Unternehmerinnen oder Unternehmer in den AGB davon freisprechen, für Personenschäden, die durch Mängel ihrer Ware verursacht wurden, zu haften. Ob eine Klausel in den AGB Überrumpelungs- oder Übertölpelungseffekt hat und deshalb unwirksam ist, muss jedoch im konkreten Einzelfall beurteilt werden. Dies hängt sowohl von der Branche und ihren Üblichkeiten ab als auch vom Erwartungshorizont des Adressatenkreises. Die akzeptierten AGB werden Bestandteil des Kaufvertrags und die Verbraucherinnen und Verbraucher müssen sie gegen sich gelten lassen. Dies ist aber nur dann der Fall, wenn die AGB wirksam in den Vertrag einbezogen wurden, also eindeutig auf diese hingewiesen wurde. Ein bloßer Hinweis auf die AGB auf der Webseite reicht nicht aus, die Käuferinnen und Käufer

müssen die Möglichkeit gehabt haben, diese eindeutig zur Kenntnis zu nehmen – beispielsweise dadurch, dass die AGB durch Anklicken des unterstrichenen Wortes „AGB“ auf der Bestellseite aufgerufen und ausgedruckt werden konnten.

Rücktritt von Kauf oder Bestellung

a) Gesetzliches Rücktrittsrecht

Verträge zwischen Käuferinnen oder Käufern und Unternehmerinnen oder Unternehmern unterliegen grundsätzlich einem zwingenden gesetzlichen Rücktrittsrecht. Wird im Internet bei einem Händler eingekauft, kann der Vertrag innerhalb von 14 Tagen nach Erhalt der Ware ohne Angabe von Gründen widerrufen werden. Ein Widerruf muss ausdrücklich kommuniziert werden, ein kommentarloses Zurückschicken der Ware reicht nicht aus. Der Widerruf ist aber an keine bestimmte Form gebunden und kann in Textform, z. B. per Brief, Fax oder E-Mail, oder auch telefonisch erfolgen. Die Rücktrittsfrist ist gewahrt, wenn die Rücktrittserklärung innerhalb der Frist abgesendet wird.

Die Frist für den Widerruf beginnt erst mit dem Erhalt der Ware zu laufen, natürlich nur, sofern die Verbraucherin oder der Verbraucher über das Widerrufsrecht klar und verständlich belehrt wurde. Bei Verträgen über Dienstleistungen beginnt die Frist mit dem Zeitpunkt des Vertragsabschlusses. Ist die Widerrufsbelehrung fehlerhaft oder nicht vorhanden, erlischt dadurch nicht das Widerrufsrecht. Das bedeutet, dass noch innerhalb von zwölf Monaten nach Ablauf der 14-Tage-Frist widerrufen werden kann. Sobald die ordnungsmäßige Rücktrittsbelehrung nachgeholt wurde, beginnt die 14-tägige Frist zu laufen.

b) Rechtsfolgen des Rücktritts

Die Rechtsfolgen eines Rücktritts bewirken, dass die von den Kundinnen und Kunden geleisteten Zahlungen, einschließlich der Lieferkosten, spätestens 14 Tage nach Einlangen der Rücktrittserklärung zu erstatten sind. Die Rückzahlung muss mit demselben Zahlungsmittel erfolgen, welches die Verbraucherin oder der Verbraucher verwendet hat. Ein anderes Zahlungsmittel ist nur dann zulässig, wenn es ausdrücklich vereinbart wurde und der Verbraucherin oder dem Verbraucher dadurch keine Kosten entstehen.

Muster-Widerrufsformulare:

Solche werden oft von den verkaufenden Unternehmen bereitgestellt, teilweise auch mit der Ware standardmäßig mitgeschickt (z. B. H&M).

Musterbriefe und Rücktrittserklärungen gibt es beim Internet-Ombudsmann www.ombudsmann.at

Die unmittelbaren Kosten der Warenrücksendung sind von der Käuferin oder dem Käufer zu tragen, außer, die Unternehmerin oder der Unternehmer hat es unterlassen, über diese Kostentragungspflicht zu unterrichten. Das Widerrufsrecht kann in manchen Fällen ausgeschlossen sein – etwa bei individuell und auf Anfrage angefertigten Waren (z. B. Maßanzug, Einbauküche), schnell verderblichen Produkten, Zeitschriften und entsiegelten CDs, DVDs oder Software. Die Händlerin oder der Händler muss in diesem Fall jedoch ausdrücklich darauf hinweisen, dass kein Widerrufsrecht besteht.

c) Ausnahmen vom Rücktritt

Kein Rücktrittsrecht besteht unter anderem bei Verträgen über

- → *schnell verderbliche Waren (z. B. Lebensmittel);*
- → *Waren, die auf Anfrage nach persönlichen Bedürfnissen zugeschnitten wurden (z. B. Maßanzüge, Einbauküchen);*
- → *versiegelte CDs, Videos, Computerspiele, Software, sofern die Versiegelung (z. B. Plastikhülle) entfernt wurde;*
- → *Zeitungen, Zeitschriften und Illustrierte, wohl aber bei der Bestellung von Abos;*
- → *Dienstleistungen, sofern die Unternehmerin oder der Unternehmer aufgrund ausdrücklichen Verlangens der Verbraucherin oder des Verbrauchers bereits vor Ablauf der 14-tägigen Frist mit der Erbringung der Leistung begonnen hat oder*
- → *über Lieferung von nicht auf einem körperlichen Datenträger gespeicherten digitalen Inhalten (z. B. iTunes, E-Books, Apps), sofern vereinbarungsgemäß mit der Erbringung der Leistung vor Ablauf der 14-tägigen Frist begonnen wurde.*

Nicht gelieferte Ware

Verzug:
Verzögerung einer fälligen Leistung.

Nachfrist:
Käuferinnen oder Käufer können bei Nichterfüllung des Vertrags seitens der Verkäuferin oder des Verkäufers eine Frist zur Nacherfüllung setzen.

Sofern die Ware nicht rechtzeitig an den vereinbarten Lieferort geliefert wurde, wird von einem ***„VERZUG“*** gesprochen. In diesem Fall ist es möglich, entweder weiterhin auf der Lieferung zu bestehen oder unter Setzung einer Nachfrist vom Vertrag zurückzutreten („Ich trete vom Vertrag zurück, sofern die Ware nicht binnen 14 Tagen geliefert wird.“).

Bei der Bemessung der ***NACHFRIST*** muss jedoch die Versanddauer miteinkalkuliert werden, sodass die Verkäuferin oder der Verkäufer tatsächlich noch die Möglichkeit hat, die Lieferung nachzuholen.

Bei ***FIXGESCHÄFTEN*** ist eine Rücktrittserklärung und Nachfristsetzung nicht notwendig. Ein Fixgeschäft liegt vor, wenn klar erkennbar ist, dass an einer

verspäteten Leistung kein Interesse besteht, beispielsweise bei Bestellung von Geburtstagstorten oder einem Weihnachtsbaum.

Mangelhafte Ware

Grundsätzlich haftet die Unternehmerin oder der Unternehmer dafür, dass die Ware bei der Übergabe mangelfrei ist. Häufig wird bei mangelhafter Ware nicht ganz korrekt der Begriff ***„GARANTIE“*** verwendet, obwohl die ***„GEWÄHRLEISTUNG“*** gemeint ist.

Bei einer Garantie verpflichtet sich die Verkäuferin oder der Verkäufer, selbst jeden Mangel zu beheben, auch wenn der Mangel erst nach Übergabe der Ware entstanden ist. Die Garantie muss ausdrücklich vereinbart werden, stellt jedoch einen Ausnahmefall dar. Sie ist somit eine freiwillige Zusatzleistung einer Herstellerin oder eines Herstellers.

Eine Verkäuferin oder ein Verkäufer muss hingegen die gesetzlich geregelte Gewährleistung erfüllen. Die Gewährleistungsfrist beträgt bei beweglichen Waren (alles außer Liegenschaften) zwei Jahre. Ist die Ware mangelhaft, können die Verbraucherinnen und Verbraucher ihre Gewährleistungsansprüche geltend machen. Dieses Recht ist mit dem Konsumentenschutzgesetz gesetzlich verankert, muss nicht ausdrücklich vereinbart werden und kann auch nicht von der Verkäuferin oder dem Verkäufer ausgeschlossen werden. AGB, die dies nicht beachten, sind unwirksam. Die Gewährleistung gilt nur zwischen Unternehmerin oder Unternehmer und Verbraucherin oder Verbraucher.

Bei Privatkauf und -verkauf kann die Gewährleistung ausgeschlossen werden (z. B., wenn privat eine Uhr weiterverkauft wird), ebenso bei Geschäften von Unternehmen mit Unternehmen.

Sofern eine Ware im Onlinehandel gekauft wurde und ein Mangel festgestellt wird, gilt auch hier das Recht auf Gewährleistung. Der Gewährleistungsanspruch besteht verschuldensunabhängig, daher unabhängig davon, ob die Verkäuferin oder den Verkäufer die Schuld an dem bestehenden Mangel trifft. Dieses Recht soll sicherstellen, dass die Ware zum Zeitpunkt der Übergabe keinen Mangel hat.

Innerhalb der ersten sechs Monate besteht eine Beweiserleichterung. Hier wird davon ausgegangen, dass der Mangel bereits bei der Übergabe bestanden

Fixgeschäfte:

Ein gegenseitiger Vertrag, bei dem die Leistung an einen bestimmten Termin geknüpft ist (z. B. Lieferung eines Weihnachtsbaums).

Gewährleistungsanspruch:

Die verschuldensunabhängige Haftung der Verkäuferin oder des Verkäufers für Sach- und Rechtsmängel, die zum Übergabe- oder Lieferzeitpunkt bereits vorhanden sind.

Garantie:

Eine ausdrückliche Verpflichtung einer Produzentin oder eines Produzenten, einen Mangel an einer Ware auch dann zu beheben, wenn dieser nach der Übergabe der Ware entstanden ist.

hat. Es liegt dann am Unternehmen, das Gegenteil zu beweisen. Nach Ablauf der ersten sechs Monate obliegt die Beweislast den Verbraucherinnen und Verbrauchern.

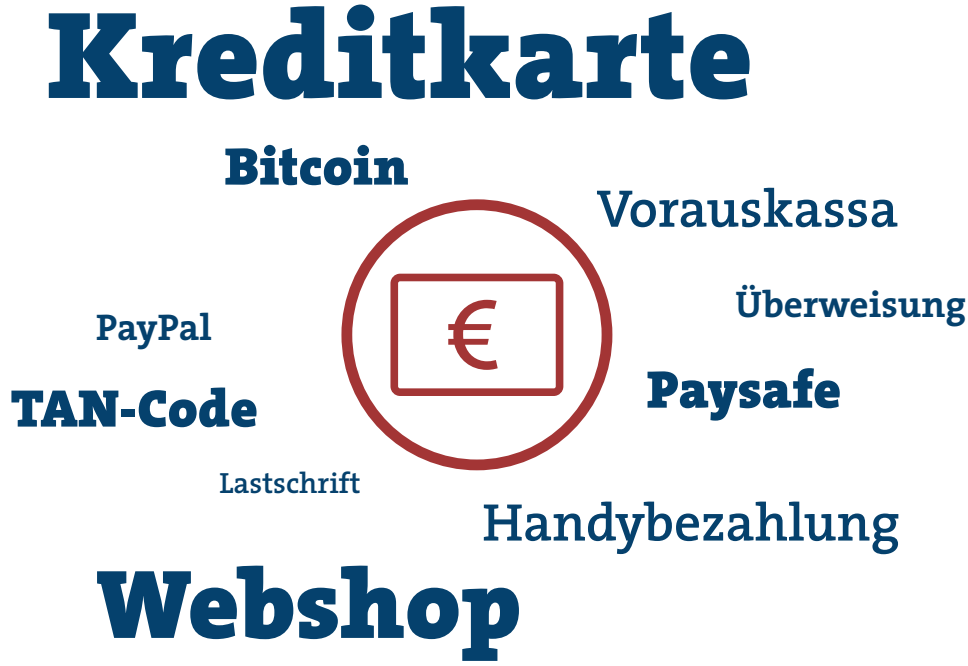
Die Gewährleistung sichert in erster Linie einen Anspruch auf Verbesserung, also z. B. Reparatur oder Nachtrag eines fehlenden Teils oder einen Austausch. Sofern die Verbesserung oder der Austausch nicht möglich sind, oder die Unternehmerin oder der Unternehmer trotz Aufforderungen nicht dazu bereit ist, könnte eine Preisminderung verlangt oder die Vertragsauflösung angestrebt werden ***(„WANDLUNG“)***. Eine Wandlung setzt jedoch einen nicht bloß geringfügigen Mangel voraus.

Wandlung:
Vertragsaufhebung aufgrund grober Warenmängel.

Beim Onlineshopping ist die Gewährleistung an jenem Ort zu erfüllen, an den die Ware versendet wurde. Jedoch kann die Unternehmerin oder der Unternehmer verlangen, dass die Konsumentin oder der Konsument die Ware auf Kosten des Unternehmens zurückschickt, damit diese ausgetauscht oder repariert werden kann.

Erst, wenn sich das Unternehmen trotz Aufforderung weigert, den Mangel zu beheben oder der Verbesserungsversuch fehlschlägt, kann eine Herabsetzung des Kaufpreises oder die Rückgängigmachung des Vertrags verlangt werden. Hier können die Käuferinnen und Käufer zwischen Preisminderung und Rückzahlung des Kaufpreises (Wandlung) wählen.

Wird über Wandlung oder Preisminderung keine Einigung erzielt, müssen diese Rechte auf gerichtlichem Weg durchgesetzt werden. Ist der Kaufpreis in solchen Fällen noch nicht bezahlt, besteht die Möglichkeit, erst nach dem Einklagen des Geldbetrags durch das Unternehmen entsprechende Einwände zu erheben. Da Gerichtsverfahren immer mit Kosten und einem Risiko verbunden sind, ist eine Einigung eher empfehlenswert. Bei Onlineshops, die im Ausland niedergelassen sind, kann sich die Durchsetzung der Ansprüche schwieriger gestalten.



In Österreich wird bei Bestellungen via Internet meistens mit Kreditkarte oder per Banküberweisung bezahlt, auf Platz drei und vier finden sich die Nachnahme und die Bezahlung per Bankeinzug. Zahlungsmittel, die speziell für die Bezahlung im Internet entwickelt wurden, rangieren eher auf den hinteren Rängen, obwohl auch sie langsam aufholen.
Quelle: ÖNB Zahlungsmittelumfrage 3/2013

Onlinebezahlung

Die Zukunft des Einkaufens liegt im Internet. Immer mehr Menschen nutzen die Möglichkeit, ihre Einkäufe einfach und bequem online zu erledigen, egal, ob es Kleidung, Unterhaltungsartikel oder sogar Lebensmittel betrifft. Eine aktuelle Studie des deutschen Branchenverbands Bitkom ergab aber, dass Sicherheitsbedenken Internetnutzerinnen und -nutzer zunehmend davon abhalten, die Vorteile von verschiedenen Online-Diensten zu nutzen. Konkret meidet ein Viertel der Befragten das Onlineshopping, da ihnen das Risiko von Betrug im Internet, beispielsweise von Datendiebstahl, zu groß ist.

Die gute Nachricht

Nahezu jede neue Statistik bestätigt eine stete Zunahme von Internetkriminalität, Passwortdiebstahl oder Betrug mit Kreditkarten, um nur ein paar Beispiele zu nennen. Die Vorfälle nehmen zwar zu, aber das ist weder überraschend noch übermäßig alarmierend. Immer mehr Menschen nutzen das Internet und machen von Online-Diensten Gebrauch. Durch die Zunahme der Nutzung und der Anwendungsmöglichkeiten steigt die Wahrscheinlichkeit von kriminellen Vorfällen. Gleichzeitig werden aber auch immer mehr Vorfälle den Behörden gemeldet; waren hier Userinnen und User früher noch zurückhaltend, zögern sie heute nicht mehr, Hilfe zu holen. Zusätzlich sind Nutzerinnen und Nutzer meistens gut informiert und kennen ihre Rechte – die sie auch durchsetzen möchten.

Als Vergleich zur Onlinebezahlung kann beispielsweise das Bezahlen bei einem Stand bei einem gut besuchten Konzert oder Fest herangezogen werden: Auch dort tummeln sich viele Menschen, es gibt Sicherheitsrisiken und eventuell auch Kriminelle. Doch was im „echten" Leben selbstverständlich ist, beispielsweise die Geldbörse nicht liegen zu lassen, diese an einem unauffälligen Ort bei sich zu tragen und schon gar nicht die Bankomatkarte samt PIN-Code an Fremde weiterzureichen, scheint sich nicht (immer) auf das Internet zu übertragen. Wenn Userinnen und User ein paar einfache Regeln befolgen, können die Gefahr verkleinert und Risiken umgangen werden. Die wichtigste Empfehlung ist, die eigene Software durch Updates auf dem aktuellen Stand zu halten, da veraltete Programme Einfallstore für Schad- oder Spionagesoftware sein können.

Bitkom-Studie „Lagebild Cybercrime":
goo.gl/t8YlIn

Was kann getan werden?

- → ***Faustregel:*** *Internationale und vertrauenswürdige Unternehmen führen oft eigene europäische, wenn nicht sogar österreichische Webshops (z. B. H&M, Thalia); bei Anbietern außerhalb der EU oder ohne europäische Verkaufsplattform sollten Nutzerinnen und Nutzer vorsichtig sein, da es für sie hier unter Umständen schwierig sein kann, ihr Recht durchzusetzen.*
- → ***Domain:*** *Nicht jede Webseite mit einer .at- oder .de-Top-Level-Domain ist automatisch vertrauenswürdig; bei Domainnamen, die auffällige Schlagwörter wie „Outlet" und „Sale" enthalten, ist Vorsicht geboten.*
- → ***Sichere Verbindung:*** *Eingaben von Daten sollten nur über verschlüsselte SSL-Verbindungen erfolgen, die SSL-Verschlüsselung ist am* ***Schlosssymbol*** *erkennbar, oder daran, dass der Webadresse ein https:// vorangestellt ist.*
- → ***Bezahlmethoden:*** *Die meisten professionellen Onlineshops bieten ihren Kundinnen und Kunden verschiedene Zahlungsverfahren an, im Zweifelsfall sollte auf die bequeme Kreditkarte verzichtet und lieber Nachnahme oder Bezahlung auf Rechnung gewählt werden.*
- → ***Konto kontrollieren:*** *Haben Userinnen und User ihre Konten im Auge, entdecken sie verdächtige Aktivitäten rasch und können diese bei ihrer Bank melden, sodass Sperren und Rückbuchungen sofort eingeleitet werden können.*
- → ***Österreichisches E-Commerce-Gütezeichen:*** *Dieses Gütezeichen kennzeichnet seriöse Onlineshops, die zuvor auf Sicherheit und Kundenservice geprüft wurden.*

Domain:
Das ist ein „Namensraum" im Internet, der eine weltweit im Internet einmalige und eindeutige Adresse darstellt.

Top-Level-Domain:
Die oberste Hierarchieebene von Internetadressen; wird unterteilt in allgemeine TLDs, wie .com oder .org, und in Länder-TLDs, wie .at oder .de.

Kreditkarte

Die Kreditkarte ist das am häufigsten verwendete Zahlungsmittel im Internet, gleichzeitig muss diese Zahlungsmethode immer als „schwarzes Schaf" herhalten, wenn es darum geht, potenzielle Gefahren im Internet aufzuzeigen. 80 Prozent der österreichischen Webshops bieten dieses Zahlungsverfahren an und die Gefahr für Kreditkarteninhaberinnen und -inhaber ist bei Weitem nicht so groß, wie sie eingeschätzt wird.

Verbraucherinnen und Verbraucher, deren Kreditkarte missbräuchlich verwendet wurde, können bei ihrer Kreditkartenfirma das Rückgängigmachen von solchen Buchungen verlangen – wenn beispielsweise mysteriöse Einkäufe getätigt wurden. Das ist eine Schutzbestimmung für Verbraucherinnen und Verbraucher, die vertraglich nicht ausgeschlossen werden kann. Somit tragen bei Kreditkartenzahlungen nicht primär die Karteninhaberinnen und -inhaber das Risiko, sondern die Händlerinnen und Händler, da diese in einem Schadensfall keinen gesicherten Zahlungsanspruch haben, das

Geld also nicht von ihren Kundinnen und Kunden verlangen können. Somit ist das Risiko, das bei den Karteninhaberinnen und -inhabern verbleibt, eher gering. Diese Schutzbestimmung für Konsumentinnen und Konsumenten gilt jedoch nicht im Fall eines völlig sorglosen Umgangs mit der Kreditkarte. Daher haben Kreditkartenunternehmen in ihren AGB diesbezüglich Bestimmungen, die festlegen, dass Verbraucherinnen und Verbraucher bestimmte Sicherheitsmaßnahmen einhalten müssen, da sonst keine Haftung übernommen wird. Hierzu gehört zum Beispiel ein sicherer Übertragungsweg bei der Weitergabe der Kreditkartendaten.

Ein sicherer Übertragungsweg ist beispielsweise das ***SSL-PROTOKOLL***. SSL ist ein offener Standard, der für die gesicherte Datenübertragung im Internet sorgt. Damit soll ein unberechtigter Zugriff auf sicherheitsrelevante Informationen, eben Kreditkartendaten, verhindert werden.

Die Kreditkartenunternehmen sind zudem bemüht, die Rahmenbedingungen für die Bezahlung mit Kreditkarte sicherer zu machen, und bieten auch ***PREPAID-KREDITKARTEN*** an. Diese Kreditkarte kann immer wieder mit einem individuell festgelegten Betrag aufgeladen und auch nur mit diesem belastet werden. Es kann also maximal der vorher einbezahlte Betrag behoben werden, somit ist die Möglichkeit für Missbrauch sehr begrenzt. Diese Kreditkarte eignet sich auch für Jugendliche, denen eine Möglichkeit der Bezahlung im Internet – und auch überall sonst – eröffnet werden soll.

Immer mehr Online-Unternehmen bieten außerdem die Möglichkeit eines gesicherten Kreditkarten-Zahlungsverfahrens an. Die bekanntesten sind „MasterCard Secure Code“ oder „Verified by VISA“. Das sind Authentifizierungsverfahren, bei denen alle Teilnehmenden (Händlerinnen oder Händler, Bank sowie Kundin oder Kunde) durch die zusätzliche Eingabe eines persönlichen Passwortes verifiziert werden, sodass anschließend die Kreditkartendaten über eine verschlüsselte Verbindung übermittelt werden können. Damit soll verhindert werden, dass die Kreditkarte missbräuchlich von unautorisierten Personen verwendet wird. Die Anmeldung zu diesem Verfahren und die Bekanntgabe des Passwortes erfolgen über die Kreditkartenfirma.

SSL-Protokoll:

Ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet (SSL für Secure Sockets Layer).

Prepaid-Kreditkarten:

Kreditkarten, die zuvor mit einem Betrag aufgeladen wurden und auch nur mit diesem belastet werden können.

Nachnahme/Lastschrift

Sofern die Onlineshops diese Option anbieten, kann auch per Nachnahme oder Lastschriftverfahren bezahlt werden. Die Bezahlung per Nachnahme hat den Vorteil, dass die bestellte Ware erst bezahlt wird, wenn sie geliefert worden ist. Diese Zahlungsmethode ist jedoch meist mit zusätzlichen Kosten verbunden.

Überweisung

Eine weitere Zahlungsmethode ist in Österreich die ***EPS-ONLINE-ÜBERWEISUNG***, ein Online-Zahlungssystem österreichischer Banken. Mit diesem System werden via Internet direkt vom Konto Online-Zahlungen durchgeführt. Über eine Schnittstelle erhält das Online-Unternehmen sofort von der Bank eine Zahlungsbestätigung. Um diese Form der Online-Überweisung nutzen zu können, müssen Userinnen und User vorher ihre Konten in ihrer Bank für Onlinebanking freischalten lassen. Mit den anschließend erhaltenen geheimen Zugangsdaten können Online-Zahlungen und -Überweisungen vorgenommen werden. Jede Transaktion wird dabei zusätzlich durch die Eingabe eines TAN-Codes bestätigt. Der ***TAN-CODE*** wird automatisch bei jeder Online-Überweisung an die Rufnummer geschickt, die Nutzerinnen und Nutzer zuvor als ihre Rufnummer angegeben haben. Mit diesem Code wird die Transaktion verifiziert. Ebenso gibt es die Möglichkeit, zuvor von der Bank TAN-Codes auf Vorrat zu erhalten, diese müssen Nutzerinnen und Nutzer persönlich beantragen.

EPS-Online-Überweisung:

„Electronic Payment Standard" ist die Schnittstelle der Online-Zahlungssysteme österreichischer Banken

www.eps.or.at

TAN-Code:

Die Transaktionsnummer ist ein Einmal-Code, der meistens aus einer sechsstelligen Zahlen- und Buchstabenkombination besteht und für Verifizierungen im Onlinebanking verwendet wird.

Prepaid-Karten

Ein weit verbreitetes Zahlungsmittel sind die Prepaid-Karten (z. B. paysafecard), die von vielen Onlineshops akzeptiert und besonders für Zahlungen im Gaming-, Filme- oder Musikbereich eingesetzt werden. Eine Prepaid-Karte ist eine anonyme Zahlungsmethode, die die (finanzielle) Privatsphäre wahrt. Weder ist eine Registrierung mit persönlichen Daten notwendig noch die Angabe von Kreditkarten- oder Kontodaten.

Die Prepaid-Karte kann mit unterschiedlich hohen Guthaben erworben werden (10, 25, 50 oder 100 Euro). Die Bezahlung funktioniert über den individuellen 16-stelligen Zahlencode, der auf dem Zahlungsmittel aufgedruckt ist. Für größere Transaktionen können auch mehrere Zahlencodes kombiniert werden.

paysafecard
pay cash. pay safe.

paysafecard - Bargeld für's Internet

Sicherheit ist ein zentrales Thema für alle, die online bequem und schnell bezahlen möchten. Hier bietet paysafecard eine zuverlässige Lösung.

Kaufe paysafecard mit Bargeld in einer der zahlreichen Verkaufsstellen (z.B. Trafik, Tankstelle) und bezahle damit sicher online durch Eingabe der 16-stelligen paysafecard PIN - ohne Bankkonto oder Kreditkarte.

1. 

Wähle paysafecard im jeweiligen Webshop als Zahlungsmittel aus.

2. 
Kaufe paysafecard im Wert von 10, 25, 50 oder 100 EUR.

3. 

Bezahle einfach durch Eingabe der 16-stelligen paysafecard PIN. Fertig!

www.paysafecard.com

Zusätzlich bieten manche Anbieter von Prepaid-Karten (wie z. B. paysafecard) u.a. ein Online-Zahlungskonto sowie eine App für iOS und Android, die die Nutzung dieses Zahlungsmittels unterstützt; beispielsweise kann das Guthaben einer Karte abgefragt oder eine Verkaufsstelle gefunden werden.

Mobile Zahlungsmittel

Weitere Möglichkeiten, online zu bezahlen, sind die Handybezahlung (z. B. Paybox) und das Bezahlen per Handyrechnung (z. B. Mehrwertdienste, manche App-Stores). Bei der Bezahlung mittels Handyrechnung werden die Kosten über die monatliche Abrechnung eingehoben, beispielsweise werden dann gekaufte Apps verrechnet oder auch die ***IN-APP-KÄUFE***. Ein weiteres Beispiel für die Bezahlung per Handyrechnung sind Mehrwertdienste, wie Klingeltöne für Handys. Jedoch sollten Nutzerinnen und Nutzer vorsichtig sein, denn nicht immer handelt es sich um einen einmaligen Kauf, sondern oft genug um kostenintensive Abos.

In-App-Käufe:
Bei manchen Apps (z. B. Spielen) besteht die Möglichkeit, im Rahmen der Anwendungen Guthaben oder Punkte zu kaufen, ohne einen klassischen Bestellvorgang zu durchlaufen.

Vorauskassa

Bei der Vorauskassa müssen Käuferinnen und Käufer den Kaufpreis im Voraus erstatten. Hierbei tragen sie daher das Risiko, die Ware – egal aus welchen Gründen – nicht zu erhalten, beispielsweise, wenn es sich um eine Betrugsmasche handelt. Vom Standpunkt des Verbraucherschutzes ist die Vorauskassa keine sichere Bezahlmethode.

PayPal

PayPal ist ein Online-Bezahlsystem für kleinere oder mittlere Geldbeträge. Hierbei haben Nutzerinnen und Nutzer ein virtuelles Konto, das sie mit Geld von ihrem regulären Bankkonto aufladen. Anschließend können Zahlungen getätigt werden. Der Vorteil dieser Zahlungsart ist, dass die Überweisungen vom PayPal-Konto sofort gutgeschrieben werden, sodass es keine langen Überweisungsdauern gibt. Obwohl der Dienst an sich kostenlos ist, fallen Transaktionskosten an.

Kryptowährung:
Digitales Zahlungssystem zur Verwaltung von privat geschöpftem, virtuellem Geld; es werden Prinzipien der Kryptografie angewandt.

Peer-to-Peer:
Auch P2P abgekürzt, ist eine Verbindungsart, bei der Daten direkt von Teilnehmerin/Teilnehmer zu Teilnehmerin/Teilnehmer übertragen werden.

Wallet:
Auch E-Wallet oder Cyberwallet, ist eine virtuelle Geldbörse.

Client:
Ein Computerprogramm, das auf einem Endgerät installiert wird und bestimmte Dienste vom Server abrufen kann.

Internetwährungen

Internet- oder auch ***KRYPTOWÄHRUNGEN*** sind digitale und länderübergreifende Zahlungsmittel. Sie funktionieren oft nach einem ähnlichen Prinzip, die meisten dieser Währungen finden aber kaum breite Verwendung. Die

wohl bekannteste und am weitesten verbreitete Kryptowährung ist Bitcoin. Bitcoin ist privat geschöpft und beruht auf kryptografischen Prinzipien, beispielsweise werden Transaktionen dezentral getätigt. Die Übertragung der Geldbeträge erfolgt auch Peer-to-Peer, sodass die üblichen Zwischenschritte des regulären Bankenverkehrs umgangen werden. Jede Transaktion wird mit einer digitalen Signatur versehen und in einer öffentlichen, vom gesamten Netzwerk betriebenen Datenbank aufgezeichnet.

Da die Popularität des virtuellen Geldes steigt, bieten immer mehr Onlinehändler die Möglichkeit, mit Bitcoin zu zahlen; sie sind aber derzeit noch in der Minderheit. Um mit Bitcoin zu zahlen, legen Nutzerinnen und Nutzer ein Wallet an (elektronische Geldbörse). Ein ***Wallet*** ist ein ***Client***, der das entsprechende Protokoll implementiert, in diesem Fall das Bitcoin-Protokoll. Dieses Wallet übernimmt die Funktion eines Kontos, das beispielsweise auch per App über das Smartphone verwaltet werden kann.

Coinmap.org:

Auf dieser Weltkarte sind alle Geschäfte und Unternehmen markiert, die Bitcoin als Zahlungsmittel akzeptieren.

Mycelium:

Österreichische App für einen Bitcoin-Client für Android-Smartphones.

Alias-Adresse

Kettenbriefe

Spam

Hoax

Searchbots

Wegwerf-Identität

E-Mail-Harvesting

Phishing

Phishing, betrügerische Webshops oder gestohlene Daten sind ärgerliche Nebenerscheinungen des Internets. Laut dem Internet-Sicherheitsbericht 2013 von Cert.at steigen die Gefahren von Onlinekriminalität, während das Bewusstsein für die Risiken vieler hinterherhinkt. Userinnen und User können sich jedoch mit einfachen Mitteln vor Spam, Phishing und kommerziellem Onlinebetrug schützen.

Onlinebetrug

Spam

Fast jede E-Mail-Adresse, die über eine gewisse Zeit in Gebrauch ist, wird früher oder später von unerwünschten Massenaussendungen heimgesucht, in denen von Potenzmitteln bis zu brachliegenden, aber prall gefüllten Konten bei Londoner Banken beinahe alles beworben wird. Spam verursacht in der weltweiten Onlinekommunikation großen Schaden, der auf die immense Datenmenge und den Aufwand der Bekämpfung zurückzuführen ist.

Die Zusendung von Werbemails an private Adressen ist ohne vorherige Zustimmung der Adressatin oder des Adressaten nicht erlaubt. Das gilt umso mehr für Zusendungen an mehr als 50 Personen, deren Einwilligung nicht vorliegt. Jedoch sieht das Gesetz eine Ausnahme vor: Unternehmen dürfen E-Mail-Werbung verschicken, wenn Userinnen und User zuvor bei ihnen etwas erworben haben und nicht die Zusendung von Werbemails aktiv abgelehnt haben. Das Unternehmen muss aber jederzeit die Gelegenheit bieten, weitere Zusendungen abzulehnen. Standardmäßig sind diese „Ausstieg-Links" in den Werbemails enthalten.

Ursprünglich wurde lediglich das ***USENET*** nach E-Mail-Adressen durchkämmt. Später wurden sogenannte ***SEARCHBOTS*** entwickelt, die das Internet nach allem absuchten, was nach einer E-Mail-Adresse aussah. Um sich diesem ***E-MAIL-HARVESTING*** zu entziehen, reicht es daher, die eigene E-Mail-Adresse nirgends öffentlich im Internet zu hinterlassen oder diese derart zu schreiben, dass Programme diese schwerer als Adressen identifizieren können (max[Punkt]mustermann [at]gmx[Punkt]at). Mit dem Aufkommen von ***VIREN*** war es aber bald möglich, einen befallenen Computer nach E-Mail-Adressen zu durchkämmen und diese „nach Hause zu telefonieren" – also an Dritte zu übermitteln.

Werden dennoch unerlaubt und ohne Zustimmung Werbemails verschickt, kann gegen die Absenderin oder den Absender Anzeige beim für das jeweilige Bundesland zuständigen Fernmeldebüro erstattet werden. Das wird jedoch bei Werbemails aus dem Ausland kaum helfen können. In diesem Fall ist auch davon abzuraten, ein E-Mail mit einer Abmelde- oder Ablehnungs-

Spam:
(Urspr. ein Markenname für Dosenfleisch, das während des Zweiten Weltkriegs als einziges Nahrungsmittel im Überfluss erhältlich war.) Sammelbegriff für jede Art von unerwünschten E-Mails, insbesondere Massenaussendungen mit Werbung.

Usenet:
Eigenständiges, weltweites elektronisches Netzwerk, welches lange vor dem World Wide Web entstand. Jenes Netz, in dem die klassischen Diskussionsforen des Internets (Newsgroups) zu Hause sind.

Searchbots:
Auch Spider oder Webcrawler genannt, sind Computerprogramme, die das Internet durchsuchen und Webseiten analysieren; sie werden vor allem zum Sammeln von E-Mail-Adressen, RSS-Newsfeeds und anderen Informationen eingesetzt.

erklärung zu schicken – denn wird auf Spam reagiert, erfahren die Spammerinnen und Spammer, dass sie eine gültige E-Mail-Adresse gefunden haben, und schicken im schlimmsten Fall noch mehr davon.
Der beste Schutz vor Spam ist Vorsorge. Es empfiehlt sich, zwei verschiedene E-Mail-Adressen zu führen: eine für berufliche und eine für private Zwecke. So kann auch das berufliche Ich vom privaten Ich getrennt werden.
Die berufliche E-Mail-Adresse sollte ausschließlich für Geschäftszwecke genutzt werden und sonst nicht weitergegeben werden. Denn eine Adresse, die nirgends öffentlich aufscheint, ist für Spammerinnen und Spammer deutlich schwerer zu bekommen.
Die private E-Mail-Adresse kann für Registrierungen bei sozialen Netzwerken, Newsletter und Gewinnspiele verwendet werden. Sie kann auch bei Bedarf leichter gewechselt werden. Es empfiehlt sich, für die Privatadresse einen großen Webmail-Anbieter zu wählen, da diese in der Regel über gute Spamfilter verfügen.

Tipp
Zwei E-Mail-Adressen zu haben bedeutet nicht zwingend, dafür zwei verschiedene Anbieter zu nutzen. Größere Mail-Provider bieten an, mehrere E-Mail-Adressen gleichzeitig zu verwenden, die dennoch in einem Postfach zusammengeführt werden. So können Userinnen und User sehr leicht ihren beruflichen und privaten E-Mail-Verkehr über ein Postfach verwalten.

Eine weitere Möglichkeit, sich vor Spam zu schützen, ist, für Anmeldungen bei Onlinediensten eine ***ALIAS-ADRESSE*** oder eine ***WEGWERF-ADRESSE*** zu verwenden. Viele Onlinedienste prüfen die Identität nicht, verlangen aber dennoch eine Datenangabe. Diese E-Mail-Adressen werden automatisch generiert und funktionieren nur für einen kurzen Zeitraum – lang genug, um die Registrierung durchzuführen. So werden keine „Datenspuren" hinterlassen.

Neben dem Angebot von Generatoren solcher Wegwerf-E-Mail-Adressen gibt es auch Generatoren für erfundene Identitäten. Per Zufallsgenerator wird eine fiktive Identität mit Namen, Geburtsdatum und Adresse erstellt. Dieser Service kann beispielsweise zum Schutz der Privatsphäre genutzt werden, aber auch, um Mängel schlecht konstruierter Webseiten und ausländischer Onlinedienste auszugleichen. Beispielsweise verweigert ein amerikanischer Onlinedienst die Anmeldung mit österreichischer Adresse, da die hiesigen Postleitzahlen vierstellig sind, das Eingabefenster aber für amerikanische, neunstellige Postleitzahlen konzipiert ist.

E-Mail-Harvesting:
(„To harvest", Engl. für ernten.) Automatisiertes Sammeln von E-Mail-Adressen aus Foren, Dokumenten und von Webseiten.

Viren:
Schädliche Computerprogramme, die sich selbstständig einschleusen und verbreiten können.

Fernmeldebüros:
www.bmvit.gv.at/telekommunikation/organisation/nachgeordnet/fmb

E-Mail-Dienste:
www.mail.google.com
www.mail.yahoo.de

Alias-Adresse:
(Engl. „alias" für Deckname oder Pseudonym.) E-Mail-Adresse, die keinen Hinweis auf die eigene Identität gibt.

Wegwerf-Adresse:
Wegwerf-E-Mail-Adressen sind provisorische E-Mail-Adressen, die nur für einen bestimmten Zeitraum gültig sind und anschließend verfallen.

Wegwerf-Identität:
Mit „Fake Identity"-Generatoren werden per Zufallsgenerator willkürlich Name, Geburtsdatum und Adresse aus Datenbanken ausgewählt.

Welche Schutzmaßnahmen zur Abwehr von Spam-Mails können getroffen werden?

- → ***Vorsorge:*** *Die eigene E-Mail-Adresse sollte nicht im Internet veröffentlicht werden; mit abonnierten Newslettern, Teilnahme an Gewinnspielen und Registrierung bei Webseiten steigt die Wahrscheinlichkeit für Spam. Ebenso empfiehlt es sich, verschiedene E-Mail-Adressen zu verwenden, beispielsweise eine für berufliche und eine für private Zwecke.*
- → ***Spamfilter beim Provider:*** *Die meisten Provider bieten einen solchen mittlerweile kostenlos an. Diese Spamfilter kennzeichnen den Spam (z. B. im Betreff) oder sortieren ihn automatisch in einen eigenen Ordner (z. B. Spam- oder Junk-Ordner).*
- → ***Spamfilter auf dem eigenen Computer:*** *Eine weitere Möglichkeit zur Abwehr ist ein Spamfilter auf dem eigenen Computer, die meisten E-Mail-Programme bieten sehr gute selbst lernende Spamfilter an; mit diesem Filter kann auch Spam aussortiert werden, der beim Provider durchgerutscht ist – der Spamfilter des Providers ist grobmaschiger, da damit viele Personen gleichzeitig bedient werden müssen.*
- → ***Robinsonliste:*** *Weiters besteht die Option, sich in die sogenannte Robinsonliste der RTR eintragen zu lassen. Das ist eine Liste mit den Kontaktdaten von Personen, die keine unangeforderte Werbung erhalten möchten. Zum Eintragen genügt ein formloses E-Mail an eintragen@ecg.rtr.at mit dem Betreff „Eintragen RTR-ECG-Liste"; diese Liste schützt jedoch nur bedingt vor Spam, da sich viele Spammerinnen und Spammer nicht an die rechtlichen Vorschriften halten.*
- → ***Achtung:*** *Userinnen und User sollten dennoch regelmäßig in ihren Spam-Ordner hineinsehen, da es vorkommen kann, dass das eine oder andere „echte" E-Mail darin landet.*

Phishing

Phishing ist eine Betrugsvariante, bei der Kriminelle versuchen, an Nutzerinformationen – beispielsweise Passwörter oder Zugangsdaten für Onlinebanking – heranzukommen. Die am weitesten verbreitete Form ist hierbei Datendiebstahl über E-Mail. In der Regel werden E-Mails verschickt, die den Anschein offizieller Nachrichten echter Unternehmen haben. In dem E-Mail werden die Userinnen und User aus einem vermeintlich wichtigen Grund dazu aufgefordert, einen Link anzuklicken, ihre Kontodaten neu einzugeben oder den Anhang zu öffnen.

Die meisten Phishing-E-Mails sind mittlerweile hochprofessionell und können oftmals auf den ersten Blick nicht als Betrug identifiziert werden. Eine andere Variante des Phishing ist, dass beim Öffnen des E-Mail-Anhangs

Phishing:
(Kunstwort aus „fishing", Engl. für fischen, und „password", Engl. für Passwort.) Betrugsmasche, um an Zugangsdaten zu kommen und somit Zugriff zu Accounts und Konten zu erhalten.

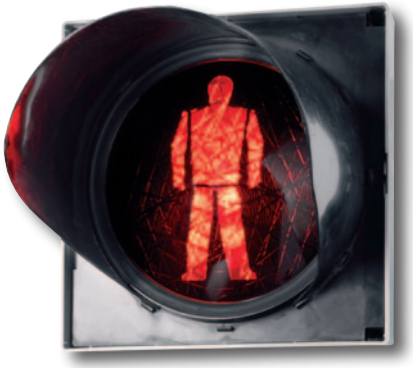
ein Virus oder ein Trojaner heruntergeladen wird, der im Hintergrund alle Tätigkeiten beobachtet und sofort „nach Hause telefoniert", sobald wertvolle Zugangsdaten oder -informationen eingetippt werden. Ebenso wurden aber auch Fälle gemeldet, bei denen sich telefonisch Unbekannte bei Nutzerinnen und Nutzern meldeten und sich z.B. als Mitarbeiter eines Computerunternehmens ausgeben. Sie behaupteten, einen Virus auf dem Computer entdeckt zu haben un d forderten die Nutzerin oder den Nutzer auf ihre Zugangsdaten durchzusagen. Seit dem Strafrechtsänderungsgesetz 2015 ist Phishing strafrechtlich erfasst und kann mit einer Freiheitsstrafe von bis zu einem Jahr verhängt werden, bei gewerbsmäßigem Phishing sogar bis zu drei Jahre.

Phishing
§ 241h Abs. 1 StGB

Wie können Phishing-E-Mails erkannt werden?

- → ***Faustregel:*** *Kein seriöses Unternehmen wie eine Bank oder ein Onlineshop fragt Daten der Kundinnen und Kunden per E-Mail ab oder tritt überhaupt über sehr allgemeine E-Mail-Aussendungen mit ihnen in Kontakt. Im Zweifelsfall sollte direkt die Webseite der Bank oder des Onlineshops besucht werden, oftmals sind dort bereits Hinweise auf aktuelle Betrugsmaschen zu finden.*
- → ***Absende-Adresse:*** *Wenden sich seriöse Unternehmen an ihre Kundinnen und Kunden – beispielsweise die Bankberaterin oder der Bankberater –, wird eine E-Mail-Nachricht auch entsprechend von der E-Mail-Adresse einer Person kommen (z. B. susanne.musterfrau@beispielbank.at) und nicht von einer allgemeinen E-Mail-Adresse; ein weiterer Hinweis kann sein, dass die E-Mail-Adresse besonders lang ist, aus Buchstaben- und Zahlenkombinationen besteht oder keiner österreichischen .at-Domain angehört, beispielsweise aus Polen, der Ukraine oder Russland kommt (.pl, .ua oder .ru).*
- → ***Original und Fälschung:*** *Professionelle Phishing-Mails imitieren bekannte Firmennamen oder deren Mail-Adressen. Beispielsweise kommt ein E-Mail statt von der echten Mail-Adresse der Bank Austria - office@unicredit-group.at – von einer auf den ersten Blick identisch aussehenden, bei der lediglich ein Buchstabe anders ist: office@unikreditgroup.at. Es empfiehlt sich, genau hinzusehen, um nicht getäuscht zu werden.*
- → ***Falsche Links:*** *Um diese zu erkennen, sollten Userinnen und User vor dem Anklicken den Mauszeiger darüberbewegen, unten links auf dem Bildschirm wird daraufhin der gesamte Linkpfad angezeigt; ist hier zu erkennen, dass es sich beispielsweise um einen Link auf eine ausländische Seite handelt, obwohl das E-Mail scheinbar aus dem Inland kommt, sollten Userinnen und User vorsichtig sein.*
- → ***Webadressen:*** *Um sicherzugehen, dass es sich auch tatsächlich um die richtige Webseite handelt, sollte die Webadresse eigenhändig in den Browser eingegeben werden.*

Stopp dem Internetbetrug.



Kostenlose Tipps für Ihre Sicherheit!

Machen Sie den Schritt zu mehr Sicherheit.

Das Sicherheitsportal der Bank Austria hält für Sie umfassende Informationen bereit – zum Beispiel aktuelle Tipps, wie Sie Betrugsversuche beim OnlineBanking erkennen.

http://sicherheit.bankaustria.at

Das Leben ist voller Höhen und Tiefen. Wir sind für Sie da.

Willkommen bei der
Bank Austria
Member of UniCredit

- → ***Sicherere Verbindung:*** *Bei der Eingabe von Daten im Internet sollte immer auf eine sichere Verbindung geachtet werden, also eine SSL-verschlüsselte Internetverbindung; hierbei wird der Webadresse https:// vorangestellt, im Browser erscheint neben der Webadresse das Schlosssymbol.*
- → ***Unpersönliche Anschreiben:*** *Seriöse Unternehmen schreiben ihre Kundinnen und Kunden persönlich an, unpersönliche Anreden wie „Guten Tag" oder „Sehr geehrte/r Kunde und Kundin" können ein Hinweis auf Phishing sein.*
- → ***Sprachliche Qualität:*** *Früher waren Phishing-Nachrichten auf den ersten Blick am schlechten Deutsch zu erkennen. Obwohl sich das mittlerweile geändert hat, können sich noch der eine oder andere Fehler oder eigenartige Formulierungen finden lassen.*
- → ***Textbaustein suchen:*** *Erscheint ein E-Mail verdächtig, kann es hilfreich sein, einen kleinen Textausschnitt daraus mittels Suchmaschine im Internet zu suchen. Meistens sind Phishing-Mails bereits weit verbreitet, und es gibt Warnungen und Artikel darüber zu finden (z. B. Hoax-Info-Service der TU Berlin (hoax-info.tubit.tu-berlin.de).*
- → ***Watchlist Internet:*** *Diese unabhängige österreichische Plattform informiert regelmäßig und aktuell über die neuesten Internetfallen. Hier können Nutzerinnen und Nutzer auch Fälle von Spam, Phishing etc. melden.*

Watchlist Internet
www.watchlist-internet.at

Hoax/Kettenbriefe/419 Scam

Hoax:
(„Hoax", Engl. für Scherz oder Schwindel.) Falschmeldung, die Userinnen und User täuschen soll, damit diese die Meldung weiterverbreiten.

419 Scam:
Sammelbezeichnung für verschiedene Betrugsvarianten per E-Mail, leitet sich vom entsprechenden Paragrafen des nigerianischen Strafgesetzes ab, da viele dieser Betrugsbanden ihren Sitz in Nigeria haben.

Ein Hoax ist eine Falschmeldung, die über E-Mail, Instant Messenger, soziale Netzwerke oder andere Wege verbreitet wird. Oftmals hat diese Meldung den Anschein einer authentischen Warnung vor Internetgefahren – beispielsweise vor Viren oder auch, sehr beliebt, einer Änderung der Nutzungsbedingungen auf Facebook – und wird daher von vielen freiwillig weitergeleitet. Die vergleichsweise harmloseren Kettenbriefe sollen nur Panik und Unsicherheit verbreiten, besonders Kinder sind hierfür anfällig. Bösartige Hoaxes sollen Nutzerinnen und Nutzer in Fallen locken, indem sie zusätzlich noch Abhilfe versprechende Links mitschicken, die jedoch nur Viren oder Malware bescheren oder zu betrügerischen Webseiten führen. Über aktuelle Hoaxes informiert beispielsweise die österreichische Plattform Watchlist Internet (www.watchlist-internet.at) oder der Hoax-Info-Service der TU Berlin (hoax-info.tubit.tu-berlin.de).

Kommerzieller Onlinebetrug

Den größten Schaden richten kommerzieller Onlinebetrug und betrugsähnliche Internetfallen an. Eine sehr verbreitete Form von Onlinebetrug sind

Webshops, die billige Markenware (z. B. Kleidung, Elektronik) anbieten. Hier sollten Nutzerinnen und Nutzer besonders misstrauisch sein, denn auch im Internet wird nichts verschenkt. Diese Betrugsform tritt üblicherweise in zwei Spielarten auf: Entweder handelt es sich statt um Originalware um billige Fälschungen (Produktpiraterie), oder die bestellte Ware kommt nach der Zahlung niemals an. Oftmals werden diese Webshops unter Angabe falscher Daten gegründet, viele davon sind in China angesiedelt. In den vergangenen Jahren hat sich auch der Onlinebetrug mit Immobilien gehäuft. Hierbei werden schöne Wohnungen in guter Lage und zu niedrigen Preisen beworben, doch die vermeintlichen Glücksgriffe existieren nicht. Unter einem Vorwand fordert die angebliche Verkäuferin oder der angebliche Verkäufer, manchmal aber auch die beauftragte Immobilienagentur, Geld für eine Besichtigung oder eine Kaufanzahlung, das angeblich bei Nichtgefallen rückerstattet wird. Oftmals ist das Geld, das die Interessierten überweisen, gar nicht das eigentliche Ziel, sondern die Bankdaten der unwissenden Userinnen und User.

Wie können Betrugsseiten erkannt werden?

- → ***Faustregel:*** *Internationale und vertrauenswürdige Unternehmen führen oft eigene europäische, wenn nicht sogar österreichische Webshops (z. B. H&M, Amazon). Bei Anbietern außerhalb der EU oder ohne europäische Verkaufsplattform sollten Nutzerinnen und Nutzer vorsichtig sein, da es hier unter Umständen schwierig sein kann, ihr Recht durchzusetzen. Jedoch ist nicht jede Webseite mit einer .at- oder .de-Domain vertrauenswürdig! Bei Domainnamen, die Schlagwörter wie „Outlet" oder „Sale" enthalten, ist Vorsicht geboten.*
- → ***Impressum:*** *Das Impressum kann Aufschluss darüber geben, wer die Eigentümerin/der Eigentümer dieser Domain ist. Webshops, die keine entsprechenden Informationen offenlegen, sollten mit Vorsicht behandelt werden.*
- → ***Rücktrittsrecht:*** *Vertrauenswürdige Unternehmen haben AGB und erläutern darin das Rücktrittsrecht.*
- → ***Vorauskassa meiden:*** *Zahlungen im Voraus sollten tunlichst vermieden werden. Mittlerweile gibt es verschiedene sichere(re) Online-Bezahlmethoden, die von den meisten Webshops unterstützt werden. Ebenso sollte bei unbekannten Webshops erst nach dem Erhalt der Ware das Geld überwiesen werden.*
- → ***Aufmerksam lesen:*** *Viele Anbieter arbeiten mit der Unachtsamkeit der Käuferinnen und Käufer. Durch die richtigen Schlagwörter und Bilder in der Produktbeschreibung soll der Eindruck vermittelt werden, dass es sich beispielsweise um ein iPad handelt, jedoch wird bei genauerem Lesen lediglich eine iPad-Hülle verkauft.*
- → ***E-Commerce-Gütezeichen:*** *Dieses Gütezeichen kennzeichnet seriöse Onlineshops, die zuvor auf Sicherheit und Kundenservice geprüft wurden.*

Klarname

Grooming

Auskunfts-pflicht

Trolle

Hacking

Haftung

Stalking

Hasspostings

Immer wieder wird im Zusammenhang mit dem Internet von Cybercrime gesprochen. Doch nicht alles, was gemeinhin darunter verstanden wird, gehört auch in diese Kategorie. Viele Delikte werden heute nur durch Zuhilfenahme des Internets begangen, sind aber wesentlich älter als dieses, Betrug etwa. Einige kriminelle Praktiken jedoch kamen erst mit dem Internet auf.

Cybercrime

Als einfache Faustregel gilt: Was in der realen Welt illegal ist, ist das auch in der virtuellen. Vollständig strafmündig sind Userinnen und User ab dem 18. Lebensjahr, jedoch können auch Jugendliche ab dem 14. Lebensjahr bereits für strafbare Handlungen zur Verantwortung gezogen werden. Das bedeutet jedoch nicht, dass Kinder unter 14 Jahren tun und lassen können, was sie wollen. In manchen Angelegenheiten haften jene Personen, die zum Tatzeitpunkt die Aufsichtspflicht hatten. In ernsten Fällen können auch Maßnahmen nach dem Jugendwohlfahrtsgesetz verhängt werden: Das Kind kann unter die Aufsicht des Jugendamts gestellt oder den Eltern das Erziehungsrecht entzogen werden.

Kinderpornografie

Prinzipiell ist in Österreich das Konsumieren von Pornografie im Internet legal. Klar davon zu unterscheiden sind illegale pornografische Inhalte, also Kinderpornografie und Missbrauchsdarstellungen von Kindern.

In Österreich ist neben dem Besitz und der Verbreitung auch bereits der wissentliche Zugriff auf kinderpornografische Darstellungen strafbar. In den Bereich der Kinderpornografie fallen Bilder oder Videos, die geschlechtliche Handlungen mit oder von Minderjährigen zeigen, aber auch die Genitalien oder die Schamgegend von Minderjährigen. Missbrauchsdarstellungen von Kindern unter 14 Jahren sind ausnahmslos strafbar. Hier reicht bereits der Eindruck, dass es zu einer sexuellen Handlung gekommen ist (z. B. eine Fotomontage).

Vom Besitz spricht man, wenn kinderpornografische Inhalte auf dem eigenen Computer oder einem anderen Endgerät gespeichert werden. 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 beispielsweise dann angenommen werden, wenn auf eine Seite mit eindeutigem Material wiederholt zugegriffen wird.

Kinderpornografie:
§ 207a StGB.

Stopline:
Meldestelle für Kinderpornografie und Nationalsozialismus im Internet.
www.stopline.at

Meldestelle Kinderpornografie und Sextourismus des Bundeskriminalamtes
meldestelle@interpol.at

Unmündige Minderjährige:
Jugendliche unter 14 Jahren.

Mündige Minderjährige:
Jugendliche ab 14 Jahren.

Sexting:
(Kombination aus „sex" und „texting", Engl. für SMS schreiben.) Das Verschicken von Texten mit sexuellen Inhalten, freizügigen Fotos oder Videos per SMS, Instant Messenger oder Chat.

Verbotsgesetz:
§ 3 VerbotsG

Abzeichengesetz:
AbzeichenG 1960.

Kinderpornografische Inhalte im Internet können anonym bei der Stopline oder der Meldestelle des BK gemeldet werden.

Ausnahmen liegen nur dann vor (§207a Abs 5), wenn eine pornografische Darstellung einer mündigen minderjährigen Person (14–18 Jahre) mit deren Einwilligung und zu deren eigenem Gebrauch hergestellt oder besessen wird; oder eine pornografische Darstellung einer mündigen minderjährigen Person zu deren eigenem Gebrauch hergestellt oder besessen wird, wenn damit keine Gefahr der Verbreitung der Darstellung verbunden ist. Beispielsweise wäre es in Ordnung, wenn zwei Jugendliche Nacktfotos voneinander besitzen, wenn diese im gegenseitigen Einvernehmen (z. B. im Rahmen einer Beziehung) aufgenommen werden.

Achtung:
Der Kinderpornografie-Paragraf ist im Zusammenhang mit ***SEXTING*** in der Praxis problematisch. Beispielsweise machen sich Jugendliche unter 14 Jahren der Kinderpornografie schuldig, wenn sie Nacktbilder oder sexuell anmutende Foto- und Videoaufnahmen von sich selbst machen und diese verbreiten (z. B. an Freunde schicken).

Nationalsozialismus

Nach dem Verbotsgesetz ist es strafbar, über Medien nationalsozialistisches Gedankengut zu verbreiten, zu leugnen, zu verharmlosen, gutzuheißen oder zu rechtfertigen. Als Medium gilt beispielsweise eine Webseite, ein öffentliches Forum oder auch ein Massen-E-Mail. Der Strafrahmen beträgt bis zu zehn Jahre Haft. Noch strengere Strafen gibt es für die Gründung von nationalsozialistischen Verbindungen, das Anwerben von Mitgliedern für eine solche Verbindung oder auch die Beteiligung daran.

Stoßen Nutzerinnen und Nutzer im Internet auf nationalsozialistische Inhalte, können sie diese anonym bei der Meldestelle Stopline melden. Viele soziale Netzwerke bieten mittlerweile integrierte Meldefunktionen, um solche und andere illegale Inhalte melden zu können (z. B. bei Facebook, Twitter, Instagram).

Das Veröffentlichen und die Zurschaustellung von nationalsozialistischen Abzeichen und Uniformen ist nach dem Abzeichengesetz ebenfalls verboten, wenn es im Zusammenhang mit der Verbreitung des verbotenen Gedankenguts steht. Das gilt auch für das Posten von entsprechendem Bild-

material in sozialen Netzwerken, was ebenfalls unter das Verbotsgesetz fällt.

Hacking

Der Begriff Hacking bezeichnet unerlaubtes Eindringen in ein fremdes Netzwerk, Computersystem oder Computer-Endgerät. Hacking ist allerdings nur dann strafbar, wenn Sicherheitsvorkehrungen des Systems verletzt bzw. überwunden wurden und sich die Täterinnen oder Täter zusätzlich einen Vermögensvorteil verschaffen oder die Betreiberin oder den Betreiber des Systems schädigen wollen (z. B. Auskundschaften von Betriebsgeheimnissen). Nach der Novelle des Strafgesetzbuches 2015 ist nun auch das Errichten von sogenannten BOT-Netzwerken unter Strafe gestellt. Dabei handelt es sich um automatisierte Computerprogramme („Bots" vom Englischen „Robot"), die ohne Wissen der Inhaberin oder des Inhabers auf deren Rechner laufen, um zum Beispiel gemeinsame, orchestrierte ***DDoS-Attacken*** durchzuführen. Die Gesetzesnovelle stellt das unbefugte Verwenden von Daten (Speichern, Verändern, Löschen wie auch Übermitteln) sowie das Verwenden eines fremden Computersystems an sich mit der Absicht, dadurch einem Dritten einen Nachteil zuzufügen, unter Strafe.

Hacking ist zudem ein ***ERMÄCHTIGUNGSDELIKT;*** die Strafverfolgung erfolgt nur mit Zustimmung der oder des Geschädigten.

Stalking

Umgangssprachlich wird oftmals jede Form des aufdringlichen Verhaltens als Stalking bezeichnet. Der Begriff des Stalkings meint den Tatbestand der beharrlichen Verfolgung einer Person. In juristischem Sinn handelt es sich um Stalking, wenn die Lebensführung des Opfers unzumutbar beeinträchtigt wird.

Rechtlich wird also von Stalking gesprochen, wenn die Stalkerinnen oder Stalker

- → *die räumliche Nähe zu ihren Opfern suchen,*
- → *Kontakt zu den Opfern mittels eines Kommunikationsmittels herstellen,*
- → *unter Verwendung der personenbezogenen Daten der Opfer Waren oder Dienstleistungen für sie bestellen,*
- → *unter Verwendung der personenbezogenen Daten der Opfer Dritte dazu veranlassen, mit ihnen Kontakt aufzunehmen.*

DDoS-Attacke:
(„Distributed Denial of Service", Engl. für Verteilte Dienstblockade.) Von einer größeren Anzahl an Systemen verursachte Überlastung eines Dienstes (z. B. einer Website).

Ermächtigungsdelikt:
Strafbare Handlung, die von der Staatsanwaltschaft nur dann verfolgt wird, wenn die oder der Betroffene zustimmt.

Anti-Stalking-Gesetz:
§ 107a StGB.

Demnach ist Telefonterror genauso gemeint wie das ständige Verschicken von SMS, E-Mails oder Briefen. Stalking ist ein ***OFFIZIALDELIKT***; die Strafverfolgung erfolgt von Amts wegen.

Offizialdelikt:
Strafbare Handlung, die von der Staatsanwaltschaft von Amts wegen verfolgt wird.

Grooming

Der Tatbestand des Cybergroomings meint die – versuchte wie auch erfolgreiche – Anbahnung von sexuellen Kontakten zu Minderjährigen. Hierbei erschleichen sich Erwachsene das Vertrauen von Kindern und Jugendlichen, beispielsweise mit dem Ziel, freizügige Fotos auszutauschen oder sich für sexuelle Handlungen in der realen Welt zu verabreden.

Grooming-Gesetz:
§ 208a StGB.

Siehe Kapitel „Cybergrooming“ S. 100.

Hasspostings bzw. strafbare Postings

Gemeinhin werden unter dem Begriff Hasspostings verschiedene Arten von negativen Äußerungen bzw. Postings im Internet zusammengefasst. Prinzipiell werden hiermit angriffige Postings gemeint, die oftmals auch einen rechtlichen Tatbestand erfüllen und somit strafbar sind, meistens jenen der Verhetzung.

Viele strafbare Postings sind sogenannte Medieninhaltsdelikte, konkret: üble Nachrede, Ehrenbeleidigung und Verleumdung. Das sind Straftaten, die durch direkte Äußerung in einem Medium begangen werden, beispielsweise auf einer Webseite veröffentlicht oder durch eine E-Mail-Aussendung verbreitet werden (der E-Mail-Versand muss mind. zehn Empfängerinnen oder Empfänger haben). Rechtlich macht es keinen Unterschied, ob die Delikte über das Internet oder am Stammtisch begangen werden.

Achtung: Nicht jedes rassistische Posting ist automatisch ein Hassposting oder erfüllt den Tatbestand der Verhetzung!

Verhetzung

Beim Straftatbestand der Verhetzung § 283 StGB nach Absatz 1 fordert eine Täterin oder ein Täter vor vielen Menschen (vor mind. 30 Personen) zu Gewalt auf oder spornt zu Hass gegen Menschen an, die einer bestimmten Religion, Nationalität oder Ethnie angehören bzw. eine bestimmte sexuelle Orientierung oder Hautfarbe haben (z. B. indem zu konkreten Gewalthandlungen wie dem Einwerfen von Fenstern oder körperlicher Gewalt gegen eine Gruppe aufgerufen wird).

Verhetzung:
§ 283 StGB.

Auch das Beschimpfen oder Verletzen anderer Menschen in ihrer Menschenwürde aufgrund ihrer Religion, Nationalität, oder Ethnie, ist von der Verhetzung erfasst. Dabei muss die Beschimpfung in einer Weise erfolgen, die geeignet ist, diese Gruppe in der öffentlichen Meinung verächtlich zu machen oder herabzusetzen. Darüber hinaus sind das öffentliche Leugnen oder Verharmlosen von gerichtlich festgestelltem Völkermord und Kriegsverbrechen oder das absichtliche Verbreiten von hetzerischem Material („reposten") unter Strafe gestellt.
Sofern die Tat vor „breiter Öffentlichkeit" (vor mind. 150 Personen) begangen wurde, ist diese mit einer Freiheitsstrafe von bis zu drei Jahre zu bestrafen. Verhetzung ist ein Offizialdelikt, muss also von Amts wegen verfolgt werden.

Die Verhetzung steht in Konkurrenz zum Verbotsgesetz, das nationalsozialistische Tätigkeiten unter Strafe stellt, und ist diesem gegenüber subsidiär anwendbar. Das bedeutet, dass die Verhetzung nur „aushilfsweise" anwendbar ist, wenn die Handlung nicht schon nach dem Verbotsgesetz oder nach anderen Strafvorschriften mit (höherer) Strafe bedroht ist.

Üble Nachrede

Üble Nachrede ist der unrechtmäßige Vorwurf

- → *einer verächtlichen Eigenschaft oder Gesinnung oder*
- → *eines unehrenhaften Verhaltens (z. B. die Bezeichnung als Faschist, Rechtsextremist u. Ä.) oder*
- → *eines Verhaltens gegen die guten Sitten*

vor zumindest einer weiteren Person. Kann die Richtigkeit der Behauptung bewiesen werden, ist die Handlung nicht strafbar, da die Aussage der Wahrheit entspricht. Einer solchen Überprüfung standhalten müssen auch Postings in sozialen Netzwerken oder in öffentlichen Foren, da hier davon ausgegangen werden kann, dass mehr als eine Person diese sieht bzw. liest. Üble Nachrede ist ein ***PRIVATANKLAGEDELIKT***.

Ehrenbeleidigung

Ehrenbeleidigung ist die Beschimpfung oder Verspottung einer anderen Person vor mindestens zwei zusätzlichen Personen. Konkret fallen unter den Begriff der Ehrenbeleidigung somit der Gebrauch von Schimpfwörtern und Spott in der Öffentlichkeit. Öffentlichkeit liegt eben dann vor, wenn die Handlung in Gegenwart von wenigstens zwei weiteren Personen begangen wird und diese die Handlung wahrnehmen können. In Foren, Chats und auf

Stopline:
anonyme Meldestelle gegen Nationalsozialismus im Internet
www.stopline.at

BMI: Meldestelle NS-Wiederbetätigung
ns-meldestelle@bvt.gv.at

Üble Nachrede:
§ 111 StGB.

Privatanklagedelikt:
Delikte, bei denen die oder der Geschädigte selbst als Privatanklägerin oder Privatankläger vor Gericht auftreten muss.

Ehrenbeleidigung:
§ 115 StGB.

Homepages kann fast immer von einer Öffentlichkeit ausgegangen werden. Bei Foren und Chats ist es vom dort üblichen Umgangston abhängig, ab welchem Grad eine Ehrenbeleidigung vorliegt. Handelt es sich um Foren und Chats, die für Nutzerinnen und Nutzer überhaupt nur den Zweck haben, sich durch Austausch wüster Beschimpfungen abzureagieren, oder in welchen sich diese auf regelmäßiger Basis gegenseitig beschimpfen, gilt wohl der Grundsatz: Teilnahme auf eigene Gefahr.

Ehrenbeleidigung ist ein Privatanklagedelikt. Neben strafrechtlicher Verfolgung droht im Falle einer öffentlichen Ehrenbeleidigung auch eine zivilrechtliche Unterlassungs- und Schadenersatzklage nach § 1330 ABGB, die sehr teuer werden kann. Die Voraussetzung hierfür ist, dass durch die Ehrenbeleidigung ein finanzieller Schaden entstanden ist oder droht (Kreditschädigungsklage).

Nickname:
Name der eigenen virtuellen Identität, im realen Leben mit einem Spitznamen zu vergleichen.

Achtung:
Selbst bei anonymer Beteiligung in einem Chatroom kann eine Beleidigung vorliegen. Wenn die beleidigte Person beispielsweise regelmäßig unter dem gleichen Nicknamen auftritt und aufgrund des Imageverlustes diesen ***NICKNAME*** nicht mehr verwenden kann. Anonymität schützt nicht vor der Begehung einer Straftat.

Verleumdung:
§ 297 StGB.

Verleumdung

Verleumdung ist die Verdächtigung einer Person, eine strafbare Handlung begangen zu haben. Hierbei beruht die Verdächtigung auf unwahren Behauptungen, es handelt sich also um eine wissentlich falsche Verdächtigung, die die beschuldigte Person in Gefahr bringt, durch die Polizei oder die Staatsanwaltschaft verfolgt zu werden. Verleumdung ist ein Offizialdelikt.

Kreditschädigung:
§ 152 StGB.

Kreditschädigung

Kreditschädigung ist die Behauptung falscher Tatsachen, wenn dadurch
→ *der Kredit,*
→ *der Erwerb oder*
→ *das berufliche Fortkommen*
anderer geschädigt oder gefährdet wird. Ein Beispiel hierfür wäre die Behauptung, dass jemand am Arbeitsplatz trinkt oder Firmengelder veruntreut hat.

Beleidigung Unbekannter

In den meisten sozialen Netzwerken und Foren herrscht keine Klarnamen-

pflicht, sodass die Userinnen und User selbst gewählte Nicknames verwenden. Werden zusätzlich keine weiteren personenbezogenen Daten – beispielsweise im eigenen Profil – veröffentlicht, können die Nutzerinnen und Nutzer durch die Verwendung von solchen Pseudonymen ihre Anonymität wahren.
Bei Medieninhalts- oder Ehrenbeleidigungsdelikten werden Personen öffentlich in ihrer Ehre beleidigt, selbst wenn ihre Identität nicht bekannt ist. Die Argumentation, dass die Identität der geschädigten Person nicht nachvollziehbar und somit nicht verletzbar ist, trifft nicht zu. Handelt es sich beispielsweise um einen regelmäßig verwendeten Nicknamen, unter dem eine Person bekannt ist (z. B. in einem Forum), also mit dem eine gewisse Identität aufgebaut wurde, kann die Person von den regelmäßigen Besucherinnen und Besuchern dieses Forums auch unter diesem identifiziert werden. Zusätzlich wird der beleidigten Person die Verwendung dieses Nicknames verleidet. Die Anonymität des Opfers schützt die Täterin oder den Täter nicht vor Begehung einer Straftat.

Handelt es sich hingegen um einen spontanen oder zufälligen Nicknamen, der lediglich dieses eine Mal verwendet wurde, ist eine Zuordnung zu einer nicht virtuellen Identität nicht möglich und damit die „Person" mangels Identifizierbarkeit nicht beleidigungsfähig.

Rauer Umgangston in Foren

In manchen Foren und Chats geht es wild bis sehr wild zu, gewisse Webseiten sind sogar für ihren rüden Umgangston oder die sinnbefreiten Postings bekannt. Teilweise sprechen sich hier die Userinnen und User prinzipiell mit Beschimpfungen an (4chan.org) oder posten (in dieser Community) bekannte Floskeln, die in den Augen Außenstehender mindestens als unhöflich, wenn nicht sogar beleidigend gelten könnten (9gag.com).

Bei Medieninhaltsdelikten wie der Beleidigung wird daher der Umgangston des Chats oder des Forums miteinbezogen, in diesem Zusammenhang wird von „milieubedingter Unmutsäußerung" gesprochen. Beispielsweise verschlechtert sich der Umgangston während eines ***SHITSTORMS*** zunehmend, da sich die Stimmung negativ auflädt bzw. unter Umständen auch ***TROLLE*** diese zusätzlich aufheizen. Die Postings der Nutzerinnen und Nutzer werden hier vom negativen Kontext bzw. der schlechten Stimmung beeinflusst, was wiederum nachkommende Posterinnen und Poster beeinflusst.

In einem rauen Milieu, also auf einer Webseite, auf der die Userinnen und

Klarname:
Auch Engl. „Realname", ist der tatsächliche Name einer Person, der auch in amtlichen Dokumenten geführt wird.

Shitstorm:
(Kombination aus „shit", Engl. für Scheiße, und „storm", Engl. für Sturm.) Sturm der Entrüstung im Internet, der zum Teil mit beleidigenden Äußerungen einhergeht.

(Internet-)Troll:
Person, die im Internet absichtlich Diskussionen anheizt oder andere Userinnen und User provoziert.

Netiquette:
(Komination aus „net“, Engl. für Netz, und „étiquette“, Franz. für Verhaltensregeln.) Der angemessene und achtvolle Umgang mit anderen Userinnen und Usern im Internet.

Pflichten von Host-Providern:
§ 16 ECG.

Auskunftspflicht:
§ 18 Abs 4 ECG.

User einen sehr unhöflichen Umgangston pflegen, kann eine Äußerung nicht strafbar sein, die es in einem Forum, in dem die ***NETIQUETTE*** befolgt wird, durchaus ist. Daneben kann eine Beleidigung, zu der sich Nutzerinnen und Nutzer aus Entrüstung über das Verhalten von anderen hinreißen lassen, unter Umständen straflos sein.

Haftung des Forumbetreibers

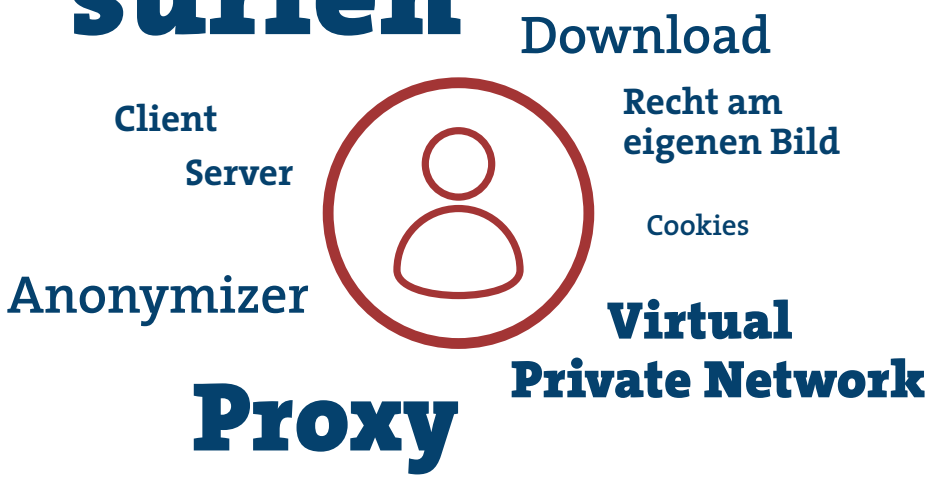
Betreiberinnen und Betreiber eines Chatforums trifft keine Verhinderungspflicht; sie müssen nicht ständig die Diskussion überwachen oder die von Userinnen und Usern geposteten Inhalte beobachten.

Betreiberinnen und Betreiber müssen rechtswidrige Inhalte entfernen, wenn sie auf diese hingewiesen werden und die Rechtswidrigkeit der Inhalte so offensichtlich ist, dass sie auch von juristischen Laien erkannt werden kann.

Probleme der strafrechtlichen Verfolgung

Schwierig(er) gestaltet sich die strafrechtliche Verfolgung von Personen, die unter einem Nicknamen auftreten. Hier können konventionelle Methoden angewendet werden (z. B. Befragung der Betreiberin oder des Betreibers wie auch der anderen Forumsteilnehmerinnen und -teilnehmer), aber ebenso technische (Ermittlung der IP-Adresse des Anschlusses), wobei Letzteres teilweise nicht möglich ist. Die Betreiberinnen und Betreiber eines Chats oder eines Forums trifft in einem solchen Fall, beispielsweise bei Anfrage durch die Exekutive, unter Umständen die Auskunftspflicht.

anonym surfen



Der Whistleblower Edward Snowden hat aufgezeigt, dass die Kommunikationsmittel des 21. Jahrhunderts dem Schutz der Privatsphäre in manchen Fällen nicht zuträglich sind. Dass aber nicht nur Geheimdienste oft mehr wissen als die engsten Freundinnen und Freunde oder manchmal auch man selbst, kann beispielsweise jeden Tag an Werbebannern beobachtet werden, die einem auf Webseiten präsentiert werden. Andererseits können diese auch hilfreich sein, wenn sie etwa passende Hotels zum soeben gebuchten Städteflug vorschlagen. Oftmals werden persönliche Daten als Gegenleistung für Gratisangebote freiwillig hergegeben. Dennoch möchten die meisten Nutzerinnen und Nutzer ihre Daten (im Internet) schützen und ihre Privatsphäre wahren.

Anonymität & Privatsphäre

IP-Adressen

Die IP-Adresse ist ein Zahlencode, der einem Gerät, das ans Netz angebunden ist, entweder fix zugewiesen oder vom Provider dynamisch vergeben wird. IP-Adressen werden verwendet, um Daten von einem absendenden Gerät zu einem empfangenden Gerät zu transportieren, sie funktionieren also wie Telefonnummern, die Absenderinnen oder Absender und Empfängerinnen oder Empfänger eindeutig identifizieren. Eine IP-Adresse wird einem Computer zugewiesen, der in ein Netz eingebunden ist, dadurch wird er adressierbar und somit erreichbar. Geräte hinter Firewalls oder ***ROUTERN*** haben dabei vom Internet aus gesehen oftmals nur eine gemeinsame Internetadresse, sind also anhand der IP-Nummer nicht unterscheidbar. Das aktuell weltweit eingesetzte Internetprotokoll ist ***IPV4***. IPv4 soll aber in den kommenden Jahren durch ***IPV6*** abgelöst werden, da dieses eine deutlich größere Zahl an Adressen ermöglicht.

Der private Modus

Die meisten Webbrowser bieten in ihren Einstellungen die Möglichkeit des „InPrivate"-Surfens. Dieser private Modus sorgt dafür, dass beim Internetsurfen keine bzw. weniger Spuren hinterlassen werden. Beispielsweise werden hierbei die Adressen der aufgerufenen Internetseiten nicht gespeichert und nicht in einer Chronik dokumentiert, Sucheinträge, Cookies und temporäre Internetdateien nicht gespeichert. Der private Modus ermöglicht, dass Nutzerinnen und Nutzer anonym(er) surfen können, kann aber keine absolute Anonymität garantieren. Empfehlenswert ist der private Modus besonders bei der Nutzung von fremden oder öffentlichen Computern.

- → ***Google Chrome:*** *Einstellungen > Neues Inkognitofenster*
- → ***Internet Explorer:*** *Einstellungen > Sicherheit > InPrivate-Browsen*
- → ***Mozilla Firefox:*** *Einstellungen > Privates Fenster*
- → ***Opera:*** *Fenster und Tabs > Neuer Privater Tab*
- → ***Safari:*** *Menü > Privates Surfen*

Router:

Netzwerkgeräte, die Informationspakete zwischen mehreren Rechnernetzen weiterleiten können. Sie werden u. a. für die Internetanbindung verwendet.

IPv4 bzw. Internet Protocol Version 4:

Aktuelles Internetprotokoll, das die technische Grundlage des Internets bildet. IPv4-Adressen sind 32 Bit lang.

IPv6 bzw. Internet Protocol next Generation (IPnG):

Neues Internetprotokoll, das IPv4 ablösen soll. IPv6-Adressen sind 128 Bit lang.

Firewall:

(Engl. für Brandwand oder Brandschutz.) Sicherungssystem, das einzelne Computer oder Netzwerke vor unerlaubten Zugriffen schützt.

Anonymizer

Server:
Computer, auf dem Programme laufen, auf die andere Computer (Clients) zugreifen können.

Client:
Computerprogramm, das auf einem Endgerät installiert ist und bestimmte Dienste vom Server abrufen kann.

Proxy:
(Engl. für Stellvertreter.) Schnittstelle in einem Netzwerk, die die Kommunikation zwischen zwei Servern/Rechnern weiterreicht.

Web Proxy Autodiscovery Protocol bzw. WPAD:
Protokoll, mit dem Web-Clients automatisch verfügbare Proxys finden können.

Virtual Private Network bzw. VPN:
(Engl. für virtuelles privates Netzwerk.) Schnittstelle in einem Netzwerk; kann eine Verbindung zwischen zwei Netzwerken sein oder zu einem bestimmten Service.

Um für mehr Anonymität zu sorgen, gibt es verschiedene Tools, die unterschiedlich viel technisches Know-how erfordern. Eine Möglichkeit sind hierbei Anonymisierungsprogramme, die die Internetverbindung eines Geräts über einen Anonymisierungsserver lenken. Dadurch wird die wahre Herkunft – also die IP-Adresse – gegenüber dem Zielserver verschleiert. Die gängigsten Varianten hierfür sind Proxy-Server oder Virtual Private Networks (VPN).

Der Proxy-***SERVER*** ist eine Schnittstelle in einem Netzwerk, die eine Vermittlerfunktion innehat. Vereinfacht formuliert nimmt ein ***PROXY*** auf der einen Seite Anfragen entgegen und leitet sie über seine eigene Adresse an die Zieladresse weiter (quasi wie eine Umleitung oder eine Zwischenstation); die Adresse des einen bleibt bei einer Proxy-Umleitung dem anderen verborgen, was eine gewisse Anonymität ermöglicht. Proxys werden aber nicht nur zur Schaffung von mehr Privatsphäre eingesetzt, sondern beispielsweise auch zum Schutz von Servern oder ***CLIENTS***. In diesem Zusammenhang werden Proxys zum Beispiel als Schnittstelle bzw. „Torhüter" zwischen einem privaten Netzwerk (z. B. Intranet einer Firma) und einem öffentlichen Netzwerk (Internet) verwendet, was das private Netzwerk weniger angreifbar macht.

Proxys sind meistens im Zusammenhang mit der Umleitung der Internetzugriffe des Browsers interessant. Mit einem WPAD-Protokoll können Web-Clients automatisch zu verwendende ***WEB-PROXYS*** innerhalb eines Computernetzwerks finden. Mit WPAD können alle Web-Clients angewiesen werden, Proxy-Server zu verwenden. Das wird von den Browsern Mozilla Firefox, Google Chrome und Internet Explorer unterstützt.

Ein ***VIRTUAL PRIVATE NETWORK (VPN)*** ist eine Schnittstelle in einem Netzwerk. VPN-Verbindungen finden in verschiedenen Formen Anwendung. Ein gängiges Beispiel hierfür ist die Verbindung von einem Netzwerk zum anderen via VPN-Zugang, der quasi einen Tunnel zwischen diesen beiden bildet. Beispielsweise, wenn eine Mitarbeiterin oder ein Mitarbeiter von zu Hause aus Zugriff auf das Firmennetz bekommt. Eine andere Variante des Virtual Private Network ermöglicht einen Fernzugriff auf bestimmte Anwendungen, ohne eine direkte Anbindung an das entsprechende Netzwerk.

Anonym surfen

Wer mit Webbrowsern im Internet surft, hinterlässt Spuren, die von den Diensteanbieterinnen und -anbietern (Webseiten, Suchmaschinen, Mail-Dienste) gesammelt werden können, um beispielsweise Profile im Hinblick auf die Aktivitäten zu erstellen. Selbst wenn Cookies oder andere Spuren im Browser gelöscht werden, bleibt immer noch die IP-Adresse, die das Endgerät oder das Netz, an dem dieses hängt, eindeutig identifiziert. Es gibt aber zahlreiche Services, die sich Anonymität und Datenschutz auf die Fahnen geschrieben haben. Sie werben damit, keine Daten über ihre Nutzerinnen und Nutzer zu sammeln, es werden also keine Logdateien mit anwenderbezogenen persönlichen Daten gespeichert. Die bekanntesten Suchmaschinen sind DuckDuckGo, Ixquick und Metager.

Nutzerinnen und Nutzer müssen sich hierbei aber darüber im Klaren sein, dass die Auswertung anwenderbezogener Daten beispielsweise für „relevantere" Suchergebnisse sorgen kann. Suchen Nutzerinnen und Nutzer aus Österreich nach einem Begriff, werden ihnen zum Beispiel eher Artikel österreichischer Medien angezeigt. Wird nach einem Geschäft gesucht, erscheinen eher jene in der eigenen Umgebung.

www.duckduckgo.com
www.Ixquick.com
www.metager.de

Das Tor Netzwerk

Tor ist ein Netzwerk zur Anonymisierung von Verbindungsdaten. Hierbei wird der Datenverkehr durch verschiedene zwischengeschaltete Server geleitet, sodass die Verbindungsdaten bzw. die Absenderin oder der Absender nicht mehr nachvollziehbar sind. Dieses Netzwerk kann für verschiedene Dienste genutzt werden, oft etwa zum Internetsurfen, für E-Mail-Verkehr, Instant Messaging oder ***P2P***.

Nutzerinnen und Nutzer können den Tor-Browser für Windows-Betriebssysteme kostenlos auf der Webseite www.torproject.org downloaden. Das anonyme Surfen über das Tor-Netzwerk funktioniert mittels Onion Proxy Client. Nutzerinnen und Nutzer installieren diesen Client auf ihrem Endgerät. Dieses Programm verbindet sich mit dem Tor-Netzwerk und erhält eine Liste mit verfügbaren Tor-Servern. Für jede Suchanfrage wählt der Client eine zufällige Verbindung über drei verschiedene Server, wodurch größtmögliche Sicherheit und Anonymität garantiert werden. Dieser Verbindungsaufbau wird in regelmäßigen Abständen wiederholt.

www.torproject.org

Peer-to-Peer bzw. P2P:
Verbindungsart, bei der direkt von Teilnehmerin oder Teilnehmer zu Teilnehmerin oder Teilnehmer übertragen wird.

Achtung
Nutzerinnen und Nutzer müssen sich bewusst sein, dass Tor kein Garant für völligen Datenschutz und mehr Privatsphäre im Internet ist. Beispielsweise gab es dieses Jahr einen größeren Angriff auf das Tor-Netzwerk bzw. die Anonymisierungsknoten, sodass teilweise nachvollzogen werden konnte, wer welche Tor-Dienste genutzt hat. Userinnen und User laufen zudem Gefahr, stärker überwacht oder sogar ausspioniert zu werden. Die NSA hat viele Nutzerinnen und Nutzer genau aus dem Grund beobachtet, dass sie Dienste über das Tor-Netzwerk in Anspruch genommen hatten.

Cookies

Cookies haben trotz ihres harmlosen Namens keinen guten Ruf. Sie sind Teil von Webseiten, speichern für verschiedene Funktionen notwendige Daten und hinterlegen diese auf dem Computer oder mobilen Endgerät. Mit diesen Datenkrümeln können Userinnen und User beim (wiederholten) Besuch einer Webseite wiedererkannt werden und die Webseiten-Betreiberinnen und -Betreiber können mittels der gesammelten Informationen ein Profil erstellen. Das hört sich im ersten Moment schlimmer an, als es ist, denn mittels Cookies kann die Webseite für jeden Besuch individuell angepasst werden. Die Verwendungsmöglichkeiten reichen dabei von Online-Einkaufswagen über automatische Sprach- und Ländereinstellungen bis hin zu personalisierter Werbung.

Firefox:
Einstellungen > Datenschutz > Chronik „niemals anlegen“

Safari:
Einstellungen > Datenschutz > Cookies blockieren

Internet Explorer:
Einstellungen > Sicherheit

Google Chrome:
Einstellungen > Erweiterte Einstellungen > Datenschutz > „Speicherung von Daten für alle Webseiten blockieren“

- → ***Firefox:*** *Einstellungen > Datenschutz > Chronik „niemals anlegen“*
- → ***Safari:*** *Einstellungen > Datenschutz > Cookies blockieren*
- → ***Internet Explorer:*** *Einstellungen > Sicherheit*
- → ***Google Chrome:*** *Einstellungen > Erweiterte Einstellungen > Datenschutz > „Speicherung von Daten für alle Webseiten blockieren“*

Wie mit Cookies umgegangen werden soll, kann ohne großen Aufwand über den Webbrowser eingestellt werden. Zusätzlich gibt es spezielle Browser-Erweiterungen ***(ADD-ONS)***, die optional installiert werden können. Empfehlenswert sind in diesem Zusammenhang die Add-ons, die Online-Werbeanzeigen blockieren (Ad-Blocker). Beim ***INTERNET EXPLORER*** können Nutzerinnen und Nutzer über eine Tracking-Schutzliste festlegen, welche Webseiten ihre Daten abfragen und ihre Online-Aktivität nachverfolgen dürfen. Auch bei anderen Browsern wie ***MOZILLA FIREFOX*** (beispielsweise NoScript, BetterPrivacy) oder ***GOOGLE CHROME*** (Ghostery, AdBlock Plus) gibt es verschiedene Add-ons, die für mehr Datenschutz sorgen. Jedoch ist auch bei Add-ons Vorsicht geboten,

Add-on:
(Engl. für Erweiterung.) Add-ons sind optionale Module, die Software oder Hardware erweitern und neue Funktionen ermöglichen.

sie sind nicht nur Hilfsmittel, sondern können unter Umständen Sicherheitsrisiken sein (siehe „Sicherheitsrisiken minimieren“, S. 84).

Daten im Internet löschen

Die beste Möglichkeit, für mehr Privatsphäre und Datenschutz zu sorgen, ist, präventive und proaktive Maßnahmen zu setzen, konkret zum Beispiel Cookies zu deaktivieren oder sich überhaupt bewusst zu machen, dass (Daten-) Spuren im Netz zurückgelassen werden.

Der erste Schritt zu mehr Kontrolle über die eigenen Daten ist, überhaupt in Erfahrung zu bringen, welche Daten vorhanden sind. Facebook bietet in diesem Zusammenhang seinen Nutzerinnen und Nutzern unter dem Menüpunkt „Einstellungen“ die Möglichkeit, eine Kopie der eigenen Facebook-Daten (z. B. Profilinformationen, Aktivitätenprotokoll, verwendete Apps, Klicks auf Werbeanzeigen) herunterzuladen. Bei Google wiederum haben Userinnen und User die Möglichkeit, auf dem ***DASHBOARD*** ihres Kontos etwa ihre Suchverläufe einzusehen und sie auch zu löschen; dies ist auch bei Bing möglich. Informationen im Internet zu veröffentlichen ist heutzutage so leicht wie noch nie. Die Schwierigkeit ist eher, die Informationen wieder wegzubekommen. Denn sind Informationen, Fotos oder sonstige Beiträge erst einmal in Umlauf, können sie über das gesamte Netz verteilt werden. Sie zu finden und wieder einzusammeln ist keine leichte Aufgabe. Finden sich im Internet unangenehme oder sensible Daten über Nutzerinnen und Nutzer, ist es zwar nicht immer leicht, sie wieder zu entfernen, es gibt aber dennoch ein paar Möglichkeiten.

Dashboard:
(Engl. für Armaturenbrett.) Je nach Onlinedienst ist es unterschiedlich ausgestaltet, meistens jedoch die persönliche Start- oder Admin-Seite, auf der Information zusammengetragen wird.

Was können Userinnen und User tun?

- → ***Die Worst-Case-Frage:*** *Es kann hilfreich sein, sich vor jedem Posting die Frage zu stellen, welche Auswirkungen „der schlimmste Fall“ hätte, wenn also das Posting oder das Foto in Umlauf geriete und auch Jahre später noch online und für andere auffindbar wäre. Der Blick in die Zukunft und der Gedanke daran, dass zukünftige Arbeitgeberinnen oder Arbeitgeber, Bekannte oder Partnerinnen und Partner ein spezielles Stück Information sehen könnten, ist oft eine gute Entscheidungshilfe vor dem Posten und Veröffentlichen.*
- → ***Personenbezogene Daten:*** *Besonders mit persönlichen Daten – Geburtsdatum, Telefonnummer, Adresse etc. – sollten Userinnen und User vorsichtig umgehen.*
- → ***Trennung von Arbeit und Vergnügen:*** *Es empfiehlt sich, die beruflichen Online-Aktivitäten von den privaten zu trennen. Für soziale Netzwerke,*

Gewinnspiele und Newsletter sind eigene E-Mail-Adressen und Nicknames von Vorteil. Der Klarname sollte dem professionellen Auftritt vorbehalten bleiben.

- → ***Soziale Netzwerke:*** *Vor allem bei sozialen Netzwerken sollten Userinnen und User unbedingt die Privatsphäre-Einstellungen im Auge behalten und gegebenenfalls die höchstmögliche Privatsphärestufe wählen.*
- → ***Webseiten Dritter:*** *Sind Informationen tatsächlich auf fremden Webseiten gelandet oder wurden anderweitig verbreitet, können sich Userinnen und User an die Webseiten-Betreiber wenden und um die Entfernung der Information bitten.*
- → ***Regelmäßige Kontrolle:*** *In regelmäßigen Abständen sollten Userinnen und User mittels Suchmaschinen das Internet nach Einträgen von und über sich selbst durchsuchen. Somit können rechtzeitig Schritte in die Wege geleitet werden, falls bei einer dieser Suchen negative Einträge gefunden werden. Um den eigenen Namen zu suchen, sollte er unter Anführungszeichen gesetzt werden, sodass die Suchmaschine nicht lediglich nach den einzelnen Wörtern sucht (z. B. „Monika Musterfrau").*

Suchmaschinen-Ergebnisse

In einem Urteil vom Mai 2014 entschied der EuGH, dass Suchmaschinen dazu verpflichtet werden können, Artikel mit veralteten oder sensiblen Personendaten aus ihren Ergebnislisten zu entfernen. Konkret müssen Verweise aus der Liste der Suchergebnisse gelöscht werden, wenn die dort aufgelisteten Informationen das Recht auf Privatsphäre und Datenschutz verletzen. Betroffene, die keine Personen des öffentlichen Lebens sind, haben laut dem EuGH einen einklagbaren Anspruch auf Löschung solcher Link-Verweise.

Ungewollte Bildaufnahmen

Laut österreichischer Rechtslage darf in öffentlichen Bereichen jede und jeder fotografieren, ebenso kann jede und jeder (ungefragt) fotografiert werden. Das gilt jedoch nicht für die Verbreitung der Aufnahmen. Sie ist nur dann erlaubt, wenn sie nicht die berechtigten Interessen der Abgebildeten verletzt. Somit sollte ein Einverständnis für die Veröffentlichung der Aufnahmen eingeholt werden. Beispielsweise müssen Club- und Partyfotografinnen oder -fotografen die Gäste vor dem Fotografieren um ihre Erlaubnis fragen, wenn das in der Praxis auch eher informell passiert.

Recht am eigenen Bild

Im österreichischen Urhebergesetz ist das Recht am eigenen Bild verankert, das ein besonderer Teil des Persönlichkeitsrechts ist. Bereits die Herstellung eines Bildes ohne Einwilligung der oder des Abgebildeten kann als Eingriff in die Persönlichkeitsrechte gelten. Fotos, Videos oder deren Begleittext dürfen nicht die berechtigten Interessen der darauf abgebildeten oder darin beschriebenen Personen verletzen. Die Aufnahmen dürfen die Abgebildeten nicht herabsetzen oder bloßstellen. Relevant bei der Bestimmung der Rechtsverletzung ist hier, ob das Bild objektiv nachteilig ist und nicht nur als solches empfunden wird. Ein Foto mit unvorteilhafter Frisur stellt somit keine Rechtsverletzung dar.

Wird ein nachteiliges Bild oder Video entdeckt, haben Userinnen und User das Recht auf Löschung oder Entfernung, da hier das Recht am eigenen Bild gilt. In vielen sozialen Netzwerken gibt es hierfür bereits standardisierte Meldeverfahren, im Rahmen derer die Nutzerinnen und Nutzer solche Bilder melden können.

Was können Nutzerinnen und Nutzer machen?

- → ***Beweissicherung:*** *Mittels Screenshots der jeweiligen Webseiten sollten Beweise gesichert werden.*
- → ***Kontaktaufnahme:*** *Als Nächstes sollte schriftlich diejenige Person kontaktiert werden, die das Foto/Video hochgeladen hat. Allenfalls können auch die Webseiten-Betreiberinnen oder -Betreiber kontaktiert werden.*
- → ***Unterlassungsklage:*** *In schwerwiegenden Fällen können Userinnen und User ihre Ansprüche auch per Unterlassungsklage und – bei Schädigung – Schadenersatzforderung vor Gericht einklagen.*
- → ***Achtung:*** *Trotz Löschung auf einer Seite kann es natürlich passieren, dass die besagten Inhalte bereits anderswo im Internet gelandet sind.*

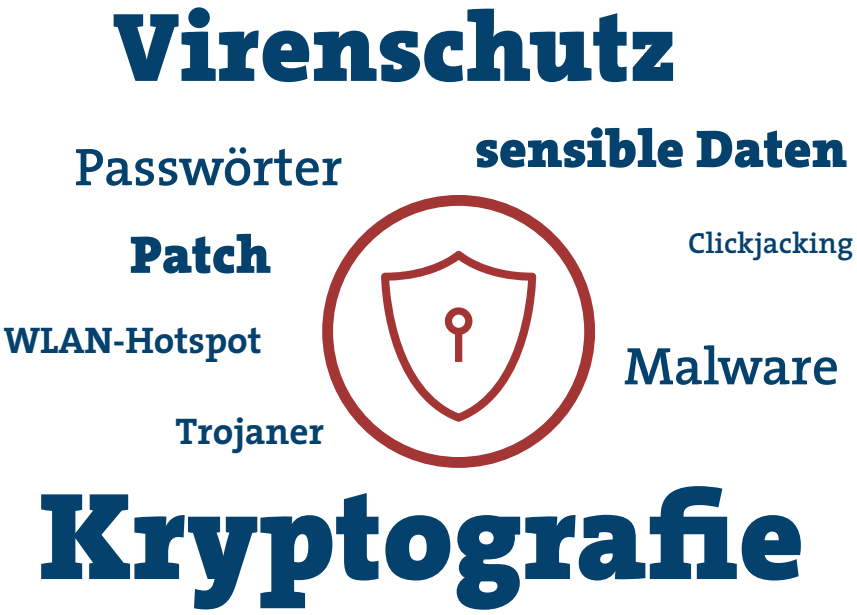
Recht am eigenen Bild:

§78 des UrhG; schützt die Abgebildeten vor ungewollter Veröffentlichung.

Internet-Ombudsmann:

Berät in schwierigen Fällen.

www.ombudsmann.at



Überwachungsskandale, Datenlecks und großflächige Passwortdiebstähle machten überdeutlich, dass die Kommunikation via Internet teilweise nicht so sicher ist, wie es sich Nutzerinnen und Nutzer wünschen würden. Viele möchten sich und ihre Daten besser schützen, fühlen sich dieser (technischen) Herausforderung jedoch nicht gewachsen. Auch, da Sicherheit kein Produkt ist, sondern ein andauernder Prozess, bei dem laufend nachgebessert werden sollte. Dennoch können einfache Maßnahmen gesetzt werden, um die Sicherheit im Internet zu verbessern. Sicherheitsmaßnahmen müssen nämlich nicht kompliziert und unbequem sein – gut implementierte Sicherheit ist einfach und im Idealfall komfortabel.

Sicherheit

Passwörter

Passwörter dienen der Authentifizierung; mit ihnen weisen sich Userinnen und User aus. Passwörter gibt es für E-Mail-Dienste, Onlineprofile in sozialen Netzwerken und mobile Endgeräte – um nur ein paar Beispiele zu nennen. Es ist besonders wichtig, auf die eigenen Passwörter zu achten, diese sicher zu gestalten und regelmäßig zu wechseln. Auch wenn es umständlich und aufwendig erscheint – der beste Tipp für mehr Sicherheit im Internet ist, sichere Passwörter zu verwenden.

Wie können Passwörter die größtmögliche Sicherheit bieten?

- → ***Geheimhaltung:*** *Passwörter sind nur dann effektiv, wenn sie geheim sind. Sie sollten nicht aufgeschrieben und, falls doch, keinesfalls an leicht auffindbaren Orten aufbewahrt werden. Ebenso ist davon abzuraten, anderen Personen seine Passwörter mitzuteilen.*
- → ***Faustregel:*** *Passwörter sollten aus mehr als acht Zeichen bestehen. Vereinfacht gesagt: Je länger das Passwort, umso sicherer ist es.*
- → ***Die üblichen „Verdächtigen“:*** *Viele Userinnen und User wählen ihr eigenes Geburtsdatum, den eigenen Namen oder einfache Zahlenkombinationen. In der jährlichen Sicherheitsanalyse von Passwörtern war auch im Jahr 2013 das häufigste Passwort „123456“, gefolgt etwa von „password“ oder „ilove you“. Solche Passwörter sind besonders unsicher, da sie leicht zu erraten sind und leicht geknackt werden können.*
- → ***Verschiedene Passwörter:*** *Auch wenn es umständlich scheint, so sollten dennoch verschiedene Passwörter zum Beispiel für verschiedene Profile oder Onlinedienste verwendet werden. Denn wird das Passwort eines Profils oder Kontos geknackt, sind bei unterschiedlichen Passwörtern nicht gleich automatisch auch andere Konten betroffen.*
- → ***Regelmäßig das Passwort ändern:*** *Das A und O von Datensicherheit und sicheren Passwörtern ist, diese regelmäßig zu ändern. Immer wieder Passwörter gegen neue auszutauschen ist die beste Empfehlung, um sich und seine Daten zu schützen.*
- → ***Sicherheitsfragen:*** *Manche Webseiten ermöglichen es, bei einem vergessenen Passwort durch sogenannte Sicherheitsfragen (z. B. „Wie lautet der Name des Haustiers?“, „Was ist Ihre Lieblingsspeise?“) dennoch auf das*

eigene Profil zuzugreifen. Diese Sicherheitsfragen bieten Userinnen und Usern die Möglichkeit, sich trotz eines vergessenen Passworts zu authentifizieren. Es sollten jedoch Fragen gewählt werden, die lediglich von den Nutzerinnen und Nutzern selbst beantwortet werden können.

→ ***Passwort-Manager:*** *Spezielle Software, die Kennwörter verschlüsselt speichert und verwaltet. Diese Programme sind aus der Notwendigkeit entstanden, unterschiedliche Passwörter für verschiedene Konten und Onlinedienste zu verwenden, die möglichst lang und sicher sind. Hierbei gibt es ein längeres Passwort für den Passwort-Manager, mit dem alle anderen Passwörter verschlüsselt werden.*

Tipp:
Ein guter Tipp ist, die Anfangsbuchstaben eines einprägsamen Merksatzes als Passwort zu verwenden. Beispielsweise „Ich bin am 28. Februar 1980 geboren" ergäbe das Passwort „Iba28.F1980g".

Sicherheitslücken minimieren

Um Sicherheitsrisiken zu vermeiden, empfiehlt es sich in erster Linie, bekannte Sicherheitslücken zu schließen. Die erste Empfehlung in diesem Zusammenhang ist, die vom Hersteller empfohlenen Software-Updates regelmäßig durchzuführen. Software-Updates enthalten kleine Systemverbesserungen: Sie reparieren Fehler oder schließen eventuelle Sicherheitslücken. Die Herstellerinnen und Hersteller haben, sobald sie Kenntnis über ein (Sicherheits-)Problem bei einem ihrer Produkte erlangen, großes Interesse daran, umgehend zu reagieren, und versuchen, schnell eine Lösung des Problems zu erarbeiten. Beispielsweise kann beim Browser oder anderen Programmen vorgesehen werden, dass sie regelmäßig auf Software-Aktualisierungen hin überprüft oder dass diese automatisch durchgeführt werden.

In einem nächsten Schritt können potenzielle Sicherheitslücken, wie unnötige Plug-ins, entfernt werden. Userinnen und User sollten generell – am besten vor Installation – genau prüfen, ob das ***PLUG-IN*** tatsächlich benötigt wird.

Ebenso prinzipiell vorsichtig sollten Userinnen und User beim Einsatz von Browser-Plug-ins wie Java oder Flash sein. Beides sind Anwendungen, die die Darstellung von multimedialen und interaktiven Inhalten ermöglichen (z. B. Videoclips, Werbebannern, Programmen oder Spielen, die über den Webbrowser laufen). Sind Flash und Java trotzdem im Einsatz, sollten Userinnen und User regelmäßig auf die aktuellste Softwareversion umstellen.

Patch:
(Engl. für flicken, auch Nachbesserung.) Software-Update, das Korrekturen enthält, Fehler behebt oder Sicherheitslücken schließt.

Plug-in:
(Engl. für einstecken, konkret auch Erweiterungsmodul.) Softwaremodul, das zur Erweiterung der Funktionalität einer bestehenden Software eingesetzt werden kann.

Auch gibt es die Möglichkeit, Java und Flash auf den manuellen Einsatz zu beschränken – hierbei fragen Webseiten, die diese Plug-ins benötigen, nach, ob diese verwendet werden sollen.

Ein weiteres Risiko stellen offene WLAN-***HOTSPOTS*** dar. Der eigene mobile Datentarif kann bei intensiver Nutzung und Überstrapazierung teuer werden, gleichzeitig gibt es immer wieder Funklöcher, in denen es weniger guten oder auch keinen Empfang gibt. Hotspots sind hier eine attraktive Alternative, vor allem im Ausland. Viele Userinnen und User verbinden ihre Geräte achtlos mit offenen WLAN-Hotspots und nutzen sie wie gewohnt. Jedoch können hier – vor allem bei unverschlüsselten Verbindungen – Passwörter und Zugangsdaten ausgelesen werden. Oft ist jedoch gar nicht erkennbar, ob die Daten verschlüsselt übertragen werden oder nicht. Um dieses Sicherheitsrisiko ohne großen Aufwand zu verringern, sollten offene WLAN-Hotspots gemieden oder die Nutzung dieser auf ein Minimum reduziert werden, beispielsweise darauf, Online-Artikel zu lesen. Für Onlineshopping sind solche Verbindungen eher nicht geeignet.

Hotspot:
(Engl. für Brennpunkt.) Öffentlicher drahtloser Internetzugriffspunkt.

Schadprogramme (Malware)

Etwa zur Jahrtausendwende brachen die ersten großen Virenepidemien über das Internet herein. „MyDoom", „Sobig" und „Slammer" waren in aller Munde – und in vielen Computern. Mittlerweile ist es um Viren etwas ruhiger geworden, die großen und medienwirksamen Epidemien wurden aber lediglich durch chronische Gefahren ersetzt. Die Schadprogramme sind heute auch nicht mehr zwingend das Produkt von Hackerinnen und Hackern, sondern von organisierten Cyberkriminellen.

Die früheren Generationen von Viren löschten einfach die Festplatte oder gewisse Dateien auf dem verseuchten Rechner und waren fähig, sich eigenständig weiterzuverbreiten. Die neue Generation der ***COMPUTERVIREN, TROJANER, SPYWARE*** oder ***RANSOMWARE,*** tarnt sich als harmloses, nützliches Programm, um so seine Opfer zu täuschen. Im Hintergrund werden jedoch ganz andere Operationen vollzogen, von denen die Nutzerinnen und Nutzer nichts mitbekommen. Anfällig sind Nutzerinnen und Nutzer, die Geräte mit veralteter und somit unsicherer Software verwenden. Regelmäßige Software-Updates sind notwendig, da in diesen oftmals Patches für Sicherheitslücken enthalten sind. Das gilt für Betriebssysteme (z. B. Windows) genauso wie für Internetbrowser (z. B. Firefox, Safari) und Softwareprogramme (z. B. Adobe). Werden sie nicht regelmäßig durchgeführt, setzen sich Nutze-

Malware:
(Engl. für Schadsoftware.) Bösartige Programme, die den Rechner oder das Betriebssystem angreifen, Daten stehlen oder diese an Dritte übertragen.

Trojaner:
Software, die sich als harmloses, nützliches Programm tarnt und dabei im Hintergrund ohne das Wissen von Nutzerinnen und Nutzern andere Operationen vollzieht.

Spyware:
(„Spy“, Engl. für Spion.) Software, die ohne das Wissen oder die Zustimmung von Nutzerinnen und Nutzern Daten ausspäht und diese an Dritte übermittelt.

Computervirus:
Software, die sich eigenständig vermehren und verbreiten und dabei Hardware, Software oder Betriebssysteme angreifen und verändern kann.

Ransomware:
(„Ransom“, Engl. für Lösegeld.) Software, mit der der Zugriff oder die Nutzung von Daten oder Computern verhindert oder verschlüsselt wird; für die Freigabe oder Entschlüsselung wird Lösegeld gefordert.

Clickjacking:
(Engl. für Klickeintreibung.) Mit Täuschungsabsicht gestaltete Internetseiten oder Klickflächen, die echte Webseiten oder Klickflächen überlagern, um Nutzerinnen und Nutzer in die Irre zu führen.

rinnen und Nutzer einem unnötigen Sicherheitsrisiko aus, da ihre Geräte (eher) für Schadsoftware angreifbar sind.

Nutzerinnen und Nutzer können sich vor diesen ungeliebten Schadprogrammen schützen, indem sie beispielsweise keine Mail-Anhänge von fragwürdigen Quellen öffnen, Programme nur von vertrauenswürdigen Quellen downloaden oder ihre Smartphone-Apps von den offiziellen App-Stores beziehen (Google Playstore für Android, App Store für iOS oder Windows Store für Windows Phone). Insbesondere sollten Nutzerinnen und Nutzer bei fragwürdigen Download- und Streaming-Webseiten aufpassen, denn hier tummelt sich oft Malware, die z. B. als Software (z. B. ein Videoplayer oder Donwload-Manager) getarnt ist. Obwohl es keinen hundertprozentigen Schutz vor Schadsoftware geben kann, ist die Reduktion von Gefahren und Risiken der erste Schritt zu mehr Sicherheit.

Malware und andere Sicherheitsrisiken verbreiten sich auch immer mehr über soziale Netzwerke, beispielsweise über Facebook. Nutzerinnen und Nutzer, die auf Links von „schockierenden“ Videos klicken, einschlägige Webseiten besuchen oder Facebook-Add-ons herunterladen, die versprechen, die Farbe der Chronik zu ändern oder diese überhaupt vollständig zu entfernen, sind leider der traurige Klassiker von Malware. Durch die Klicks oder Downloads kann schlimmstenfalls das Konto von fremder Seite übernommen werden, und ohne das Zutun der Userinnen und User wird in ihrem Namen gespammt, gepostet und verlinkt – mit dem Ziel, die Freundinnen und Freunde in die gleiche Falle zu locken. Besonders gefälschte Spiele und Seiten machen sich dieses System zunutze.

Eine weitere beliebte, ähnliche Betrugsmethode ist ***CLICKJACKING***. Hierbei werden Schalt- und Klickflächen mit einer Täuschungsabsicht gestaltet; nichts ahnende Nutzerinnen und Nutzer klicken auf einen scheinbar harmlosen Link und bewerten plötzlich zum Beispiel unwissentlich eine dubiose Fanseite mit „Gefällt mir“.

Achtung:
Malware kann man sich nicht nur im Internet holen. Ein Sicherheitsrisiko sind infizierte Endgeräte, die das eigene „anstecken“ (beispielsweise über USB-Verbindungen), oder ***USB***-Sticks. Über eine USB-Schnittstelle können verschiedene Geräte an einen Computer angeschlossen werden (z. B. Maus, Tastatur, USB-Sticks). Die Malware liegt dabei in den kontaminierten Geräten verborgen. Wird etwa ein infizierter USB-Stick an den Computer an-

geschlossen (z. B. BadUSB), kann die Schadsoftware ohne Zutun übertragen werden; es kommt zu Datenverlust, technischen Störungen, „Nach-Hause-Telefonieren“ (Übertragung von Daten an Dritte) bis hin zum Kontrollverlust über das Gerät. Daher ist es ratsam, keine unbekannten (z. B. gefundenen) USB-Sticks an den eigenen Computer anzustecken.

Virenschutz

Eine ***VIRENSCHUTZ***-Software ist ein Programm, das Daten auf Viren, Würmer, Spyware und Trojaner, also generell auf Malware prüft und diese blockiert. Prinzipiell wird zwischen drei Arten von Virenscannern unterschieden: Echtzeitscanner, manuellem Scanner und Online-Virenscanner.

Ein Echtzeitscanner ist eine installierte Software, die im Hintergrund aktiv ist und Dateien und Programme auf Malware scannt und beim Finden einer solchen die Userin oder den User darauf aufmerksam macht; der Echtzeitscanner eignet sich besonders zum präventiven Schutz eines Systems.

Manuelle Scanner müssen – wie ihr Name verrät – manuell von den Nutzerinnen und Nutzern gestartet werden, beispielsweise, wenn ein Mail-Attachment downgeloadet und geöffnet werden soll.

Bei einem Online-Virenscanner braucht der Rechner eine Internetverbindung, die Virenmuster werden online abgeglichen. Ist das Gerät jedoch tatsächlich von Viren befallen, ist gerade die Internetverbindung nicht ohne Risiko, da hier das Gerät ferngesteuert werden kann, um beispielsweise Spam zu verschicken oder andere Rechner anzugreifen. Es empfiehlt sich daher, ein potenziell infiziertes Gerät offline zu nehmen und mit einem Offline-Virenscanner zu untersuchen.

Achtung:
Nutzerinnen und Nutzer müssen sich bewusst sein, dass ein Virenscanner nur gegen bereits bekannte Schadsoftware oder Schadlogiken etwas ausrichten kann; somit kann kein absoluter Schutz garantiert werden. Virenscanner sind dennoch eine sehr gute Ergänzung zu sonstigen Sicherheitsmaßnahmen.

Sensible Daten

Der wichtigste Tipp in diesem Zusammenhang ist, die eigenen schutzwür-

USB bzw. Universal Serial Bus:

Ein Bus ist ein System zur Datenübertragung zwischen mehreren Teilnehmerinnen oder Teilnehmern über einen gemeinsamen Übertragungsweg (= Schnittstelle). Mit USB ausgestattete Medien können bei laufendem Betrieb miteinander verbunden werden, die angeschlossenen Geräte werden automatisch erkannt.

Virenschutz:

(Auch Virenscanner oder Antivirenprogramm genannt.) Software, die Computerviren und andere Schadprogramme aufspürt, blockiert und beseitigt.

digen Zugangsdaten nicht weiterzugeben (z. B. Zugangsdaten für Finanzonline.at). Möchten Nutzerinnen und Nutzer sie dennoch weitergeben, beispielsweise an die Partnerin oder den Partner, sollte dies persönlich geschehen. Besteht ein triftiger Grund dafür, sie schriftlich zu übermitteln, sollten Log-in-Daten getrennt voneinander übermittelt werden (z. B. Username per E-Mail und Passwort telefonisch).

Um sensible Daten, die per E-Mail versandt werden sollen, zu schützen, können sie als passwortgeschützte PDFs im Anhang übermittelt werden. Dies ist bei der Erstellung von PDFs auf Basis eines Word-Dokuments unter Datei > Vorbereiten > Dokument verschlüsseln möglich.

Werden sensible oder private Daten auf einem USB-Stick oder anderen Wechseldatenträgern (z. B. auf einer externen Festplatte) weitergegeben, sollten sie unbedingt verschlüsselt werden, um beispielsweise Datenmissbrauch bei Verlust des Geräts zu verhindern; ein kleiner USB-Stick kann schnell einmal verloren gehen. Für Windows-Systeme kann zum Beispiel die Verschlüsselungssoftware BitLocker to go empfohlen werden.

Kryptografie

Kryptografie:
(„Kryptós", Altgr. für geheim, und „gráphein", Altgr. für schreiben.) Verschlüsselung von Informationen; ist Teil der Kryptologie, der Wissenschaft von der Informationssicherheit.

Verschlüsselung und kryptografische Verfahren gewinnen als eine Möglichkeit des Daten- und Privatsphärenschutzes mehr und mehr an Gewicht. Userinnen und User sollten sich nicht von diesen Begriffen einschüchtern lassen, denn es gibt einfache Sicherheitsmaßnahmen, die nicht unbedingt großes technisches Vorwissen voraussetzen. Viele Dienste bieten einfache Lösungen für technisch durchschnittlich kompetente Userinnen und User an.

Es gibt verschiedene Wege, die eigene E-Mail-Kommunikation zu sichern. Eine Option, um den eigenen Mail-Account zu schützen, ist es, diesen auf Verschlüsselung umzustellen. Der Sicherheitsmodus heißt je nach Anbieterin oder Anbieter unterschiedlich, beispielsweise „SSL" oder „verschlüsselte Verbindung". Diese Einstellungen können bei den erweiterten Kontoeinstellungen vorgenommen werden, doch nicht alle E-Mail-Dienste bieten eine Möglichkeit durchgängiger Verschlüsselung an.

Eine weitere Option ist, auf Mail-Dienste umzusteigen, die verschlüsselte Kommunikation unterstützen (z. B. ProtonMail). Einige von diesen Diensten bieten auch die Möglichkeit an, dass nicht nur die Nachrichten selbst verschlüsselt werden, sondern es auch eine Signatur gibt, die die Authentizität

der Absenderin oder des Absenders belegt.
Möchten Nutzerinnen und Nutzer auf keinen neuen Mail-Dienst umsteigen, können sie entsprechende Software einsetzen. Zur Sicherung der eigenen E-Mail-Kommunikation, aber auch zur Verschlüsselung der eigenen Daten empfiehlt sich beispielsweise die freie Software Gpg4win (für Windows). Das Herzstück, Gnu Privacy Guard, erledigt die kryptografischen Operationen, also das Ver- und Entschlüsseln von Nachrichten, wie auch das Erzeugen und Überprüfen von elektronischen Signaturen. Für Mac OS X empfiehlt sich GPGTools.

Achtung:
Obwohl es mittlerweile einige verhältnismäßig einfache Lösungen gibt, wird für die Implementierung von Verschlüsselungssoftware oder dergleichen ein technisches Grundverständnis notwendig sein. Es empfiehlt sich daher, dass sich weniger versierte Nutzerinnen und Nutzer Unterstützung holen oder sich (zusätzlich) über die verschiedenen Verschlüsselungsarten informieren.

Kinder-profile

Alters-empfehlungen

Positivlisten

soziale Netzwerke

Computerspiele

Apps

Smartphones

Medien-kompetenz

Drei Viertel aller Jugendlichen haben Zugang zu Computern mit Internetanschluss und nutzen diesen am liebsten zum Internetsurfen, Computerspielen und Musikhören. Um sich mit Freunden zu verabreden, die Hausaufgaben zu erfragen oder schnell den Eltern Bescheid zu geben – hierfür wird das Handy genutzt. Viele Kinder und Jugendliche besitzen dafür auch ein eigenes Gerät: 72 Prozent der 12- bis 19-Jährigen besitzen ein Smartphone, aber auch in der Kategorie der Jüngeren, bei den 6- bis 10-Jährigen, liegt der Handyanteil bereits bei 40 Prozent. Besonders die Kommunikation per SMS, Instant Messenger und über soziale Netzwerke ist populär.
Quelle: 4. Oö Kinder-Medien Studie 2014 & JIM-Studie 2013

Kinder, Teenager & Medien

(Elterliche) Medienkompetenz

Sicherheit für Kinder und Jugendliche in der Online-Welt wird ein immer wichtigeres Thema, da immer mehr Kinder und Jugendliche immer früher das Internet nutzen. Wie bei allen Medien müssen sie aber die Anwendung und vor allem den sicheren Umgang damit erst lernen. Auch wenn die neue Generation der „Digital Natives" sehr gerne – vor allem medial – als Generation verstanden wird, die den Umgang mit allen digitalen Medien von Kindesbeinen an und quasi automatisch erlernt, ist das nicht der Fall. Kinder wachsen heutzutage zwar mit einer Vielzahl an mobilen Endgeräten, dem Internet und anderen digitalen Gadgets auf, dies bedeutet aber nicht, dass sie keine Unterstützung dabei brauchen; im Gegenteil, es ist heute noch mehr als früher notwendig, dass Eltern ihre Kinder dabei unterstützen, die richtigen Verhaltensweisen zur sicheren Internet- und Gerätenutzung zu erwerben.

Bis 3 Jahre

Damit Kinder beim Erwerb der wichtigen digitalen Kompetenzen am besten unterstützt werden können, ist es sehr wichtig zu akzeptieren, dass Eltern eine wichtige Vorbildfunktion haben. Kinder ahmen das Computer-, Smartphone-, Tablet- und generelle Medienverhalten der Eltern und großen Geschwister nach. In diesem Zusammenhang bietet es sich an, gemeinsam mit dem Kind praktische Erfahrung zu sammeln, sich zusammen mit dem Computer zu beschäftigen (z. B. tippen Kinder sehr gerne auf Tastaturen oder Tablet-Oberflächen). So können Kinder langsam an die Welt der digitalen Medien herangeführt werden. Beispiele für solch eine Mediennutzung sind, gemeinsam kinderfreundliche Webseiten zu besuchen oder ein kurzes Video auf YouTube anzuschauen. Wichtig ist aber, dass die Kinder nicht überfordert werden. Kleinkinder sollten nicht unbeaufsichtigt mit Computern, Tablets oder Handys hantieren.

4–6 Jahre

In diesem Alter kann das Interesse durch Lern- und Spielprogramme geweckt werden, in diesem Bereich gibt es viele Angebote, die Kinder gefahrlos nutzen können. Dennoch empfiehlt es sich, Kinder beim Vertrautmachen nicht unbeaufsichtigt zu lassen und sie beim Besuch von

Fragen und Antworten für Eltern:

www.saferinternet.at/fuer-eltern

Saferinternet.at-Elternratgeber:

www.saferinternet.at/broschuerenservice

ISPA Kinderbuch: „Der Online-Zoo"

Kostenloser Download unter www.ispa.at/kinderbuch

Sicher mehr Spaß!

UPC Fiber Power Internet macht allen Spaß:
vom Single bis zur Großfamilie.

0800 700 767 oder upc.at

More power. More joy.

upc

(kinderfreundlichen) Webseiten zu begleiten, wobei sie nun die Navigation übernehmen können, um selbstständig Videos anzuklicken oder zu scrollen. Kinder, die noch nicht lesen und schreiben können, orientieren sich eher an Bildern und brauchen daher Webseiten mit grafisch aufbereiteten Oberflächen. Eine weitere Möglichkeit ist, medienpädagogisch aufbereitete Bücher oder andere Inhalte zu lesen, da diese die kleinen Nutzerinnen und Nutzer spielerisch und altersgerecht ans Internet und an Medien heranführen (z. B. ISPA-Kinderbuch „Der Online-Zoo").

7–11 Jahre

In diesem Alter wird es zunehmend interessant, das Internet zu entdecken. Kinder informieren sich gerne über ihre Hobbys, die Filme, die ihnen gefallen, oder sie möchten ihre Lieblingsmusik hören. Auch die Kommunikation mit Freundinnen und Freunden per Chat oder Handy wird attraktiv. Auch in diesem Alter sind altersgerechte Webseiten empfehlenswert. Sie können mit einem Lesezeichen markiert werden, damit Kinder einen leichten Zugang zu ihnen haben. Besonders im frühen Schulalter sollten langsam die Fähigkeiten zur kompetenten Internetnutzung aufgebaut und beispielsweise gelernt werden, wie Suchmaschinen genutzt werden können. Als Einstieg eignen sich kinderfreundliche Suchmaschinen, die nur redaktionell geprüfte Inhalte in den Ergebnissen anzeigen (z. B. www.fragfinn.de). Werden anschließend „echte" Suchmaschinen wie Google oder Bing verwendet, kann es nützlich sein, diese in den kindersicheren Modus („SafeSearch") zu schalten, sodass ungeeignete Inhalte (z. B. Pornografie) nicht angezeigt werden. Auch das gezielte Recherchieren zu spannenden Themen oder den eigenen Interessen im Internet kann sich anbieten, um mit Kindern zu üben, wie sie mit der großen Fülle an Informationen im WWW umgehen können. Ein Tipp ist beispielsweise, den Kindern zu zeigen, wie sie zielgerichtet nach Informationen suchen können: Anstatt nach allgemeinen Begriffen wie „Feuerwehr" zu suchen, sollte die Suchanfrage möglichst präzisiert werden,beispielsweise zu „Feuerwehrauto" oder „Ausbildung Feuerwehr". Ebenso ist es notwendig, mit Kindern darüber zu sprechen, dass nicht alle Informationen im Internet auch wahr und richtig sind. Besonders jüngere Kinder können noch nicht zwischen glaubwürdigen und unglaubwürdigen Quellen oder Werbeinhalten unterscheiden und glauben oft alles, was im Internet steht. Dass Kinder erst die Fähigkeit, Informationen zu bewerten, lernen müssen, zeigt sich besonders am Beispiel von Kettenbriefen („Schicke diese Nachricht an zehn Menschen weiter, sonst …"), die ihnen im schlimmsten Fall wirklich große Angst machen können. Es ist daher notwendig, mit Kindern darüber zu sprechen, dass nicht alles, worauf sie im Internet stoßen, wahr und glaubwürdig ist.

Tipp:

Sendung mit dem Elefanten

www.wdrmaus.de/elefantenseite

Empfehlenswerte Kinderapps:

www.kinderapps.info

www.iphonekinderapps.de

www.bestekinderapps.de

Suchmaschinen für Kinder:

www. blindekuh.de

ww.fragfinn.de

ISPA Broschüre: „Das Internet für 1 bis 11"

Tipps für altersgerechte Webseiten

Kostenloser Download unter www.ispa.at/internetfür1bis11

Ab 12 Jahre

Die meisten Kinder in diesem Alter besitzen bereits ein eigenes internetfähiges Smartphone mit einem Datentarif und sind in den meisten Fällen regelmäßig im Internet unterwegs. Nun werden Videos angeschaut, es wird auf verschiedene Arten und über die verschiedensten Online-Dienste mit Freundinnen und Freunden kommuniziert – das Internet wird und mobile Endgeräte werden auf täglicher Basis genutzt. Die Zeit, die Kinder damit verbringen, nimmt immer mehr zu, was in manchen Fällen auch zu einer finanziellen Belastung werden kann. Daher müssen geeignete Handy- und Internetverträge abgeschlossen oder (konsequente) Regeln zur Nutzung aufgestellt werden. Bald überholen die Kinder auch ihre Eltern in der Internetkompetenz und nutzen Dienste, von denen Erwachsene noch gar nicht gehört haben, oder tun Dinge mit dem Handy, bei denen sich die Eltern nur verwundert den Kopf kratzen. Dann gilt es für Eltern, einen kühlen Kopf zu bewahren! Verbote, Sperren und anlassloses Kritisieren funktionieren wenig bis gar nicht. Vor allem heimliche Kontrollen der Geräte können als Vertrauensbruch empfunden werden. Auch Kinder haben ein Recht auf Privatsphäre, das respektiert werden sollte. Gibt es keine Vertrauensbasis, fragen Kinder in tatsächlichen Ernstfällen nicht um Hilfe, weil sie sich vor den Konsequenzen fürchten. Eltern können stattdessen punkten, indem sie für die Mediennutzung ihrer Kinder aufgeschlossen sind und interessiert nachfragen oder sich bei technischen Fragen von ihnen unterstützen lassen.

Filterprogramme

?

Positivlisten:
Vorher festgelegte Webseiten, die erlaubt sind.

Negativlisten:
Vorher festgelegte Webseiten, die verboten sind.

Es gibt verschiedene kommerzielle Filterprogramme, die damit werben, den Computer bzw. den Zugang zum Internet kindersicher zu gestalten. Diese Programme verwenden dabei eine Mischung aus ***POSITIVLISTEN*** und einer Sperre aufgrund diverser Stichwörter (z. B. Nazi, Porno). Zum Teil wird auch die Verwendung anderer Programme auf dem Computer eingeschränkt. Diese Filterprogramme bzw. deren Standards funktionieren jedoch nicht für jede Familie gleich. Welche Seiten ein Kind einer bestimmten Altersstufe sehen darf und welche nicht, ist nicht nur vom familiären, sondern auch vom kulturellen Umfeld abhängig. Zusätzlich werden mit dem Erwerb dieser Programme auch die Wertehaltungen der Unternehmen, die diese Software herstellen, mitgekauft. Es ist bei Produkttests beispielsweise schon öfter vorgekommen, dass gerade Aufklärungsseiten, die sich an Jugendliche richten, vom Filter blockiert wurden (dies ist auch beim berühmten Pornofilter in Großbritannien der Fall – ein großer Kritikpunkt). Filterprogramme bieten auch nur einen beschränkten Schutz, bei E-Mails, Tauschbörsen oder Chats

können sie nicht angewendet werden. Auf jeden Fall gilt aber, dass Filtersoftware kein Allheilmittel ist und auch nicht die Medienbildung ersetzen kann.

Kinderkontrolle per App

Immer mehr Eltern setzen Apps und andere Hilfsmittel ein, um das Medien- und Online-Verhalten ihrer Kinder zu kontrollieren. Mit der Verbreitung von mobilen Endgeräten – vor allem von Smartphones – bei Kindern ist es nicht überraschend, dass auch das Angebot an Kontrollapps immer weiter zunimmt. Auf der einen Seite sorgen sich Erziehungsberechtigte um ihren Nachwuchs und möchten kontrollieren, was die Kinder tun oder wo sie sich befinden, auf der anderen Seite müssen Eltern akzeptieren, dass auch Kinder ein Recht auf Privatsphäre haben und nicht bei den Ausflügen ins Netz überwacht werden sollten.

Dabei gibt es durchaus sinnvolle Apps, die der Familienvernetzung dienen und beispielsweise über GPS-Lokalisierung darüber informieren, ob der Nachwuchs gut nach Hause gekommen ist. Viele Smartphones bieten zudem eigene Kinderprofile an, bei denen die Nutzung von Handybezahlung, In-App-Kauf oder der Datenverbrauch eingeschränkt werden können, sodass das Handy für die jüngeren Nutzerinnen und Nutzer eingerichtet werden kann. Andere Apps bieten SOS-Knöpfe oder -Nachrichten, versetzen das Smartphone ab voreingestellter Uhrzeit in den Schlafmodus und empfangen keine Anrufe und SMS mehr, um einen ruhigen Schlaf zu ermöglichen, oder beobachten das Download- und Spieleverhalten der Kinder. Eher extrem ist das Sperren des Handys per Fernsteuerung, wenn der Nachwuchs nicht auf Anrufe reagiert. Erst, wenn sich der Nachwuchs meldet und der elterliche Freischaltcode eingegeben wird, kann das Smartphone wieder benützt werden.

Ob, wann und in welchem Ausmaß diese Hilfsmittel zum Einsatz kommen sollten, muss im Einzelfall beantwortet werden. Eltern sollten sich jedoch bewusst sein, dass nur in den wenigsten Fällen das Medienverhalten der Kinder derart extrem und risikofreudig ist, wie es in den Medien dargestellt wird. Zudem brauchen auch Kinder Privatsphäre und Freiraum, um den Umgang mit ihrem Smartphone oder anderen Geräten erlernen zu können. Je älter Kinder sind und je häufiger und eigenständiger sie sich im Internet bewegen, desto wirkungsloser werden Filter und andere technische Lösungen. Vor allem kann Medienerziehung nicht an Programme delegiert werden. Es ist daher absolut notwendig, dass Eltern und Erziehungsberechtigte mit ihren Kindern über

Kinderfreundliche Einstellungen für Smartphones und Tablets (Apple, Android, BlackBerry, Windows):
www.ispa.at/smartphone

GPS-Lokalisierung:
App „Family Locator“

Kinderprofile:
„Einschränkungen“ bei iPhones, App „Kids Place“ oder „Care 4 your child“ für Android

SOS-Hilferuf:
App „Protegon SOS“

Nachtruhe:
App „Peace of Mind“ für Android, „Nicht stören“-Einstellungen bei iPhones

Rückrufzwang:
App „Ignore no more“

das Internet, ungeeignete Inhalte und Online-Gefahren sprechen. Denn es wird immer wieder neue Online-Dienste und -herausforderungen geben, die zumindest anfänglich nicht moderiert oder reguliert werden. Verbote und die elterliche Opposition bewirken bei Kindern und Jugendlichen oft genau das Gegenteil von dem, was erreicht werden soll. Eltern sollten offen und nicht „besserwisserisch" auf ihre Kinder zugehen, um gemeinsam über das Online-Verhalten und sinnvolle Regeln zu sprechen. Medienerziehung kann in den Alltag eingebaut werden und auch nebenbei passieren. Besonders sollten Eltern und ältere Geschwister bedenken, dass sie eine Vorbildfunktion haben, denn Kinder ahmen gerne das Verhalten von Älteren nach.

Wichtig ist, in ständiger Kommunikation miteinander zu stehen. Eltern sollten regelmäßig beim Nachwuchs nachfragen, wie es um das Online-Verhalten steht: Somit zeigen sie nicht nur Interesse und bauen eine Vertrauensbeziehung auf, sondern sind auch informiert und erfahren, was die neuesten Online-Trends sind. Kommen Kinder mit Fragen oder Problemen, gilt es, besonders aufmerksam zu sein. Beispielsweise ist ein beliebter Satz, um auf schwierige Situationen hinzuweisen: „Meine Freundin / mein Freund hat …". Hier handelt es sich weniger um eigene Erfahrungen, die verschleiert werden, sondern tatsächlich um Erfahrungen von anderen, die große Betroffenheit auslösen. Besonders solche Aussagen sollten ernst genommen werden. Denn mit einer Vertrauensbeziehung kann garantiert werden, dass sich Kinder in schwierigen Situationen an ihre Eltern wenden oder sich anderswo Hilfe holen.

Computerspiele

Jugendschutzeinstellungen:
Xbox:
goo.gl/77v4Pn
Nintendo:
goo.gl/ApvnBp
Sony Playstation:
goo.gl/sIiKLd

Empfehlenswerte altersgerechte Spiele:
von BuPP:
www.bupp.at

Das Spielen der Kinder am Bildschirm weckt häufig Sorgen bei Eltern. Sie sind unsicher, welche Auswirkungen das Spielen auf die Kinder haben könnte und in welchem Ausmaß sie das zulassen sollten. Für die kleinsten Spielerinnen und Spieler gibt es beispielsweise bei Spielkonsolen Jugendschutzeinstellungen.

Bei Computerspielen können sich Eltern vorab informieren, ob diese für ihre Kinder infrage kommen. Die Bundesstelle für die Positivprädikatisierung von Computer- und Konsolenspielen (BuPP) testet Spiele und gibt (Alters-)Empfehlungen über gute Computerspiele ab, die nach verschiedenen Kriterien beurteilt werden.

Besonders beliebt ist aktuell auch Social Gaming, das sind Online-Spiele, die direkt über den Internetbrowser gespielt werden. Bekannt wurde Social Gaming im Zusammenhang mit sozialen Netzwerken, auf denen sie sich

rasant verbreiteten („Clash of Clans“, „Candycrush“, „MobWars“) und auch Erwachsene begeistern konnten. Die meisten dieser Spiele sind gratis, auf den zweiten Blick werden aber ein paar Nachteile sichtbar. Sie erfordern einen großen Zeitaufwand und über ein „Belohnungssystem“ werden die Spielerinnen und Spieler möglichst eng an das Spiel gebunden, indem sie für verschiedene Tätigkeiten oder das Bewerben Guthaben („Credits“) gutgeschrieben bekommen. Dieses „Spielgeld“ kann gegen Leistungen des Spiels eingetauscht werden, beispielsweise schnelleres Vorankommen in den einzelnen Level. Mit dem Guthaben wird also besonders regelmäßiges und wiederkehrendes Online-Verhalten belohnt, es kann aber – natürlich – auch käuflich erworben werden. Oft gibt es auch kostenpflichtige Mitgliedschaften, Abos oder virtuelle Premiumartikel, die nur mit echtem Geld gekauft werden können. Besonders jüngere Kinder können dieser Versuchung oft nicht widerstehen und können ein Suchtverhalten entwickeln.

Tipps für Eltern:

www.saferinternet.at/computerspiele/social-gaming-elterntipps

Soziale Netzwerke

Es ist nichts Neues, dass Kinder und Jugendliche gerne über soziale Netzwerke in Verbindung treten. Die Frage, ob und ab wann Eltern ihren Kindern erlauben sollten, soziale Netzwerke zu nutzen, kann nicht pauschal beantwortet werden. Wichtig ist jedoch, mit den Kindern über mögliche Risiken zu sprechen, besonders jüngere Kinder sind sich der möglichen Implikationen und Gefahren nicht bewusst. Vor allem in Bezug auf den Umgang mit den eigenen persönlichen Daten sollten Kinder sensibilisiert werden.
Die meisten dieser Plattformen haben Nutzungsbedingungen, in denen sie sich in unterschiedlichem Ausmaß dem Daten- und Privatsphäreschutz ihrer Nutzerinnen und Nutzer verpflichten. Auch haben die meisten dieser Online-Dienste ein Mindestalter für ihre Nutzerinnen und Nutzer festgelegt, das Kinder und Jugendliche aber durch die Angabe eines falschen Geburtsdatums gerne umgehen. Das Mindestalter bei Facebook ist derzeit bei 13 Jahren angesetzt.

Es ist auf jeden Fall zu empfehlen, gemeinsam mit dem Kind über die Privatsphäre-Einstellungen zu sprechen oder diese gemeinsam festzulegen. Eine wichtige Funktion, von der unbedingt Gebrauch gemacht werden sollte, ist die Schaltung des Profils auf „nicht öffentlich“, wodurch es nicht von Suchmaschinen gefunden werden kann.

Weiters gibt es bei Facebook die Option, dass Fotos und Statusmeldungen beispielsweise nur mit den Freunden geteilt werden. Standardmäßig sind

Klarname:
Auch engl. „Realname", ist der wirkliche Name einer Person, der auch in amtlichen Dokumenten geführt wird.

Alterseinschränkungen für Google-Dienste:
goo.gl/jTVPx6

Tipps zu den Privatsphäre-Einstellungen für jugendliche Nutzerinnen und Nutzer in verschiedenen sozialen Netzwerken:
www.saferinternet.at/privatsphaere-leitfaeden

Rat auf Draht:
Tel: 147
www.rataufdraht.orf.at

die Einstellungen der Privatsphäre bei Facebook für Jugendliche im Alter von 13 bis 17 Jahren voreingestellt auf „Freunde", bei allen anderen Facebook-Nutzerinnen und -Nutzern sind sie vorerst automatisch „öffentlich". Auch empfiehlt es sich für Kinder, nicht den eigenen Namen ***(„KLARNAMEN")*** zu verwenden, sondern einen Nickname oder eine leicht abgeänderte Version des eigenen Namens, statt „Susanne Musterfrau" könnte beispielsweise „Susi Musterfrau" gewählt werden.

Für alle Google-Dienste (YouTube, Gmail, Picasa etc.) wird ein Google-Konto benötigt. Die Alterseinschränkung für ein Google-Konto liegt bei 13 Jahren, jedoch gelten nicht überall dieselben Regeln. In den Niederlanden müssen Userinnen und User mindestens 16 Jahre alt sein, um ein Google-Konto eröffnen zu können, für den Dienst Google Wallet gilt die Alterseinschränkung ab 18 Jahren.

Cybermobbing

Studien bestätigen, dass Cybermobbing nicht nur Teil des Sprachgebrauchs geworden ist, sondern auch des jugendlichen Alltags. Regelmäßig wird auch in den Medien über das Thema berichtet. Das erhöht die Aufmerksamkeit und Sensibilität für diese Gefahr und trägt zur Früherkennung bei. Allerdings ist hier auch Vorsicht geboten: Nicht jeder (kleine) Konflikt zwischen Jugendlichen fällt gleich in die Kategorie Cybermobbing.
Jedoch hat Mobbing mit dem Internet einen neuen Tatort gefunden: beleidigende Kommentare in sozialen Netzwerken, gemeine Fake-Profile, beschämende Videos auf YouTube, Terror über Instant-Messenger-Dienste – um nur einige Beispiele zu nennen. Cybermobbing findet rund um die Uhr statt, hat ein großes Publikum und verbreitet sich rasend schnell, während die Täterinnen und Täter auf einfache Art anonym bleiben können. Gleichzeitig sind die Rollen nicht klar verteilt und können sich sehr schnell umkehren: Opfer werden aus Rache zu Angreifern und Täterinnen oder Täter sind plötzlich selbst betroffen.

In die Novelle des Strafgesetzbuches 2015 wurde eine neue Bestimmung aufgenommen, die Fälle von Cybermobbing explizit unter Strafe stellt. Durch dieses Delikt sind Verletzungen der Ehre oder des höchstpersönlichen Lebensbereichs erfasst, die durch das Aussenden, Empfangen sowie Übermitteln von Nachrichten aller Art, insbesondere E-Mails, SMS und Anrufe, aber auch Postings oder Nachrichten in sozialen Medien erfolgen. Dabei muss die Tathandlung für eine größere Zahl von Menschen (mind. 10 Personen) wahr-

nehmbar sein. Wie lang die Belästigung dauern oder wie oft die Tathandlung wiederholt werden muss, um das Delikt der „fortgesetzten Belästigung" zu erfüllen, ist im Einzelfall zu beurteilen; jedenfalls sind aber wiederholte Tathandlungen erforderlich. Bei massiven Verstößen hingegen, wie beim unerlaubten Posten von Nacktbildern im Internet, könnte unter Umständen bereits eine einmalige Begehung ein strafrechtliches Nachspiel haben.

Die Täterin oder der Täter hat in Hinkunft dabei entweder mit einer hohen Geldstrafe – bis zu 720 Tagessätzen – oder mit einer Freiheitsstrafe bis zu einem Jahr zu rechnen. Sofern die Tat zum Selbstmord oder zum Selbstmordversuch des Opfers führt, droht eine Freiheitsstrafe bis zu drei Jahren.

Was tun im Ernstfall?

- → ***Verständnis zeigen:*** *Berichten Kinder über Cybermobbing, sollte ihnen unbedingt Glauben geschenkt und Unterstützung geboten werden.*
- → ***Beweise sichern:*** *Screenshots und Kopien der beleidigenden Bilder, Postings und Chats machen. Mit Beweisen kann besser um Hilfe gebeten werden, und die Täterinnen und Täter können leichter gefunden und überführt werden.*
- → ***Postings löschen:*** *Geschieht die Verunglimpfung in sozialen Netzwerken oder auf anderen öffentlichen Plattformen, unbedingt diese sofort löschen lassen. Viele soziale Netzwerke haben hierfür eine eigene Meldefunktion.*
- → ***Privatsphäre schützen:*** *Sichere Privatsphäre-Einstellungen sind ein guter Anfang, um Attacken zu vermeiden. Beispielsweise auf Facebook kann vorgesehen werden, dass Verlinkungen auf Fotos nicht ohne Zustimmung der Nutzerin oder des Nutzers vorgenommen werden können.*
- → ***Die eigenen Rechte kennen:*** *Das „Recht am eigenen Bild" sieht vor, dass niemand ohne die Erlaubnis der Abgebildeten oder des Abgebildeten Fotos veröffentlichen darf, besonders, wenn sie bloßstellender Natur sind.*

Cybergrooming

Cybergrooming ist nach §208a StGB mit bis zu 2 Jahren strafbar.

goo.gl/HRff2q

Beim Cybergrooming erschleichen sich (überwiegend männliche) Erwachsene im Internet das Vertrauen von Kindern und Jugendlichen, mit dem Ziel der Anbahnung von sexuellen Kontakten. Hierbei geben sich die Erwachsenen oft als Gleichaltrige aus, zunehmend machen die Groomer aber aus ihrem Alter kein Hehl mehr und versuchen, sich direkt den Minderjährigen zu nähern. Groomer kontaktieren Jugendliche und versuchen, Vertrauen aufzubauen. Ist ein Kontakt hergestellt, versuchen sie, möglichst viele Informationen über die Minderjährigen zu bekommen, sie durch Schmeicheleien und vielleicht sogar Geschenke an sich zu binden und zuletzt zu freizügigen Fotos, einem Videochat, in dem sexuelle Handlungen simuliert werden sollen, oder sogar zu einem Treffen zu überreden.
Cybergrooming ist seit längerer Zeit Thema. Viele Jugendliche denken, dass nur besonders „naive" Userinnen und User Groomern zum Opfer fallen können. Eltern denken wiederum, dass jedes Kind gefährdet ist. Doch wo liegt die Wahrheit? Cybergrooming ist kein Einzelphänomen, kommt aber seltener vor, als beispielsweise durch Medienberichterstattung glaubhaft gemacht wird. Viele Jugendliche sind für dieses Thema sensibilisiert und wissen, dass sich im Internet Erwachsene und auch Groomer bewegen, und sie wissen auch, bei welchen Online-Diensten sie diesen eher begegnen können.

Wie können Groomer erkannt und abgewehrt werden?

- → ***Gesundes Misstrauen:*** *Bei Fremden sollten Kinder und Jugendliche anfangs prinzipiell misstrauisch sein, vor allem, wenn die Unbekannten wenig von sich preisgeben, persönliche Fragen stellen und sofort private Chats oder sogar freizügige Fotos wollen.*
- → ***Erschlichenes Vertrauen:*** *Groomer versuchen, sich das Vertrauen ihrer Opfer zu erschleichen, indem sie sehr rasch eine intensive Freundschaft vorgaukeln, besonders freundlich sind, Komplimente machen oder sogar Geschenke anbieten.*
- → ***Testfragen stellen:*** *Das Gegenüber mit Fragen zu aktuellen (Jugend-)Themen und Internetausdrücken auf altersgerechtes Wissen abklopfen.*
- → ***Keine persönlichen Daten:*** *Wohn- und Schuladresse, Telefonnummer und Geburtsdatum sind privat und sollen auch privat bleiben.*
- → ***Privatsphäre-Einstellungen:*** *Viele soziale Netzwerke und andere Online-Dienste bieten Sicherheitsfunktionen an, von denen unbedingt Gebrauch gemacht werden sollte. Bei Facebook kann beispielsweise vorgesehen werden, dass Unbekannte einen nicht kontaktieren können.*
- → ***Fototest:*** *Soll doch ein Chat oder ein intensiverer Austausch stattfinden,*

sollte der Fototest gemacht werden. Hierzu sollte ein aktuelles Foto verlangt werden, auf dem eine spezielle Tätigkeit ausgeübt oder ein Gegenstand in die Kamera gehalten wird.

→ ***Blind Dates:*** *Hier gilt die LLL-Faustregel: Licht, Lärm, Leute – ein Einkaufszentrum oder ein gut besuchtes Café zum Beispiel. Unbedingt sollte jemand von dem vereinbarten Treffen wissen und regelmäßig Lebenszeichen erhalten. Auch vorher festgelegte Codewörter sind hilfreich: Sollte das Blind Date unangenehm werden, kann mittels eines unauffälligen Geheimwortes die Freundin oder der Freund zu Hilfe gerufen werden.*

Rachepornos

Mit der zunehmenden Verbreitung von Cybermobbing wandeln sich aber auch dessen Methoden und Spielarten. Kinder agieren eher mit Beleidigungen und Beschimpfungen allgemeiner Art, bei Jugendlichen dominieren eher sexuell konnotierte Themen. Speziell die sexuelle Belästigung und die Veröffentlichung von Nacktbildern nehmen zu.

„Rachepornos" sind sexuelle Bilder oder Videos, die meist von der Ex-Partnerin oder dem Ex-Partner ohne Zustimmung der abgelichteten Personen im Internet veröffentlicht werden. In den letzten Jahren sind viele Webseiten aus dem Boden geschossen, auf denen frustrierte Ex-Partnerinnen und -Partner intime Bilder und Videos ihrer Verflossenen hochladen. Meist unter Angabe des echten Namens, mit einem direkten Link zum Facebook-Profil oder auch anderen persönlichen Daten wie Wohnadresse, Arbeitsplatz oder Telefonnummer. Das unerlaubte Veröffentlichen von Rachepornos oder Nacktfotos im Internet fällt nach der Strafgesetznovelle 2015 unter den Tatbestand des Cybermobbings!

Aber auch bei Jugendlichen kommt derartiges vor, meistens in abgewandelter Form. Freizügige Aufnahmen oder Nachrichten, die in den Bereich Sexting fallen, werden veröffentlicht, um die abgebildete Person bloßzustellen. Dass sexuell konnotierte Bilder und Videos auch als kinderpornografisches Material gewertet werden müssen, ist dabei den wenigsten (Eltern) bekannt. Cybermobbing hat speziell im Bereich der Verbreitung von Nacktfotos und -videos eine neue Drehscheibe gefunden: Der Kommunikationsdienst WhatsApp hat Facebook hierbei den Rang abgelaufen. Problematisch an dieser App ist vor allem, dass Nachrichten und Bilder sehr schnell an große Personengruppen

verschickt werden können. Der Dienst wird häufig von Jugendlichen zur raschen und einfachen Streuung von Bildern mit sexuellem Inhalt verwendet.

Was kann getan werden?

- → ***Prävention:*** *Selten trifft der Vorsatz „Lieber Vorsicht als Nachsicht" mehr zu als beim Thema Rachepornos. Die Liebe kann groß sein, das Bedauern und die späteren negativen Auswirkungen auf das Berufs- und Privatleben aber noch viel größer.*
- → ***Speicherort:*** *Nicht jeder Speicherort oder Datenträger ist sicher. Ein Hackingangriff auf eine Cloud oder nicht mit PIN-Code geschützte Smartphones, und schon können Fotos in falschen Händen sein, auch gewöhnliche Sicherungskopien (z. B. auf CDs oder USB-Sticks) können leicht für eine Verbreitung missbraucht werden.*
- → ***Beziehungsende:*** *Unbedingt einschlägige Fotos zurückverlangen oder auf deren Löschung beharren.*
- → ***Recht am eigenen Bild:*** *Bereits das Anfertigen eines Bildes ohne Einwilligung der oder des Abgebildeten kann einen Eingriff in die Persönlichkeitsrechte darstellen. Fotos, Videos oder deren Begleittext dürfen nicht die berechtigten Interessen der darauf abgebildeten Personen verletzen. Die Aufnahmen dürfen die Abgebildeten nicht herabsetzen oder bloßstellen. Videos, die freizügig gekleidete Personen oder sexuelle Handlungen zeigen, verletzen jedenfalls Persönlichkeitsrechte. Wird ein nachteiliges Bild oder Video entdeckt, haben Userinnen und User das Recht auf Löschung oder Entfernung, da hier das Recht am eigenen Bild gilt. Zusätzlich kann das Verbreiten intimer Fotos unter Umständen auch als Ehrenbeleidigung strafbar sein.*
- → ***Social Media:*** *Viele soziale Medien haben einen Meldemechanismus, über den solche Fotos gemeldet und gelöscht lassen werden können.*
- → ***Webseiten:*** *Tauchen Fotos auf Webseiten auf, sofort die Webseiten-Betreiberinnen oder -betreiber informieren; Informationen über die Vorgehensweise in einem solchen Fall gibt es beim Internet Ombudsmann unter www.ombudsmann.at.*
- → ***Anzeige:*** *In schwerwiegenden Fällen kann das Veröffentlichen von Nacktfotos oder -videos nach §120a StGB (Cybermobbing) angezeigt werden.*
- → ***Unterlassungsklage:*** *In gravierenden Fällen hilft nur noch der Weg vor Gericht mittels Unterlassungsklage und Schadenersatzforderung. Hierfür Beweise sichern (z. B. mittels Screenshots) und vorher juristisch beraten lassen.*

Recht am eigenen Bild:
UrhG § 78

Beleidigung:
StGB §115

Face Rape

Das Phänomen hat viele Namen: „Facebook Rape", „Face Rape" oder beide Wörter zusammengezogen zu „Frape". Hierbei verschafft sich eine fremde Person Zugriff zum Facebook-Konto und postet im Namen des unwissenden Opfers, verändert das Profil, veröffentlicht erniedrigende Kommentare oder peinliche Fotos. Üblicherweise geschieht ein Face Rape unter Freunden oder Mitschülern, in sozialen Situationen, in denen mehrere Kinder oder Jugendliche zusammen sind. Vergisst jemand, sich von seinem Konto abzumelden, oder schützt sein Smartphone nicht durch eine Passwortsperre, wird das oft gnadenlos ausgenützt. Häufig wird das Profilfoto oder die Profilinformation geändert, oder es werden im Namen des Opfers eigenartige oder peinliche Kommentare an die Freunde geschickt. Beliebte Facebook Rapes sind zum Beispiel, eine neue sexuelle Orientierung in der Profilinformation anzugeben oder ein Posting zu einer angeblichen Geschlechtskrankheit des Betroffenen zu veröffentlichen.

Viele Jugendliche sind bereits in irgendeiner Form mit Facebook Rape in Berührung gekommen, meistens jedoch nur als Zuseher und nicht als Opfer. Das Fatale an Facebook Rape ist, dass es von vielen Jugendlichen als harmloser Streich angesehen wird. Facebook Rape fällt jedoch in die Kategorie von Cybermobbing: der absichtlichen Bloßstellung anderer.

Was kann getan werden?

- → ***Ausloggen:*** *Nach dem Ende der Nutzung von Facebook und Co. ausloggen.*
- → ***Passwörter:*** *Keine Passwörter speichern und diese auch nicht weitergeben, keine Passwörter verwenden, die leicht zu erraten sind.*
- → ***Passwortsperren:*** *Auch für das Smartphone, Tablet und andere Endgeräte einrichten.*
- → ***Im Ernstfall:*** *Ist der Account doch gefrapet, die erniedrigenden Kommentare oder peinlichen Fotos löschen lassen oder über die Meldefunktion melden, andere darüber informieren, dass der eigene Account missbraucht wurde.*
- → ***Hilfe holen:*** *In Klassenverbänden die Lehrkörper informieren oder die Eltern um Hilfe bitten.*

Pro-ANA- und -MIA-Webseiten

Die Abkürzungen ***ANA*** und ***MIA*** stehen für Krankheiten aus dem Bereich der Essstörungen. Im Internet gibt es viele Pro-ANA- und Pro-MIA-Webseiten, die diese Krankheiten als Lifestyle bewerben und die gesundheitlichen

ANA:
Magersucht „Anorexia nervosa"

MIA:
Ess-Brech-Sucht „Bulimia nervosa"

Implikationen verharmlosen. Diese Webseiten werden meistens von selbst essgestörten Personen betrieben, die ihre Essstörung verherrlichen. Auf den Webseiten finden sich Diättipps, Fastenwettbewerbe, Abnehmverträge und Tagebücher von anderen (essgestörten) Anhängerinnen und Anhängern. Die Inhalte sind nach dem Jugendschutzgesetz als jugendgefährdend einzustufen, erfüllen aber keinen Straftatbestand und werden oftmals auf ausländischen Servern gehostet.

Wiener Initiative gegen Essstörungen:
www.ess-stoerungen.at

Essstörungs-Hotline:
www.essstoerungs-hotline.at

Live-Streaming

Es gibt eine neue Quelle der (Online-)Begeisterung unter Jugendlichen und ein dankbares, weil kontroverses Thema für die Medien: die App YouNow. YouNow funktioniert nach einem simplen Prinzip: Nach dem Einloggen können Userinnen und User mit nur einem Klick die Liveübertragung von Bild- und Tonaufnahmen ins Internet starten, wo andere diese Streams anschauen können. Über eine Chatfunktion steht das Publikum direkt mit der Streamerin oder dem Streamer in Kontakt.

Das größte Problem ist, dass viele besonders junge Userinnen und User auf dem Streaming-Dienst zu finden sind und live aus Klassen- und Kinderzimmern streamen. Die AGB der Plattform erlauben offiziell die Nutzung erst ab 13 Jahren, doch in der Praxis sind auch weitaus jüngere Kinder auf der Seite anzutreffen. Sie haben unter Umständen nur wenig Bewusstsein für auf ihre Privatsphäre und geben zu viele private Informationen preis. Manche Jugendliche sind sich aber auch durchaus bewusst, dass private Daten nicht für das Internet geeignet sind, ignorieren solche Bedenken aber der Popularität und der Unterhaltung des Publikums zuliebe.

Ein weiterer Punkt, der von den jugendlichen Nutzerinnen und Nutzern oftmals nicht bedacht wird, ist das Urheberrecht. Werden beispielsweise andere Personen ungefragt und ohne deren Zustimmung mitgestreamt – beispielsweise im Klassenzimmer –, verletzt dies das Recht am eigenen Bild. Ebenso können Nutzungs- und Verwertungsrechte verletzt werden, wenn etwa Musik im Hintergrund läuft, die urheberrechtlich geschützt ist.

Recht am eigenen Bild:
UrhG § 78

Generell lässt sich bei der Berichterstattung über neue Kommunikationsdienste und -apps die Tendenz zu anfänglicher Schwarzmalerei feststellen. War dies schon bei sozialen Netzwerken, Datingseiten für Jugendliche oder Foto-Apps wie Snapchat der Fall, sind es nun die Broadcastingdienste. Doch YouNow ist per se nicht schlecht und auch nicht jugendgefährdend. Es ist

eine neue Online-Spielwiese für Teenager und eine konsequente Fortsetzung der aktuellen Mediennutzung: sich selbst zeigen und mit anderen über verschiedene Kanäle gleichzeitig interagieren.

Sexting

Sexting (Engl. „sex" und „texting") ist das gegenseitige Tauschen von freizügigen Fotos per Smartphone oder Internet und ist bei Jugendlichen inzwischen sehr populär. Die freizügigen Bilder oder auch Nacktaufnahmen werden in erster Linie unter besten Freundinnen und Freunden wie auch unter Pärchen ausgetauscht und gelten als eine Art Freundschafts- und Liebesbeweis. ***SEXTING*** ist mittlerweile auch Teil des Flirtens, sich Fotos voneinander zu schicken, ist nicht mehr unüblich.

Problematisch an Sexting ist vor allem, dass Nachrichten und Bilder sehr schnell an große Personengruppen verschickt werden können. Besonders Instant Messenger wie WhatsApp werden häufig von Jugendlichen hierfür genutzt. Doch sind solche Inhalte einmal in Umlauf, kann ihre weitere Streuung kaum noch aufgehalten werden.
Häufig wird ebenfalls die Foto-App Snapchat für das Versenden von freizügigen Fotos genutzt, da die übermittelten Fotos, je nach voreingestelltem Zeitstempel, nach ein paar Sekunden nicht mehr sichtbar sind. Doch die Bilder können per Screenshot oder mit eigenen Apps (z. B. Snap Save) vor dem Erlöschen gespeichert werden und sind somit auch hier nicht sicher.

Das neue Strafrechtsänderungsgesetz 2015 sieht nun in § 207a StGB, „Pornographische Darstellungen Minderjähriger", sowohl für VersenderInnen als auch EmpfängerInnen bei einvernehmlichem Sexting einen Strafausschließungsgrund vor. Demnach dürfen nun auch allzu freizügige bzw. pornographische Aufnahmen einer mündigen minderjährigen Person (14 bis 18 Jahre), die grundsätzlich Kinderpornografie darstellen, von dieser (straffrei) an eine andere Person weitergegeben werden, sofern diese andere Person die Aufnahmen nur für ihren eigenen Gebrauch verwendet; beispielsweise kann ein 16-Jähriger die von sich selbst gemachten freizügigen Aufnahmen an die feste Freundin weitergeben. Das Gesetz schränkt dabei nicht ein, wer diese andere Person sein darf. Ebenso ist es erlaubt, von einer mündigen minderjährigen Person mit deren Einwilligung freizügige Aufnahmen zu machen, sofern diese Aufnahmen nur zum eigenen Gebrauch jener Person gedacht sind, die sie macht; beispielsweise kann eine Freundin von ihrem Freund eine freizügige Aufnahme machen und diese straffrei behalten.

?

Sexting:

(Kombination aus „sex" und „texting", Engl. SMS schreiben.) Das Verschicken von Texten mit sexuellen Inhalten, freizügigen Fotos oder Videos per SMS, Instant Messenger oder Chat.

?

Mündige Minderjährige:

14 bis 18 Jahre

Unmündige Minderjährige:

unter 14 Jahren

Erpressung per Webcam: Der „Sex Scam“

Sextorsion:
(Kombination aus „sex“ und „extorsion“ Engl. für Erpressung.) Erpressung mit sexuell expliziten Fotos und Videos.

Seit einiger Zeit häufen sich die Vorfälle einer besonders perfiden Erpressungsstrategie, die vor allem auf männliche Jugendliche und Erwachsene abzielt. Die Masche wird im großen Stil von internationalen Betrügerbanden abgezogen und funktioniert immer nach einem ähnlichen Schema: Zuerst werden die Opfer über soziale Netzwerke angeschrieben und zu einem vermeintlich privaten Videochat per Webcam überredet. Beim Videochatten werden sie dazu animiert, sich vor der Kamera auszuziehen oder sexuelle Handlungen an sich selbst vorzunehmen, immer unter dem Deckmantel eines vertraulichen und privaten Chats. Die Opfer wiegen sich in Sicherheit, weil sie mit der Täterin oder dem Täter befreundet oder bekannt sind, oder weil das Gegenüber sogar selbst mitmacht und sich zum Beispiel der Kleidung entledigt.
Was die Opfer nicht bedenken ist, dass der Chat keineswegs ein geschützter privater Raum ist. Denn währenddessen kann jederzeit ein Screenshot vom Chat oder sogar ein Videomitschnitt gemacht werden – und genau das nutzen die Kriminellen aus. Sehr bald nach dem Videochat – oder sogar währenddessen – wird von den Betrügerinnen oder Betrügern Kontakt aufgenommen und die miese Masche wird aufgedeckt. Sie verlangen Geldzahlungen oder nötigen ihre Opfer zu neuen demütigenden Handlungen. Sie drohen damit, die peinliche Videoaufnahme über soziale Netzwerke oder Videoplattformen zu verbreiten oder direkt an Eltern, Freundinnen und Freunde des Opfers zu schicken. Die Täter nutzen die Angst und Scham der Opfer als Druckmittel, um ihre Forderungen durchzusetzen.
Oftmals werden die Videos auch auf YouTube hochgeladen und auf „privat“ eingestellt, sodass sie nicht öffentlich sind. Im Titel und in der Videobeschreibung werden so viele Informationen über das Opfer genannt wie nur möglich. Dieser Link wird dann an die Opfer geschickt, was noch mehr Druck erzeugt.

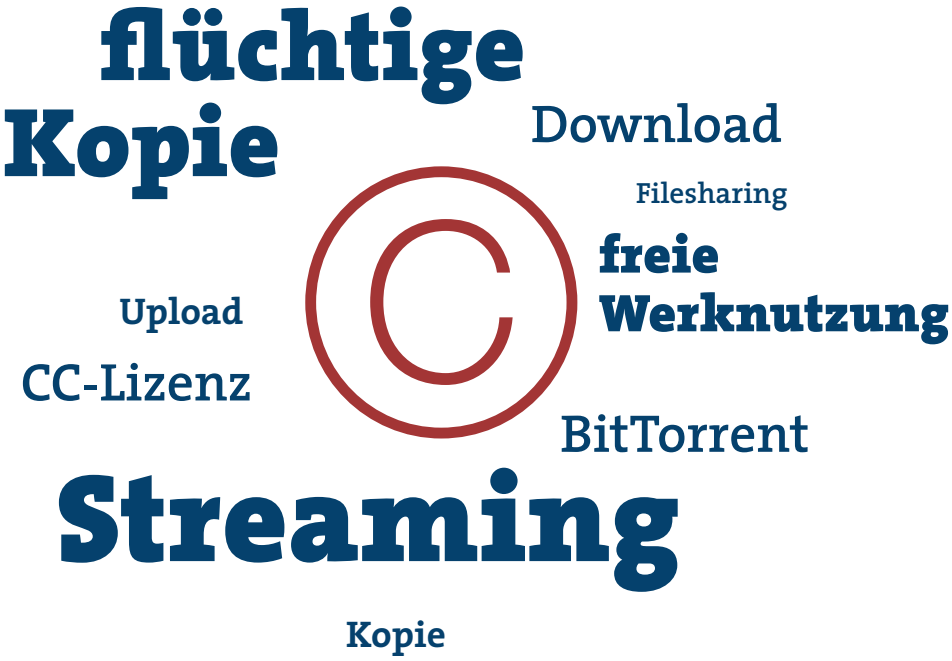
Was kann getan werden?

- → ***Ruhe bewahren:*** *Wird man zum Opfer einer solchen Betrugsmasche, gilt es in erster Linie, Ruhe zu bewahren und nicht auf die Forderungen einzugehen. Die Betrügerbanden setzen nämlich auf die Angst und Scham der Opfer und darauf, dass diese sofort auf ihre Drohungen reagieren.*
- → ***Beweissicherung:*** *Alle relevanten Informationen, um den Betrug zu belegen, dokumentieren, Screenshots der Betrüger-Accounts machen, das Chatprotokoll und den E-Mail-Verkehr speichern.*

- → ***Kontaktabbruch:*** *Der Kontakt sollte sofort abgebrochen und die Erpresserinnen und Erpresser sollten von der Freundes- und Kontaktliste entfernt werden.*
- → ***Melden:*** *Die Accounts der Erpresserinnen und Erpresser sofort über die Meldefunktion – sofern vorhanden – der sozialen Netzwerke oder des Chatdienstes melden, auch die Betreiber der Webseite sollten informiert werden.*
- → ***Hilfe:*** *Opfer sprechen oft aus Scham nicht über ihre Probleme oder wollen nicht um Hilfe bitten. Mit der Familie oder Freundinnen und Freunden zu sprechen kann jedoch sehr helfen; auch kann Hilfe bei professionellen Helplines wie „Rat auf Draht" gesucht werden – dort gibt es anonyme und kostenlose Beratung.*
- → ***Alert-Dienst:*** *Einen Alert-Dienst für den eigenen Namen anlegen, so wird man über jedes neue Video oder jeden Artikel mit dem eigenen Namen informiert.*
- → ***Die eigenen Rechte kennen:*** *Unerlaubte Aufnahmen von einem selbst sind rechtlich nicht zulässig. Nach §207a, „pornografische Darstellung Minderjähriger", ist es verboten, pornografische Aufnahmen von minderjährigen Personen zu machen, zu besitzen und auch zu veröffentlichen.*
- → ***Anzeige:*** *Eine strafrechtliche Verfolgung solcher Erpresserbanden ist nur bei einer Anzeige möglich.*
- → ***Andere warnen:*** *Damit nicht noch mehr Personen Opfer solcher Betrugsmaschen werden, sollten Bekannte oder Freundinnen und Freunde informiert werden!*

Rat auf Draht:

www.rataufdraht.orf.at
Tel.: 147



Die vielen Paragrafen des Urheberrechts sind für viele Internetnutzerinnen und -nutzer nicht leicht verständlich. Zusätzlich hat jedes (europäische) Land unterschiedliche Bestimmungen. In den Medienberichten geht es meistens um Urheberrechtsverletzungen, auch Betrugsvarianten mit Abmahnschreiben von Anwältinnen und Anwälten häufen sich. Die meisten Userinnen und User sind verunsichert: Was dürfen sie nun und was nicht?

Urheberrecht

Streaming

STREAMING ist eine Form von Datenübertragung, bei der Video- und Audiodateien downgeloadet und gleichzeitig auf dem Endgerät abgespielt werden. Die Daten werden üblicherweise nicht bleibend auf der Festplatte gespeichert, es wird lediglich für die Dauer des Abspielens eine ***FLÜCHTIGE KOPIE*** im Arbeitsspeicher erstellt. Diese flüchtige Vervielfältigung fällt unter eine Ausnahmeregelung des Urheberrechts und ist daher zulässig und legal. Prinzipiell gilt für die Wiedergabe von Werken zu privaten Zwecken das Recht der freien Werknutzung.

Download

Der Download zu privaten Zwecken ist zulässig. Prinzipiell ist der Download von Dateien aus dem Internet legal, wenn das Recht zur ***WERKNUTZUNG*** erworben wurde, beispielsweise durch einen Kauf. Selbstverständlich ist der Download von Werken, deren urheberrechtliche Schutzfrist abgelaufen ist, legal (z. B. bei Büchern 70 Jahre nach dem Tod der Urheberin oder des Urhebers), ebenso der Download und die Nutzung von Werken, die beispielsweise mittels einer ***CC-LIZENZ*** der Öffentlichkeit frei zur Verfügung gestellt werden.

Achtung:
Beim Vorlagestück für den Download ist Vorsicht geboten. Die Urheberrechtsnovelle 2015 hat das Recht der Nutzerinnen und Nutzer auf Anfertigung einer Privatkopie dahin gehend eingeschränkt, dass die Vervielfältigung zum eigenen Gebrauch nur von rechtmäßig hergestellten und veröffentlichten Vorlagestücken erfolgen darf. Das bedeutet, dass ein Download nur dann legal ist, wenn auch das originale Vorlagestück legal erworben oder veröffentlicht wurde; somit entfallen viele zum Download angebotene Werke auf Onlineplattformen, da es sich hierbei oft um urheberrechtsverletzende Kopien handelt.

Es bleibt den Onlinenutzerinnen und -nutzern selbst überlassen zu beurteilen, ob der gewünschte Film, das kostenlose Musikstück oder das Com-

Streaming:
(„Stream", Engl. für fließen, strömen.) Datenübertragung, bei der Video- und Audiodaten gleichzeitig downgeloadet und über einen Browser abgespielt werden können.

Flüchtige Kopie:
Temporäre Vervielfältigung, die im Hintergrund passiert und nach dem Abspielen wieder gelöscht wird.

Freie Werknutzung:
Das urheberrechtlich geschützte Werk darf zum eigenen und privaten Gebrauch frei genutzt werden (gelesen, angeschaut oder abgespielt), solange es sich dabei nicht um eine kommerzielle Nutzung handelt.

CC-Lizenz bzw. Creative-Commons-Lizenz:
(„Creative commons" Engl. für schöpferisches Gemeingut.) Standard-Vertrag, der es der Autorin oder dem Autor auf einfache Art ermöglicht die Nutzungsrechte des Werkes mit der Öffentlichkeit zu teilen.

Siehe auch: Creative-Commons-Lizenzen: S. 33

puterspiel rechtmäßig ins Internet gestellt wurde oder nicht. Bei dieser Differenzierung ist vor allem der weitverbreitete Download urheberrechtlich geschützter Werke aus nicht lizenzierten Internet-Tauschbörsen ***(P2P-TAUSCHBÖRSEN)*** erfasst. Der Download von P2P-Tauschbörsen ist in der Regel mit einem gleichzeitigen Upload der bereits downgeloadeten Dateien verbunden, was eine nicht genehmigte Zurverfügungstellung nach § 18a UrhG darstellt und daher ohnehin eine Rechtsverletzung ist.

P2P-Tauschbörsen:
(„Peer-to-Peer", Engl. für von Gleichgestelltem zu Gleichgestelltem oder Kommunikation unter Gleichen.) In einem P2P-Netz sind alle Computer gleichberechtigt und können Dienste in Anspruch nehmen und gleichzeitig zur Verfügung stellen.

Torrent bzw. BitTorrent:
(„Bit", Engl. für kleinste Dateneinheit, und „torrent", Engl. für reißender Strom.) Kollaboratives Filesharing-Protokoll, das den Datenaustausch über ein großes Netzwerk ermöglicht.

Filesharing:
(„File", Engl. für Dateien, und „sharing", Engl. für teilen.) Das direkte Weitergeben von Dateien zwischen Internetnutzerinnen und -nutzern.

HTTP bzw. Hypertext Transfer Protocol:
(Engl. für Hypertext-Übertragungsprotokoll.) Standardverfahren zur Übertragung von Daten über das Internet, findet hauptsächlich beim Laden von Webseiten aus dem WWW in Webbrowsern Anwendung.

Filesharing & Torrents

Online-Tauschbörsen, in denen Musik, Filme oder auch Software getauscht bzw. heruntergeladen werden können, sind so beliebt wie umstritten. Diese Tauschbörsen funktionieren über ***BITTORRENT***-Protokolle, die einen schnellen Datenaustausch ermöglichen. Im Vergleich zum herkömmlichen Download einer Datei mittels ***HTTP*** oder ***FTP*** werden beim BitTorrent-Protokoll die (ansonsten ungenützten) Upload-Kapazitäten der anderen Downloaderinnen und Downloader mitgenutzt, auch wenn sie die Datei erst unvollständig heruntergeladen haben. Der Download per BitTorrent erfolgt in der Regel nicht linear (vom Anfang bis zum Ende), sondern setzt sich aus vielen kleinen Teilen zusammen, die je nach Verfügbarkeit downgeloadet werden.

Achtung:
Problematisch (in Bezug auf das Urheberrecht) bei der BitTorrent-Technologie ist, dass die Datei beim Download gleichzeitig zum Upload zur Verfügung gestellt wird. In dem Moment, in dem ein Download eines Torrent-Files gestartet wird, werden sofort Teile des Files anderen Downloaderinnen und Downloadern zur Verfügung gestellt. Das stellt im urheberrechtlichen Sinn eine rechtswidrige Zurverfügungstellung dar.

Upload

Möchten Nutzerinnen und Nutzer ihre Werke (z. B. selbst komponierte Musikstücke, eigene Texte, Bilder oder Fotos) zur Verfügung stellen, versehen sie diese am besten mit einer CC-Lizenz und können sie anschließend anderen Nutzerinnen und Nutzern zum Download zur Verfügung stellen. Werke zum (kostenlosen wie auch zum kostenpflichtigen) Download zur Verfügung zu stellen ist legal, solange die Nutzerinnen und Nutzer die Urheberinnen und Urheber des Werks sind.
Stellen Nutzerinnen oder Nutzer ihre eigenen Werke, also jene, deren Urhe-

berinnen oder Urheber sie sind, ohne Angabe zur Werknutzung (beispielsweise mit einer CC-Lizenz versehen) ins Netz, ist es für andere nicht zulässig, sie zu verwenden, außer zur freien Werknutzung, auf gesetzliche Lizenzen beschränkt (z. B. die Urheberin oder der Urheber ist gesetzlich verpflichtet, die Nutzung zuzulassen, wird aber dafür entlohnt) oder nach einem käuflichen Erwerb. Somit ist es sinnvoll, Angaben zur Werknutzung zu veröffentlichen, vorgeschrieben ist es aber nicht.

Achtung:
Freie Werknutzung bedeutet jedoch nicht, dass ein fremdes Werk auf die eigene Webseite hochgeladen werden darf, da dies den Gebrauch für private Zwecke übersteigt. Stellt eine Nutzerin oder ein Nutzer ein vorher käuflich erworbenes Werk beispielsweise auf einer Filesharing-Börse zur Verfügung, ist das eine Urheberrechtsverletzung und somit eine strafbare Handlung.

Abmahnungen & Unterlassungsaufforderungen

Wurde eine Urheberrechtsverletzung begangen, kann die Urheberin oder der Urheber bzw. die Rechteinhaberin oder der Rechteinhaber die Person, die das Urheberrecht verletzt hat, abmahnen. Eine solche ***ABMAHNUNG*** kommt in den meisten Fällen von einer Anwaltskanzlei und wird in Briefform verschickt, in manchen Fällen auch vorab per E-Mail. In einer solchen Abmahnung wird die Person, die das Urheberrecht verletzt hat, dazu aufgefordert, innerhalb einer bestimmten Frist die konkrete Rechtsverletzung zu unterbinden (z. B. ein veröffentlichtes Foto zu löschen), eine Unterlassungserklärung abzugeben, Schadenersatz zu zahlen sowie die Anwaltskosten zu übernehmen.

Achtung:
Abmahnungen sollten keinesfalls ignoriert werden, da sonst ein teures Gerichtsverfahren droht. Jedoch sind oft die Schadenersatzforderungen überhöht und die Unterlassungserklärung zum Nachteil der Rechteverletzerin oder des Rechteverletzers ausformuliert. Es empfiehlt sich auf jeden Fall, Kontakt mit einer Konsumentenschutz-Organisation aufzunehmen (z. B. Internet-Ombudsmann) oder sich juristische Unterstützung zu holen. In Extremfällen kann eine Urheberrechtsverletzung mehrere tausend Euro kosten.

Kinder & Urheberrecht

Erziehungsberechtigte sind sehr wohl verpflichtet, oberflächlich über die Internetaktivitäten der eigenen Kinder Bescheid zu wissen. Jedoch sind Eltern nicht

FTP bzw. File Transfer Protocol:

(Engl. für Dateiübertragungsprotokoll.) Protokoll zur Dateiübertragung über IP-Netzwerke, konkret, um Dateien von FTP-Server zu Client (Download), von Client zu FTP-Server (Upload) oder clientgesteuert zwischen zwei FTP-Servern (Exchange) zu übertragen.

Weitere Infos zum Urheberrecht:

ISPA Ratgeber Urheberrecht

kostenloser Download unter www.ispa.at/urheberrecht

Abmahnung:

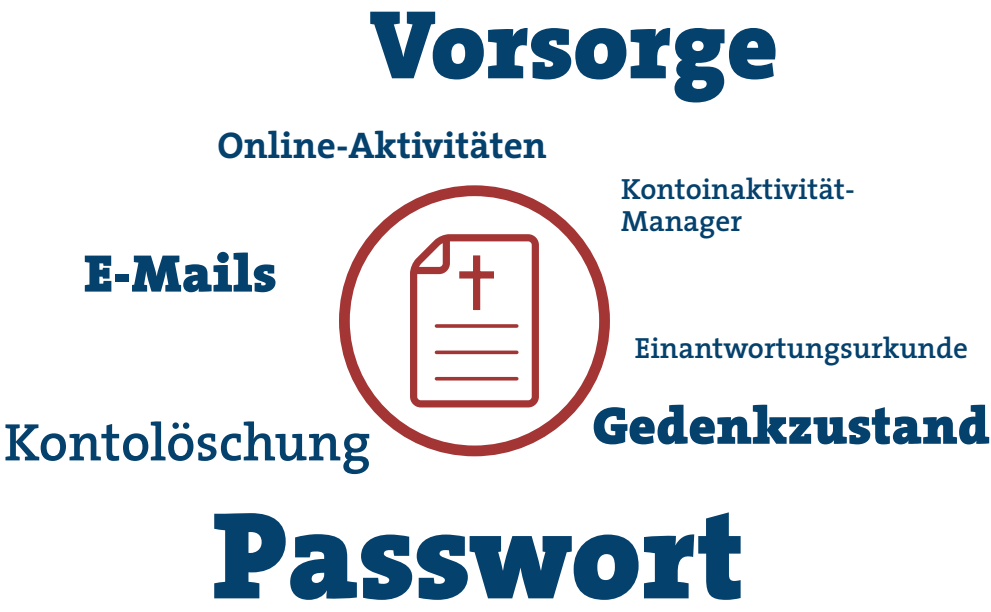
Ist eine juristische Aufforderung, eine bestimmte Handlung zu unterlassen.

Infos zu Abmahnungen:

www.ombudsmann.at

verpflichtet, deren gesamte Aktivitäten im Internet zu überwachen. Diesbezüglich ist ein Urteil des Obersten Gerichtshofs in Österreich richtungsweisend: Ein Vater wurde von der Haftung für die Tauschbörsenaktivitäten seiner Tochter freigesprochen, da er von den Aktivitäten seiner Tochter nichts wusste. Die Funktionsweise von Filesharing-Systemen kann laut dem OGH bei Erwachsenen nicht als allgemein bekannt vorausgesetzt werden. Jedoch müssen Elternteile sehr wohl oberflächlich prüfen, ob das eigene Kind grobe oder auffallende Urheberrechtsverstöße begeht. Es gibt jedoch keine Verpflichtung, die Aktivitäten des Nachwuchses von vornherein zu überwachen.

Achtung:
Dieses Urteil ist jedoch kein Garant dafür, dass Eltern in einer ähnlichen Situation niemals rechtlich belangt werden. Ein Gericht wird sich voraussichtlich an dem Freispruch des OGH orientieren, aber sehr wohl die äußeren Umstände – die in jedem Fall anders sein werden – berücksichtigen. Hierbei kommt es beispielsweise auf das Alter des Kindes an oder auf das Ausmaß der Urheberrechtsverletzung.



Als digitaler Nachlass werden jene Daten bezeichnet, die nach dem Tod einer Userin oder eines Users im Internet weiter bestehen. Dazu zählen Profile in sozialen Netzwerken wie Facebook, Twitter, YouTube, Xing, Partnervermittlungsbörsen oder Benutzerkonten bei E-Mail-Diensten. Auch um Blogs, Domainnamen oder Websites und deren Weiterbestehen, Nutzung oder Löschung sollten sich die Hinterbliebenen kümmern.

Digitaler Nachlass

Grundsätzlich gibt es vier Möglichkeiten, wie mit dem digitalen Nachlass umgegangen werden kann:

→ *Erhaltung*
→ *Löschung*
→ *Archivierung*
→ *Übertragung der Daten an Angehörige/Erben*

Die meisten Menschen können sich unter dem Begriff des digitalen Nachlasses etwas vorstellen, doch eine allgemein gültige Definition, was alles unter diesen Begriff fällt, gibt es nicht. Ebenso ist rechtlich nicht geklärt, wie mit einer Hinterlassenschaft in der Online-Welt umzugehen ist. Viele Punkte sind noch unklar und die Materie weitgehend ungeregelt, sowohl auf österreichischer als auch auf europäischer Ebene. Das Erbrecht ist in fast allen Staaten der Welt unterschiedlich, beispielsweise gibt es bereits (große) Unterschiede zwischen Österreich und Deutschland. Verkompliziert wird die Sache zudem, wenn ein Todesfall mehrere Staaten betrifft, z. B. die verstorbene Person in Österreich gelebt und einen E-Mail-Dienst eines US-amerikanischen Unternehmens genutzt hat.

Zu all diesen Problemen kommt zusätzlich, dass Unternehmen vor Betrug und geschmacklosen Scherzbolden auf der Hut sein müssen. Es mag auf den ersten Blick den Anschein haben, die Verfahren und Regelungen rund um den digitalen Nachlass seien teilweise sehr bürokratisch und kompliziert, doch dies ist notwendig, um Missbrauch zu vermeiden.

Vorsorge

Der erste Schritt der Vorsorge ist, eine Bestandsaufnahme durchzuführen. Sich über den persönlichen digitalen Nachlass und sein digitales Alter Ego Gedanken zu machen muss nicht unbedingt einen akuten Anlass haben. Es ist durchaus sinnvoll, von Zeit zu Zeit eine Bestandsaufnahme durchzuführen und zu überlegen, welche persönlichen Daten im Internet vorhanden sind und was in der digitalen Welt – soweit das beeinflussbar ist – nach dem eigenen Ableben weiterhin bestehen sollte.

Je konkreter festgelegt wird, was mit dem digitalen Nachlass geschehen soll, desto selbstbestimmter ist das im digitalen Raum verbleibende Bild einer Person nach ihrem Ableben.

Eine möglichst vollständige Liste mit allen Online-Mitgliedschaften, Profilen und sonstigen Onlineaktivitäten ist meistens schon die halbe Miete. In dieser Liste sollten auch Nicknames oder Zugangsdaten verzeichnet sein. Die Liste sollte regelmäßig aktualisiert werden. Da diese Liste der Schlüssel zur privaten Onlineaktivität ist, sollte sie sicher und sorgsam verwahrt werden. Sie kann in Form einer physischen Liste an einem den Hinterbliebenen bekannten und zugänglichen Ort (z. B. Safe, Dokumentenmappe) oder im Rahmen eines Testaments beim Notar hinterlegt werden.
Ebenfalls zu empfehlen ist, den gewünschten Umgang mit Benutzerkonten und Daten schriftlich festzuhalten. So kann etwa niedergeschrieben werden, welche privaten Daten und Einträge (z. B. E-Mails, Fotoalben) nach dem Tod im Internet weiterhin zugänglich sein bzw. welche Daten gelöscht werden sollen. In diesem Schriftstück sollte auch festgelegt werden, wer im Todesfall Zugriff auf diese sensiblen und persönlichen Daten erhält. Die betraute Person sollte genügend Internetkompetenz besitzen, um bei auftretenden Problemen mit Onlinediensten adäquat reagieren zu können.

Mittlerweile gibt es im Internet zahlreiche Unternehmen, die sich auf die Verwaltung des digitalen Erbes spezialisiert haben. Diese Unternehmen bieten beispielsweise an, Daten oder Passwörter gegen Entgelt in einer Art digitalem Schließfach aufzubewahren. Diese Form der digitalen Aufbewahrung birgt jedoch einige Risiken: So ist oft unklar, ob und in welchem Rahmen ein Unternehmen langfristig Datensicherheit gewährleisten kann bzw. was mit den Daten passiert, sofern das Unternehmen Konkurs anmelden muss. Sollte die Firma ihren Sitz im Ausland haben, könnten auch juristische Unklarheiten oder eine unterschiedliche Rechtslage zu Problemen führen. Darüber hinaus gibt es auch sogenannte „Online-Bestatter". Solche Firmen bieten als Dienstleistung an, das Internet nach Onlineaktivitäten der Verstorbenen zu durchsuchen und sich beispielsweise um die Löschung von Profilen oder die Kündigung von Verträgen und Mitgliedschaften zu kümmern.

Checkliste

Kommunikation

- → *E-Mail-Accounts/Postfächer*
- → *Soziale Netzwerke: Facebook, Twitter, Google+, Myspace*
- → *Business-Netzwerke: Xing, LinkedIn*
- → *Fotodienste: Flickr, Picasa, Instagram*
- → *Instant Messenger: WhatsApp, Kik, Skype, MSN*
- → *Blog-Dienste: blogger.com, Tumblr, Wordpress*
- → *Partnerbörsen & Dating-Apps: Parship, Tinder, Lovoo*
- → *Vlog- und Videodienste: YouTube, Vine*

Bezahlung/Einkauf

- → *Onlinebanking*
- → *Online-Bezahlsysteme: PayPal*
- → *Konten*
  - → *Versandhandel: eBay, Amazon*
  - → *Wettanbieter*
  - → *Spiele-Plattformen*
- → *Kostenpflichtige Onlinedienste*
  - → *Mitgliedschaften bei Partnerbörsen*
  - → *Abos: Video-on-Demand-Mediendienste (z. B. Netflix), Onlinezeitungen*
  - → *Multimedia-Verwaltungs- und -Vertriebsplattformen: iTunes, BlackBerry World, Google Play Store, Windows (Phone) Store*
- → *Internetwährungen (& Wallets): Bitcoin, Ripple etc.*

Sonstige Internetaktivitäten

- → *Cloud-Dienste: Dropbox, Google Drive, RapidShare, iCloud etc.*
- → *Blogs & Websites*
- → *Rechte für Domains (Internetadressen die mit http://www. beginnen)*

Offline – Daten, die auf einem Gerät gespeichert sind

- → *Persönliche Dokumente (Fotos oder gespeicherte E-Mails)*
- → *Mediale Inhalte (Musikdateien, Filme, elektronische Bücher)*
- → *Softwarelizenzen*

Anforderungen unterscheiden sich

Viele Onlinedienste (z. B. GMX, Twitter) haben für den Fall des Ablebens einer Nutzerin oder eines Nutzers standardisierte Prozedere eingeführt und bemühen sich, den schwierigen Prozess der Nachlassverwaltung für Hinterbliebene bei allen Sicherheitsvorkehrungen dennoch so unbürokratisch wie möglich zu gestalten. Links zu entsprechenden Antragsformularen finden sich oft bei den „häufig gestellten Fragen" (FAQ).

Möchten die Hinterbliebenen eine Kontolöschung durchführen lassen, müssen sie üblicherweise einen Antrag stellen und den Tod der betreffenden Person nachweisen (Sterbeurkunde); in manchen Fällen bedarf es auch einer ***EINANTWORTUNGSURKUNDE***. Nach Vorlage dieser Unterlagen und deren Bearbeitung seitens der Onlinedienste werden – je nach Bedarf – die Konten gelöscht oder unter Umständen die Daten an die Hinterbliebenen weitergegeben. Die Dauer dieses Verfahrens variiert stark von Onlinedienst zu Onlinedienst, in einigen Fällen ist es ein langwieriger Prozess von mehreren Monaten. Erschwert wird das Ganze, da viele dieser Dienste und Firmen ihren Sitz im Ausland haben und sich sprachliche Barrieren, bürokratische Hürden oder Herausforderungen resultierend aus den unterschiedlichen Gesetzeslagen ergeben können.

Einantwortungsurkunde:
Offizielle Bestätigung der Rechtsnachfolge.

In der Regel benötigen Hinterbliebene folgende Informationen und Nachweise:

- → *Vor- und Nachnamen der verstorbenen Person*
- → *Account-Namen (User-ID, Nickname) der verstorbenen Person bzw.*
- → *Link zum Profil*
- → *Sterbeurkunde*
- → *Kontaktdaten der oder des Hinterbliebenen*
- → *Einantwortungsurkunde*

Bei einigen Online-Communitys oder sozialen Netzwerken (z. B. Xing, Skype oder Flickr) gibt es aber momentan noch kein ausgewiesenes Prozedere oder Formular für den Todesfall, sodass sich Angehörige individuell an den Kundenservice wenden und um Hilfestellung seitens der Anbieter bemühen müssen. Um herauszufinden, was bei einem bestimmten Angebot im Ablebensfall getan werden kann, empfiehlt es sich, in den AGB des entsprechenden Dienstes nachzulesen. Eine weitere Möglichkeit ist, per Suchmaschine nach dem Namen des Internetdienstes und nach Schlagworten wie „verstorben", „Todesfall" oder Ähnlichem zu suchen. Mit hoher Wahrscheinlichkeit

wurde eine solche Frage bereits im Internet gestellt und im besten Fall sogar beantwortet. Aber auch hier werden die Erben alle entsprechenden Unterlagen vorweisen müssen.

Einen ersten Überblick können sich Hinterbliebene mithilfe des Onlinedienstes justdelete.me verschaffen. Diese Webseite informiert über die Möglichkeiten, wie Online-Profile gelöscht werden können, der unterschiedliche Schwierigkeitsgrad bzw. notwendige Aufwand ist mit einem Farbcode gekennzeichnet.

Informiert über Löschmöglichkeiten von Onlinediensten:
www.justdelete.de

Zwei Möglichkeiten bei Facebook

Facebook bietet zwei Möglichkeiten, mit dem Konto einer verstorbenen Person umzugehen: Die Hinterbliebenen können das Konto vollständig löschen oder es in den Gedenkzustand versetzen lassen. Beim Gedenkzustand wird das entsprechende Profil eingefroren, sodass es nicht mehr verändert werden kann, befreundete Nutzerinnen und Nutzer aber beispielsweise Erinnerungen an die Person in deren Chronik posten können.

Darüber hinaus haben Facebook-Nutzerinnen und -Nutzer die Möglichkeit, eine Erbin oder einen Erben für ihr Konto auszuwählen. Einer der Facebook-Kontakte bekommt hierbei die Ermächtigung, im Falle des eigenen Todes das digitale Erbe des Facebook-Profils übernehmen zu können. Hier bekommt die Erbin oder der Erbe gewisse Rechte, kann aber nicht auf private Nachrichten zugreifen oder im Namen der verstorbenen Person posten.

Vorsorge bei Google

Google bietet eine Möglichkeit für Userinnen und User, sich um ihren digitalen Nachlass zu kümmern. Mit dem Service des Kontoinaktivität-Managers haben Nutzerinnen und Nutzer die Option, ihren digitalen Nachlass vorsorglich zu regeln. Hierbei legen sie fest, was nach ihrem Ableben mit ihren Daten bzw. dem Google-Konto passieren soll.

Eine Möglichkeit der Vorsorge besteht im Informieren von vertrauenswürdigen Dritten, wenn das Konto längere Zeit nicht benutzt wurde. Hier können bis zu zehn Vertrauenspersonen angegeben werden. Zusätzlich können Nutzerinnen und Nutzer ihre Daten mit diesen zuvor ausgewählten vertrau-

enswürdigen Dritten teilen. Dabei besteht die Möglichkeit – bei der Nutzung von mehreren Google-Services –, zielgenau festzulegen, welche Daten mit wem geteilt werden sollen. So kann eingestellt werden, dass zum Beispiel die Fotoalben von Picasa lediglich mit der Familie geteilt werden, die Video-Inhalte von YouTube aber auch mit den Freundinnen und Freunden.

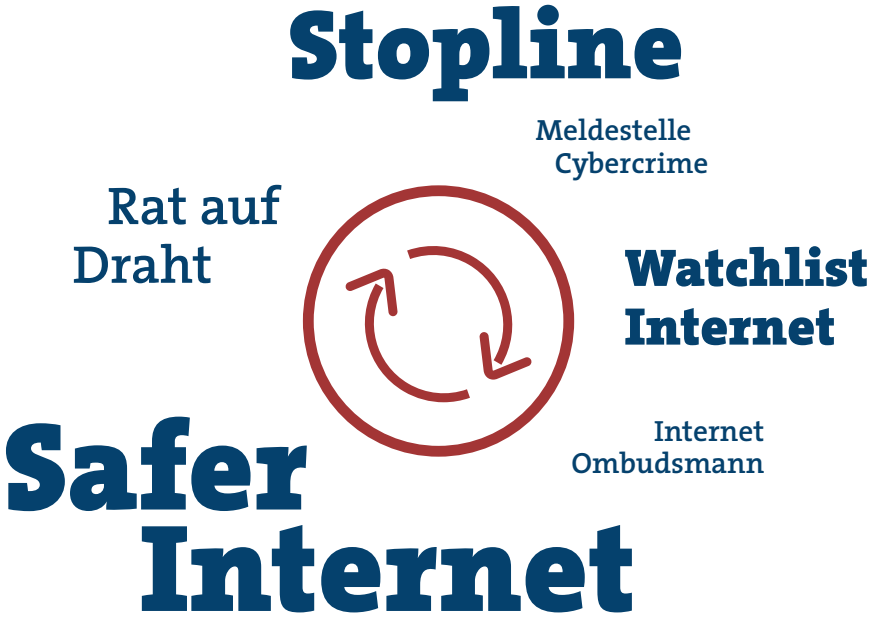
Was sonst getan werden kann

Was kann aber getan werden, wenn die oder der Verstorbene keine Aufzeichnungen bezüglich der Onlineaktivitäten hinterlassen hat? Bei Unsicherheit, wie und wo die verstorbene Person im Internet aktiv war, kann es hilfreich sein, mittels Internetsuchmaschinen nach dem Namen der verstorbenen Person zu suchen. Sind Spitzname oder Namenskürzel bekannt, empfiehlt es sich, ebenfalls nach diesen Schlagwörtern zu suchen. Oftmals können auch Bekannte darüber Auskunft geben, welche Dienste der oder die Verstorbene genutzt hat. Hierbei empfiehlt es sich das gesamte soziale Umfeld zu befragen, sowohl Verwandte, Freundinnen und Freunde, (Ehe-) Partnerin oder Partner als auch die Kollegenschaft.

Zugriff auf E-Mails

Nach dem Ableben einer oder eines Angehörigen stehen die Hinterbliebenen oft vor vielen Herausforderungen: Sie müssen Bekannte, berufliche Kontakte und Freundinnen und Freunde informieren, noch offene Angelegenheiten der oder des Verstorbenen klären oder brauchen ganz einfach Zugang zu wichtigen Unterlagen. Einige größere Onlinedienste (z. B. Google, Microsoft, GMX) bieten Verbliebenen die Option, Zugriff auf die E-Mails der oder des Verstorbenen zu erlangen.

Auch hierfür können Angehörige einen Antrag stellen und bekommen nach dessen Prüfung Zugang zum elektronischen Postfach oder eine Kopie des Postfachinhalts. Dieser Prozess ist aber oftmals sehr beschwerlich und langwierig. Hinterbliebene sollten sich also darauf einstellen, dass der Zugriff auf die E-Mails der verstorbenen Person nicht innerhalb kürzester Zeit ermöglicht werden wird.



Die österreichische Informations- und Koordinierungsstelle Saferinternet.at unterstützt Internetuserinnen und -user bei der sicheren Nutzung von Internet, mobilen Endgeräten 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 Zusammenarbeit mit der öffentlichen Hand und der Wirtschaft umgesetzt.

Melde- & Beratungsstellen

Für die Beantwortung von weiterführenden Fragen zur sicheren Internetnutzung sowie für Hilfe und Beratungen steht Ihnen das Team der Safer-Internet-Trainerinnen und -Trainer 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.

www.saferinternet.at
www.rataufdraht.at

Allgemeines

Haben Nutzerinnen und Nutzer allgemeine Anliegen, sind in Abo-Fallen getappt oder haben Fragen zu ihren Rechten beim Onlinekauf, so hilft der Internet Ombudsmann bzw. sein Team an Expertinnen und Experten.

www.ombudsmann.at

Beratungsstelle Extremismus

Befürchten Angehörige oder Lehrende, dass sich eine Person radikalen religiösen Gruppierung oder einer politisch extremen Gruppe angeschlossen hat oder mit rechtsextremem oder radikal islamistischem Gedankengut sympathisiert, können sie sich an die Beratungsstelle Extremismus des BMFJ wenden.

Telefon: 0800 20 20 44
Email: office@beratungsstelleextremismus.at

Onlinebetrug

Die Watchlist Internet informiert österreichische Nutzerinnen und Nutzer über Internetbetrug und betrugsähnliche Online-Angebote. Sie informiert über aktuelle Betrugsfälle und gibt Tipps zum Schutz vor solchen.

www.watchlist-internet.at

Illegale Inhalte

Stoßen Nutzerinnen und Nutzer auf illegale Inhalte – also kinderpornografische oder nationalsozialistische Inhalte –, können sie diese bei der Meldestelle Stopline anonym und unbürokratisch melden.

www.stopline.at

Internetkriminalität

Haben Nutzerinnen und Nutzer einen begründeten Verdacht auf Internetbetrug oder Internetkriminalität, können sie sich an die Meldestelle Cybercrime des Bundeskriminalamtes wenden. Straftaten können jedoch nach wie vor nur bei einer Polizeidienststelle zur Anzeige gebracht werden.

against-cybercrime@bmi.gv.at

Glossar

419 Scam: Sammelbezeichnung für verschiedene Betrugsvarianten per E-Mail, leitet sich vom entsprechenden Paragrafen des nigerianischen Strafgesetzes ab, da viele dieser Betrugsbanden ihren Sitz in Nigeria haben.

Add-on: (Engl. für Erweiterung.) Add-ons sind optionale Module, die Software oder Hardware erweitern und neue Funktionen ermöglichen.

Alert-Dienst: Der wohl bekannteste Alert-Dienst ist der Google-Alert. Ein Alert-Dienst ist ein Informationsdienst, der per E-Mail-Benachrichtigung oder RSS informiert, wenn neue Ergebnisse zu einem vorher festgelegten Schlagwort, Namen oder sonstigen Abfragekriterien auftauchen.

Alias-Adresse: (Engl. „alias" für Deckname oder Pseudonym.) E-Mail-Adresse, die keinen Hinweis auf die eigene Identität gibt.

Blog bzw. Weblog: (Kombination aus Engl. „web" und „log" für Logbuch.), ist ein auf einer Webseite geführtes, periodisches und meist öffentliches Journal zu einem bestimmten Thema.

Business-Netzwerke: Dienen der beruflichen Vernetzung und der Präsentation der eigenen Person als Fachkraft; funktionieren wie soziale Netzwerke.

CC-Lizenz bzw. Creative-Commons-Lizenz: („Creative commons" Engl. für schöpferisches Gemeingut.) Standard-Vertrag, der es der Autorin oder dem Autor auf einfache Art ermöglicht die Nutzungsrechte des Werkes mit der Öffentlichkeit zu teilen.

Clickjacking: (Engl. für Klickeintreibung.) Mit Täuschungsabsicht gestaltete Internetseiten oder Klickflächen, die echte Webseiten oder Klickflächen überlagern, um Nutzerinnen und Nutzer in die Irre zu führen.

Client: Ein Computerprogramm, das auf einem Endgerät installiert wird und bestimmte Dienste vom Server abrufen kann.

Community: (Engl. für Gemeinschaft.) Gruppe im Internet, deren Mitglieder miteinander (mit Bezug zu einem bestimmten Thema) kommunizieren und interagieren.

Dashboard: (Engl. für Armaturenbrett.) Es ist je nach Onlinedienst unterschiedlich ausgestaltet, meistens jedoch die persönliche Start- oder Admin-Seite, auf der Information zusammengetragen wird.

Date-Baits: (Engl. Date-Köder.) Von Dating-Plattformen engagierte Personen, die Mitglieder in eine (kostenpflichtige) Mitgliedschaft locken sollen.

Disclaimer: (Engl. für Haftungsausschluss.) Ablehnung, für fremde Inhalte zu haften.

Domain: Das ist ein „Namensraum" im Internet, der eine weltweit im Internet einmalige und eindeutige Adresse darstellt.

Domaingrabbing: Missbräuchliche Registrierung eines oder mehrerer Domainnamen.

E-Mail-Harvesting: („To harvest", Engl. für ernten.) Automatisiertes Sammeln von E-Mail-Adressen aus Foren, Dokumenten und von Webseiten.

Filesharing: („File", Engl. für Dateien, und „sharing", Engl. für teilen.) Das direkte Weitergeben von Dateien zwischen Internetnutzerinnen und -nutzern.

Firewall: (Engl. für Brandwand oder Brandschutz.) Sicherungssystem, das einzelne Computer oder Netzwerke vor unerlaubten Zugriffen schützt.

Flüchtige Kopie: Temporäre Vervielfältigung, die im Hintergrund passiert und nach dem Abspielen wieder gelöscht wird.

Freemium: (Kombination aus „free", Engl. gratis, und „premium", Engl. Belohnung.) Geschäftsmodell, bei dem Basisprodukte oder -funktionen kostenlos sind, die Vollversion bzw. deren Freischaltung ist jedoch kostenpflichtig.

Freie Werknutzung: Das urheberrechtlich geschützte Werk darf zum eigenen und privaten Gebrauch frei genutzt werden (gelesen, angeschaut oder abgespielt), solange es sich dabei nicht um eine kommerzielle Nutzung handelt.

FTP bzw. File Transfer Protocol: (Engl. für Dateiübertragungsprotokoll.) Protokoll zur Dateiübertragung über IP-Netzwerke, konkret, um Dateien von FTP-Server zu Client (Download), von Client zu FTP-Server (Upload) oder clientgesteuert zwischen zwei FTPServern (Exchange) zu übertragen.

Geosocial Networking: Soziale Netzwerke, die mit standortbezogenen Daten arbeiten.

Hasspostings: Postings mit Inhalten, die unter strafrechtliche Tatbestände wie Verhetzung, Rufschädigung, Ehrenbeleidigung oder üble Nachrede fallen.

HTML bzw. Hypertext Markup Language: Textbasierte Auszeichnungssprache zur Strukturierung von digitalen Inhalten wie Texten, Bildern und Hyperlinks in elektronischen Dokumenten.

HTTP bzw. Hypertext Transfer Protocol: (Engl. für Hypertext Übertragungsprotokoll.) Standardverfahren zur Übertragung von Daten über das Internet, findet hauptsächlich beim Laden von Webseiten aus dem WWW in Webbrowsern Anwendung.

Hoax: („Hoax", Engl. für Scherz oder Schwindel.) Falschmeldung, die Userinnen und User täuschen soll, damit diese die Meldung weiterverbreiten.

Hotspot: (Engl. für Brennpunkt.) Öffentlicher drahtloser Internetzugriffspunkt.

In-App-Käufe: Bei manchen Apps (z. B. Spielen) besteht die Möglichkeit, im Rahmen der Anwendungen Guthaben oder Punkte zu kaufen, ohne einen klassischen Bestellvorgang zu durchlaufen.

IPv4 bzw. Internet Protocol Version 4: Aktuelles Internetprotokoll, das die technische Grundlage des Internets bildet. IPv4-Adressen sind 32 Bit lang.

IPv6 bzw. Internet Protocol next Generation (IPnG): Neues Internetprotokoll, das IPv4 ablösen soll. IPv6-Adressen sind 128 Bit lang.

Klarname: Auch engl. „Realname", ist der tatsächliche Name einer Person, der auch in amtlichen Dokumenten geführt wird.

Kryptografie: („Kryptós", Altgr. für geheim, und „gráphein", Altgr. für schreiben.) Verschlüsselung von Informationen; ist Teil der Kryptologie, der Wissenschaft von der Informationssicherheit.

Kryptowährung: Digitales Zahlungssystem zur Verwaltung von privat geschöpftem, virtuellem Geld; es werden Prinzipien der Kryptografie angewandt.

Lurker: Userinnen und User von sozialen Netzwerken, die nur passiv am Online-Geschehen teilnehmen und kaum aktiv Content produzieren.

Netiquette: (Kombination aus „net", Engl. für Netz, und „étiquette", Franz. für Verhaltensregeln.) Der angemessene und achtsame Umgang mit anderen Userinnen und Usern im Internet.

Nickname: Name der eigenen virtuellen Identität, im realen Leben mit einem Spitznamen zu vergleichen.

Malware: (Engl. für Schadsoftware.) Bösartige Programme, die den Rechner oder das Betriebssystem angreifen, Daten stehlen oder diese an Dritte übertragen.

Patch: (Engl. für flicken, auch Nachbesserung.) Software-Update, das Korrekturen enthält, Fehler behebt oder Sicherheitslücken schließt.

PDF bzw. Portable Document Format: Plattformunabhängiges Dateiformat, das sich dadurch auszeichnet, den Inhalt originalgetreu wiederzugeben.

Peer-to-Peer: Auch P2P abgekürzt, ist eine Verbindungsart, bei der Daten direkt von Teilnehmerin/Teilnehmer zu Teilnehmerin/Teilnehmer übertragen werden.

Phishing: (Kunstwort aus „fishing", Engl. für fischen, und „password", Engl. für Passwort.) Betrugsmasche, um an Zugangsdaten zu kommen und somit Zugriff zu Accountsund Konten zu erhalten.

Plug-in: (Engl. für einstecken, konkret auch Erweiterungsmodul.) Softwaremodul, das zur Erweiterung der Funktionalität einer bestehenden Software eingesetzt werden kann.

Positivlisten: Vorher festgelegte Webseiten, die erlaubt sind.

Provider: Unternehmen, die den Zugang zum Internet gewährleisten.

Proxy: (Engl. für Stellvertreter.) Schnittstelle in einem Netzwerk, die die Kommunikation zwischen zwei Servern/Rechnern weiterreicht.

Reblog bzw. Reblogging: Das Posten von fremden Inhalten, genauer gesagt, das Posten von bereits veröffentlichten Inhalten anderer Nutzerinnen und Nutzer auf dem eigenen Blog.

Recht am eigenen Bild: Bereits die Herstellung eines Bildes ohne Einwilligung der oder des Abgebildeten kann als Eingriff in die Persönlichkeitsrechte gelten. Fotos, Videos oder deren Begleittext dürfen die Abgebildeten nicht herabsetzen oder bloßstellen.

Rechteinhaberin oder Rechteinhaber: Jene Person, die die Rechte an einem bestimmten Werk hat; meint gemeinhin die Urheberin oder den Urheber.

Router: Netzwerkgeräte, die Informationspakete zwischen mehreren Rechnernetzen weiterleiten können. Sie werden u. a. für die Internetanbindung verwendet.

Searchbots: Auch Spider oder Webcrawler genannt, sind Computerprogramme, die das Internet durchsuchen und Webseiten analysieren; sie werden vor allem zum Sammeln von E-Mail-Adressen, RSS-Newsfeeds und anderen Informationen eingesetzt.

Server: Computer, auf dem Programme laufen, auf die andere Computer (Clients) zugreifen können.

Sexting: (Kombination aus „sex“ und „texting“, Engl. für SMS schreiben.) Das Verschicken von Texten mit sexuellen Inhalten, freizügigen Fotos oder Videos per SMS, Instant Messenger oder Chat.

Social-Media-Richtlinien: Von Unternehmen erstellte Richtlinien für die Angestellten, die das Verhalten in und die Nutzung von sozialen Netzwerken während der Arbeitszeit festlegen.

Shitstorm: (Kombination aus „shit“, Engl. für Scheiße und „storm“, Engl. für Sturm.) Sturm der Entrüstung im Internet, der zum Teil mit beleidigenden Äußerungen einhergeht.

Spam: (Urspr. ein Markenname für Dosenfleisch, das während des Zweiten Weltkriegs als einziges Nahrungsmittel im Überfluss erhältlich war.) Sammelbegriff für jede Art von unerwünschten E-Mails, insbesondere Massenaussendungen mit Werbung.

SSL-Protokoll: Ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet (SSL = Secure Sockets Layer), seit Version 3.0 wird das Protokoll unter TLS weiterentwickelt und standardisiert (TLS = Transport Layer Security).

Streaming: („Stream“, Engl. für fließen, strömen). Datenübertragung, bei der Video- und Audiodaten gleichzeitig downgeloadet und über einen Browser abgespielt werden können.

Subdomain: Eine Domain, die in der Hierarchie unter einer anderen liegt; meistens sind damit Domains der dritten oder vierten Ebene gemeint (die Top-Level-Domain ist .at, die Second-Level-Domain ist beispiel.at und eine Subdomain davon wäre irgendein.beispiel.at).

Top-Level-Domain: Die oberste Hierarchieebene von Internetadressen; wird unterteilt in allgemeine TLDs, wie .com oder .org, und in Länder-TLDs, wie .at oder .de.

Torrent bzw. BitTorrent: („Bit“, Engl. für kleinste Dateneinheit, und „torrent“, Engl. für reißender Strom.) Kollaboratives Filesharing-Protokoll, das den Datenaustausch über ein großes Netzwerk ermöglicht.

Troll: Person, die im Internet absichtlich Diskussionen anheizt und meist andere Userinnen und User provoziert.

Urheberin oder Urheber: Eine Person, die durch eigene geistige Leistung ein Werk erschaffen hat.

Usenet: Eigenständiges, weltweites elektronisches Netzwerk, welches lange vor dem World Wide Web entstand. Jenes Netz, in dem die klassischen Diskussionsforen des Internets (Newsgroups) zu Hause sind.

USB bzw. Universal Serial Bus: Ein Bus ist ein System zur Datenübertragung zwischen mehreren Teilnehmerinnen oder Teilnehmern über einen gemeinsamen Übertragungsweg (= Schnittstelle). Mit USB ausgestattete Medien können bei laufendem Betrieb miteinander verbunden werden, die angeschlossenen Geräte werden automatisch erkannt.

Viren: Schädliche Computerprogramme, die sich selbstständig einschleusen und verbreiten können.

Virenschutz: (Auch Virenscanner oder Antivirenprogramm genannt.) Software, die Computerviren und andere Schadprogramme aufspürt, blockiert und beseitigt.

Virtual Private Network bzw. VPN: (Engl. für virtuelles privates Netzwerk.) Schnittstelle in einem Netzwerk; kann eine Verbindung zwischen zwei Netzwerken sein oder zu einem bestimmten Service.

Vlog: (Kombination aus „Video" und „Blog".) Blog, dessen Einträge aus Videos bestehen.

Wallet: Auch E-Wallet oder Cyberwallet, ist eine virtuelle Geldbörse.

Web Proxy Autodiscovery Protocol bzw. WPAD: Protokoll, mit dem Web-Clients automatisch verfügbare Proxys finden können.

Wegwerf-Adresse: Wegwerf-E-Mail-Adressen sind provisorische E-Mail-Adressen, die nur für einen bestimmten Zeitraum gültig sind und anschließend verfallen.

Wegwerf-Identität: Mit „Fake Identity"-Generatoren werden per Zufallsgenerator willkürlich Name, Geburtsdatum und Adresse aus Datenbanken ausgewählt.

Impressum

Medieninhaber, Herausgeber, Verleger: ISPA – Internet Service Providers Austria
Verband der österreichischen Internet-Anbieter
1090 Wien, Währinger Straße 3/18
Redaktion: Daniela Drobna, Nona Parvanova, Maximilian Schubert
Stand: November 2015
Lektorat: Gudrun Harlass
Layout: allesgrafik GmbH, 1200 Wien
Druck: Gutenberg Druck GmbH, 2700 Wiener Neustadt
Fotos: Bundesministerium für Justiz (S. 5), Bundeskanzleramt (S. 6), ISPA (S. 7)

Gefördert durch die Europäische Union – Safer Internet Programm

Österreichische Meldestelle gegen Kinderpornografie & Nationalsozialismus im Internet

www.stopline.at

So helfen Sie mit - für ein sicheres Internet:

- Bedenkliche Inhalte melden
- Stopline Logo verlinken
- Kostenloses Infomaterial verteilen

Finanziert von:

nic at
the austrian registry

The project is co-funded by the European Union, through the Safer Internet plus programme.
http://ec.europa.eu/saferinternet

Eine Initiative der:

ispa Internet Service Providers Austria

Währinger Straße 3 / 18, 1090 Wien
Tel.: +43 (0)1 409 55 76 | office@ispa.at
www.ispa.at | twitter.com/ispa_at
facebook.com/ISPA.InternetserviceProvidersAustria