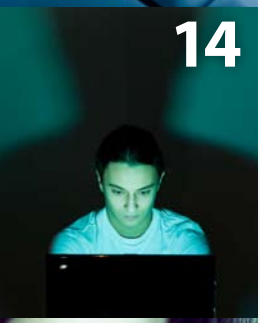
2. überarbeitete Auflage 2012
+ Gütesiegel zum Aufkleben

GUT ZU WISSEN!
Sicher surfen sicher handeln

INITIATIVE D21

Bayerisches Staatsministerium der Justiz und für Verbraucherschutz



Grußwort

Dr. Beate Merk, MdL
Bayerische Staatsministerin der
Justiz und für Verbraucherschutz

Hannes Schwaderer
Präsident der Initiative D21

Liebe Leserin, lieber Leser,

das Internet ist eine der größten Erfindungen der Menschheitsgeschichte. Es begleitet uns mittlerweile in nahezu allen Lebensbereichen. Komplexität und Umfang nehmen in atemberaubendem Tempo zu. Aber hält auch der Verbraucher damit Schritt? Aktuelle Untersuchungen aus dem Jahr 2011 haben ergeben, dass 62 Prozent der deutschen Internetnutzer noch Informationsbedarf beim Umgang mit den neuen Medien haben. Auf dem Weg in die Digitale Gesellschaft sind also noch einige Stolpersteine zu überwinden.

Sicherheit im Internet und das Vertrauen der Verbraucher sind auch für die Wirtschaft von besonderer Bedeutung. Sie sind wesentliche Voraussetzungen dafür, dass Verbraucher Online-Angebote erst nutzen. Ziel muss es daher sein, für Transparenz und Schutz im Netz zu sorgen. Die aktuellen Debatten über die sozialen Netzwerke zeigen: Internetnutzer sollten über Fragen des Persönlichkeits- und Datenschutzes Bescheid wissen.

Furcht vor dem Internet muss keiner haben, aber wachsam sollte man sein. Diese Broschüre gibt praktische und verständliche Hilfestellungen, wie man sicher im Internet surfen kann. Als Besonderheit sind der Broschüre Aufkleber der empfohlenen Gütesiegel beigefügt.

Wir wünschen Ihnen eine informative Lektüre!

Online einkaufen, aber sicher!

Der Einkauf im Internet erfreut sich bei Verbrauchern immer größerer Beliebtheit. Die Vorteile liegen auf der Hand: Rund um die Uhr entspannt shoppen – ohne Stress, Parkplatzsuche oder Schlangestehen. Wenn etwas nicht gefällt oder passt, schickt man es einfach zurück. Es verwundert daher kaum, dass 9 von 10 Internetnutzern bereits im Web eingekauft haben.

Auch beim Online-Kauf ist der Verbraucher durch die bestehenden Gesetze gut geschützt. Dennoch sollte man bei Bestellungen im Internet mit der nötigen Aufmerksamkeit vorgehen.

Aufschlussreich ist oft schon der geschäftliche Auftritt des Internetanbieters. Ist klar ersichtlich, wer Anbieter ist und wie man ihn im Zweifel erreichen kann? Macht die Seite selbst einen ordentlichen Eindruck? Welche Daten werden beim Einkauf abgefragt? Gibt es auf einer der zahlreichen Bewertungsseiten bereits Kundenmeinungen zum Anbieter? Diese sind zwar nicht immer aussagekräftig, vermitteln aber einen ersten Eindruck.

Nach dem Gesetz ist der Händler verpflichtet, ein Impressum (Name des Anbieters, Anschrift, Erreichbarkeit, Hinweis auf das Registergericht etc.) und Allgemeine Geschäftsbedingungen (AGB) anzugeben sowie auf das Widerrufsrecht für Verbraucher hinzuweisen.

Der Verbraucher ist für gewöhnlich durch ein Widerrufsrecht geschützt. Wird er hierüber nicht ordnungsgemäß belehrt, so kann er jederzeit - also auch nach mehreren Jahren - widerrufen. Denn die gesetzliche Frist (in der Regel 14 Tage ab Erhalt der Ware) läuft dann nicht ab.

Beim Online-Einkauf selbst sollte die Eingabe der persönlichen Daten (Anschrift, Kontoverbindung etc.) über eine verschlüsselte Verbindung erfolgen, um sicherzustellen, dass diese Daten nicht „mitgelesen" werden können. Zu erkennen ist dies an den Buchstaben „https" in der Adresse der Internetseite und einem Schloss- oder Schlüssel-Symbol im Internet-Browser.

Vorsicht ist bei Bestellungen bei ausländischen Anbietern geboten. Nicht nur, dass eine etwaige Verfolgung der eigenen Verbraucherrechte im Ausland erschwert sein kann. Zu beachten sind auch mögliche Zusatzkosten (höhere Versandgebühren, Steuern und Zölle, Bankgebühren). Diese zusätzlichen Kosten lassen vermeintliche Schnäppchen schnell teurer werden als vergleichbare Angebote im Inland.

Checkliste

- Anzeige der AGB und des Impressums
- Hinweis auf Widerrufsrecht
- Angabe der Versandkosten sowie der Gesamtkosten
- verschlüsselte Verbindung („https" in der Adresszeile)
- Überprüfung von Kundenmeinungen auf Bewertungsportalen

Internet-Gütesiegel

Die Auszeichnung einer Internetseite mit einem Gütesiegel oder einem Label kann ein Indiz für einen seriösen Anbieter sein. Jedoch ist nicht jede Auszeichnung gleich zu bewerten. Leider gibt es immer wieder Anbieter, die eine solche Auszeichnung selbst erfinden oder der Einfachheit halber auf ein Label zurückgreifen, das ohne sonderliche Anforderungen verliehen wird.

Umso wichtiger ist es, darauf zu achten, dass das Siegel auch für eine gewisse Qualität bürgt, die durch eine neutrale Stelle geprüft wird. Die Anbieter der vier Internet-Gütesiegel engagieren sich in einem Projekt der Initiative D21 und haben sich freiwillig zu mehr Verbraucherschutz im Netz verpflichtet, als es das Gesetz verlangt.

Die vier empfohlenen Gütesiegel:

Trusted Shops
www.trusted-shops.de

s@fer-shopping
www.safer-shopping.de

EHI Geprüfter Online-Shop
www.shopinfo.net

Datenschutz-Gütesiegel ips
www.datenschutz-cert.de

Beiliegend: Die Gütesiegel zum Herausnehmen und Aufkleben

In Deutschland sind mehr als 12.000 Internet-Shops mit diesen vier Siegeln zertifiziert und bieten daher die Gewähr für einen sicheren und reibungslosen Online-Handel. Und sollte doch einmal etwas schiefgehen, dann bieten Siegelanbieter wie Trusted Shops die Streitschlichtung zwischen dem Kunden und dem Internetshop oder gar die Erstattung etwaiger Auslagen an.

Sichere Bezahlverfahren

Auch im Hinblick auf die Bezahlmethoden sollte man Vorsicht walten lassen. Vorauskasse ist immer mit dem Risiko behaftet, bei einer Insolvenz des Händlers plötzlich ohne Ware dazustehen. Auch die Zahlung per Nachnahme ist nicht unbedingt zu empfehlen, da sie immer mit zusätzlichen Kosten verbunden ist. Im Zweifel besser auf Zahlung per Rechnung oder wenigstens per Kreditkarte drängen!

Um auf Nummer sicher zu gehen, bieten sich auch Bezahlverfahren wie etwa PayPal oder giropay an. Hier ist das Geld geschützt: Im Notfall wird es – wie bei einigen Kreditkartenunternehmen auch – sogar zurückerstattet. Eine weitere Alternative ist die sogenannte Sofortüberweisung. Bei dieser übernimmt ein zwischengeschalteter Dienstleister die Überweisung und gleichzeitig die Zahlungsvermittlung an den Verkäufer. Hier ist jedoch zu beachten, dass die Weitergabe von PIN und TAN unter Umständen gegen die AGB der eigenen Bank verstoßen kann. Es sollte daher zunächst bei der eigenen Bank nachgefragt werden.

Bei den genannten Verfahren erhält der Verkäufer selbst keinen Zugriff auf sensible Bezahldaten des Kunden, dafür jedoch das beauftragte Unternehmen.

Informationen und Hilfe im Netz

- Kampagne „Online Kaufen – mit Verstand!“: Eine Initiative von Versandhändlern und eBay für mehr Sicherheit im Onlinehandel mit Tipps und Tricks für den Notfall **www.kaufenmitverstand.de**
- Portal der Verbraucherzentralen: Die Verbraucherzentralen in den Ländern bieten schnelle und unbürokratische Unterstützung, wenn man doch mal auf ein „schwarzes Schaf“ des Onlinehandels gestoßen ist **www.verbraucherzentrale.de**
- Verbraucherinformationssystem Bayern: Das Portal der Ministerien des Freistaats Bayern mit Hinweisen, was man im Fall der Fälle tun muss **www.vis.bayern.de**

Sicher im Netz unterwegs

Verbraucher fürchten um die Sicherheit ihrer Daten im Netz. Dieses Problem stellt eines der größten Hemmnisse in der Entwicklung des Internet dar. Nach einer Umfrage der Gesellschaft für Konsumforschung im Auftrag des Bayerischen Staatsministeriums der Justiz und für Verbraucherschutz sehen 55 Prozent der bayerischen Verbraucher die Gefahr des Ausspioniertwerdens, des unbefugten Zugriffs auf Konten oder des mangelnden Datenschutzes als großes oder sehr großes Problem an.

Die Gefahren existieren, sind für den normalen Nutzer jedoch mit einem gewissen Maß an Sorgfalt minimierbar. Zuallererst ist darauf zu achten, den **Virenschutz** des Computers permanent auf dem neuesten Stand zu halten. Viele gute Virenschutzprogramme erkennen neben den eigentlichen Schadprogrammen auch Trojaner oder sogenannte Spy-Programme, die dafür konzipiert sind, Daten vom Rechner der Opfer auszuspähen.

Welche Daten werden beim Surfen erfasst?

So gut wie niemand surft anonym im Netz. Mit ein wenig Aufwand lässt sich fast jeder Schritt eines Nutzers auf einer Internetseite nachvollziehen. Viele Webseitenbetreiber tun ihr Übriges, um noch mehr Daten zu erheben.

Cookies

Manche Seiten legen **Cookies**, also kleine Dateien, auf dem Rechner des Besuchers ab. Sie dienen der Wiedererkennung bei einem späteren Besuch. Auf Basis der Daten des letzten Besuches werden bei einer Wiederkehr passende Waren oder Dienstleistungen zur Auswahl angeboten. Auch Browsereinstellungen für die Anzeige einer Website werden auf diesem Wege gespeichert.

Webanalyse

Einige Webseitenbetreiber verfolgen die Bewegungen der Besucher auf der eigenen Seite aus Marketinginteresse. Datenschutzrechtlich ist der Einsatz solcher Analysetools nicht unbedenklich, da Rückschlüsse auf die Person des Besuchers möglich werden. In Deutschland dürfen personenbezogene Nutzerprofile nur mit Einwilligung des Nutzers oder bei Verwendung von Pseudonymen unter Einräumung eines Widerspruchsrechts erstellt werden.

Behavioral Targeting

In Ergänzung zum Einsatz von Cookies können Anbieter etwa durch Einsatz von Webumfragen das Nutzerverhalten noch besser analysieren. Ziel des **„Behavioral Targeting"** ist es, Verbrauchern passgenaue Werbung zukommen zu lassen. Für die einen Fluch – für die anderen Segen: der gläserne Verbraucher. Geizen Sie daher mit der Herausgabe Ihrer Daten!

Datenerfassung	Cookie	Webanalyse	Behavioral Targeting
Ziel	Wiedererkennung und Individualisierung des Angebotes	Analyse des Nutzerverhaltens	Analyse des Nutzerverhaltens
Verfahren	Speichern von Textdateien auf dem lokalen Computer	Auswertung des Surfverhaltens anhand identifizierender Merkmale	Auswertung des Surfverhaltens + Befragung von Internetnutzern
Schutzmöglichkeiten	Browsereinstellungen anpassen (+ evtl. weitere Add-ons*)	Browser Add-ons* zur Sicherung der Privatsphäre	Browser Add-ons* zur Sicherung der Privatsphäre

* Browser Add-ons oder auch Plug-ins erweitern die Funktionen des Internetbrowsers.

Identitätsdiebstahl und -missbrauch

Ein großes Problem im Bereich der Datensicherheit ist der **Identitätsdiebstahl** oder der **Identitätsmissbrauch**. Dabei gibt eine Person vor, eine andere zu sein, um auf diese Weise etwa Waren zu bestellen, aber nicht bezahlen zu müssen. Auch die Verwendung der Daten eines anderen, um damit zum Beispiel andere Leute ungestraft bedrohen oder beleidigen zu können, ist leider nicht selten. Diese Identität hat sich der Täter zuvor durch den Identitätsdiebstahl verschafft.

Das Problem des Identitätsdiebstahls oder des Identitätsmissbrauchs ist vor allem bei solchen Portalen anzutreffen, die keine rechtsverbindliche Identifizierung verlangen. Insofern würde es helfen, wenn diese Portale künftig sicherstellen, dass auch wirklich nur der Berechtigte unter dem angegebenen Namen agieren kann. Die Identifizierungskomponente des neuen elektronischen Personalausweises wird hier möglicherweise künftig für mehr Sicherheit sorgen. Dem Internetnutzer sei geraten: mit den Daten geizen und so wenigen Menschen wie möglich Hinweise auf eigene Profile im Netz geben.

Phishing, Pharming & Co.

Was ist **„Phishing“**? Mit Phishing wird der Versuch umschrieben, mittels des Internet an sensible Daten von Nutzern zu gelangen. Im Regelfall wird hierbei versucht, Nutzer mit Hilfe einer E-Mail auf eine (gefälschte) Internetseite zu lotsen und sie dazu zu bringen, dort sensible Daten (Kontodaten, PINs, TANs) einzugeben. Als Absender der Mail wird meistens eine seriöse Institution vorgegaukelt. Die Nachrichten sehen oft täuschend echt aus.

Es gibt jedoch einige Anzeichen, dass die Nachricht nicht vom angegebenen Absender stammen könnte. So wird als Anrede oft nur die Floskel „Sehr geehrter Kunde" verwendet. Viele Banken schreiben ihre Kunden nicht per E-Mail an und wenn, dann mit persönlicher Anrede des Kunden. Auch finden sich in den Phishing-Mails häufig Grammatik- oder Rechtschreibfehler. Entdeckt man solche, ist in jedem Fall Vorsicht geboten.

In der gefährlicheren Variante der Phishing-Mails wird das Opfer auf eine Seite geleitet, deren Besuch allein schon eine Infizierung mit Schadsoftware (sog. „Malware") verursacht. Nur durch Anklicken des in der Nachricht enthaltenen Links (z.B. mit Hinweis auf eine völlig überhöhte Telefonrechnung) besteht schon die Gefahr, dass der Computer mit einem Virus oder einem **Trojanischen Pferd** verseucht wird. Dieser zeichnet u.a. Tastatureingaben am Rechner auf und übermittelt diese an die Täter weiter, die diese für strafbare Zwecke nutzen. In der „harmloseren" Variante bedarf es zusätzlich der Eingabe der angeforderten Daten auf der Zielseite, um Schadsoftware einzuschleusen.

Eine besonders hinterhältige Variante ist das sogenannte **„Pharming"**. Hier wird der Nutzer durch eine technische Manipulation auf eine gefälschte Seite geleitet, obwohl er die Adresse richtig eingegeben hat. Pharming ist aber aufgrund des Aufwands nicht besonders verbreitet.

Wichtige Schutzmaßnahmen

- E-Mails sind **keine sichere Kommunikationsform**, daher sollten E-Mails von unbekannten Absendern, wenn überhaupt, nur im Textmodus geöffnet werden (niemals auf darin enthaltene Links klicken)
- Installation von **Browser-Plug-ins**, die verhindern, dass man auf bekannte Phishingseiten geleitet wird
- Für die Übermittlung personenbezogener Daten ist der Einsatz von häufig kostenfrei erhältlichen **Verschlüsselungsprogrammen** (sogenannte Mail-Encryption-Software) oder künftig die Nutzung von DE-Mail ratsam, um eine sichere Kommunikation zu gewährleisten

Online-Banking

Der Nutzen des Internet besteht auch darin, Zeit und Geld bei alltäglichen Dingen zu sparen. Dies gilt auch und vor allem für den Einsatz des Internet für die Abwicklung von Bankgeschäften.

Aber auch Online-Banking kann mit Risiken verbunden sein, wenn man nicht die gebotene Sorgfalt an den Tag legt. So können etwa Daten mithilfe von Schadsoftware ausspioniert werden, mittels derer dann Kriminelle die Zahlungsströme umleiten können. Auch bietet Online-Banking den Nährboden für die meisten professionellen Phishing-Attacken, da immer wieder der eine oder andere Bankkunde auf die gewieften Tricks professioneller Phishingbetrüger hereinfällt.

Mit der Einführung der iTan oder der mobilen Tan ist das Risiko beim Onlinebanking bereits erheblich gesunken. Am sichersten ist aber nach wie vor die Erledigung der Bankgeschäfte unter Einsatz des signaturgestützten HBCI-Verfahrens, bei dem sich der Kunde mit einer Chipkarte und einem Kartenlesegerät identifiziert. Nachteil dieser Variante ist die Beschaffung zusätzlicher Hardware und das Erfordernis, ein relativ komplexes Banking-Programm zu installieren.

Oberstes Gebot ist in jedem Fall, sich die Internetseite genau anzuschauen, auf der die eigenen Daten einzugeben sind. Bankseiten, die sensible Daten von einem Nutzer verlangen, verwenden immer das sichere Hypertext-Übertragungsprotokoll („https“ = Hypertext Transfer Protocol Secure). Tipps für sicheres Online-Banking finden Sie unter https://www.bankenverband.de

Soziale Netzwerke

Die Möglichkeit, im Internet Freunde und Bekannte auf dem Laufenden zu halten, findet auch hierzulande immer mehr Anhänger. Führender Anbieter bei den „Social Networks" ist Facebook mit mittlerweile über 800 Millionen Nutzern weltweit und mit Google hat inzwischen auch ein weiterer Internetriese ein erfolgreiches Netzwerk gestartet.

Die Netzwerke leben von den Inhalten der Nutzer, die jederzeit und von überall hochgeladen werden können. Es interessieren sich jedoch nicht nur die „Freunde" für diese Inhalte. Auch Unternehmen möchten wissen, was die Mitglieder mögen. So lässt sich Werbung individueller gestalten. Und im Zuge von Bewerbungen kann es vorkommen, dass auch Personalabteilungen zunächst einen Blick ins Profil des Kandidaten werfen. Kompromittierende Fotos oder Pinnwandeinträge sollten sie dabei besser nicht finden.

Soziale Netzwerke sind ein öffentlicher Raum, der nur durch aktive Änderungen der Einstellungen zur Privatsphäre eingeschränkt werden kann. So finden sich bei einigen Netzwerken Hinweise, wie man eigene Daten am besten schützen und was man tun kann, wenn man von anderen Personen belästigt wird (siehe auch Seite 20). Andere Netzwerke tun sich hier schwerer. Daher sollte immer auf Datenschutzaspekte geachtet werden.

Wichtige Hinweise

- Die Angaben auf das Nötigste beschränken. Je mehr Angaben man macht, desto mehr Informationen gelangen nach außen. Einmal Veröffentlichtes ist nur sehr schwer wieder zu entfernen. Das Netz vergisst nicht!
- Nur ausgewählten Personen Zugriff auf das eigene Profil und die darin enthaltenen Informationen gestatten (siehe **www.jugendinfo.de**)
- Die Angaben in den Geschäftsbedingungen und der Datenschutzerklärung sowie Hinweise auf Änderungen des jeweiligen Anbieters sorgfältig lesen
- Netzwerke, die den freiwilligen Verhaltenskodex für Betreiber von Social Communities unterzeichnet haben, finden sich unter **www.fsm.de**

Licht und Schatten

Man findet an einigen Stellen im Internet anstößige Inhalte oder gar solche, die gegen Gesetze verstoßen – mitunter schon durch einen unbedachten Klick. Bei Kindern und Jugendlichen kann dies zu traumatischen Erlebnissen führen.

Nach einer EU-weiten Studie sind im Jahr 2010 fünf Prozent der befragten Kinder und Jugendlichen zufällig über „Schmuddelseiten" gestolpert. In derselben Untersuchung gaben acht Prozent der befragten Kinder und Jugendlichen an, im Netz schon einmal „schlechte Erfahrungen" gemacht zu haben.

Kommerzielle Anbieter nicht jugendfreier Inhalte sind verpflichtet, eine zusätzliche Barriere einzubauen. So wird verhindert, dass Kinder und Jugendliche auf die Inhalte zugreifen können. Ein Altersnachweissystem (auch Altersverifikationssystem, AVS) ist dabei eine technische Lösung, um die Volljährigkeit von Personen zu bestätigen. Anwendung finden diese Systeme vor allem auf Internetseiten mit pornografischen Inhalten oder in Onlineshops, die FSK18-Filme oder entsprechende Computerspiele vertreiben.

5

Prozent der Kinder und Jugendlichen begegnen „Schmuddelseiten“

Weitere Hinweise zur Alterskennzeichnung finden sich zum Beispiel auf www.kjm.de, der Seite der Kommission für Jugendmedienschutz oder auf www.was-spielt-mein-kind.de.

Diese Zugangsblockierung ist in Deutschland gesetzlich vorgeschrieben. Leider ist das jedoch nicht überall so und das Internet kennt bekanntlich keine Grenzen. Daher ist es wichtig, Kindern und Jugendlichen die Funktionsweise des Internet zu erklären und dafür Sorge zu tragen, dass sie nur in bestimmten Bereichen surfen können.

An dieser Stelle ist die frühzeitige Aneignung von Medienkompetenz schon im Kindesalter unerlässlich. So sollten bereits Kindergärten – spätestens jedoch Grundschulen – in Ergänzung zu den Eltern nachhaltig Medienkompetenz vermitteln. Der bayerische Medienführerschein, eine Kampagne der bayerischen Staatsregierung, stellt hierfür geeignete Materialien zur Verfügung. Auch kommerzielle Angebote, wie etwa der Europäische Computerführerschein (www.ecdl.de), bilden eine geeignete Grundlage.

Für Eltern jüngerer Kinder bietet sich der Einsatz von Filtersoftware an. Oder man richtet den Browser so ein, dass bestimmte Seiten nicht verlassen werden können. Bei manchen Betriebssystemen ist es sogar möglich, das ganze System darauf auszurichten. Wichtig ist aber stets: Erklären Sie dem Kind, warum Sie das tun. Oftmals werden die Kinder dann von sich aus nur für sie geeignete Webseiten besuchen.

Ins Netz gegangen

Als Abofalle oder auch Kostenfalle wird der Versuch des Unterschiebens eines entgeltlichen Vertrages im Internet bezeichnet, wobei der Nutzer im Regelfall davon ausgeht, dass das Angebot kostenfrei ist.

Viele Internetnutzer reiben sich verwundert die Augen, wenn zwei Wochen nach dem Besuch einer Internetseite die Rechnung ins Haus flattert. Sie sind in eine Abofalle getappt. Eine typische Methode der Irreführung besteht etwa darin, einzelne Vertragsmodalitäten wie die Kostenpflicht zu verschleiern, indem ein regelmäßig zu entrichtender Euro-Betrag nicht als Zahl, sondern als Fließtext im Kleingedruckten dargestellt wird.

Auch eine Schriftfarbe, die sich kaum vom Hintergrund unterscheidet, ist oft anzutreffen (etwa dunkelgraue Schrift auf hellgrauem Hintergrund). Geködert wird der Besucher in der Regel durch vermeintlich kostenfreie Downloadangebote oder Dienstleistungen – etwa eine Mitfahrbörse oder Hausaufgabenhilfe.

Die Angst, in eine Abofalle zu tappen, ist unter den Internetnutzern groß: Nach einer Untersuchung der Gesellschaft für Konsumforschung im Auftrag des Bayerischen Staatsministeriums der Justiz und für Verbraucherschutz hegt fast jeder sechste der befragten Internetnutzer die Befürchtung, Verträge untergeschoben zu bekommen. Die Folge ist, dass das Vertrauen in das Internet und seine Dienste zurückgeht.

Dies hat die Politik erkannt und Maßnahmen ergriffen: Die sogenannte Button-Lösung sorgt künftig dafür, dass ein im Internet geschlossener Vertrag nur wirksam ist, wenn der Verbraucher ausdrücklich die Kenntnisnahme der Kostenpflichtigkeit durch Klicken auf eine entsprechend beschriftete Schaltfläche („Button") bestätigt.

Eine neue Generation von Kostenfallen lauert in Smartphones. Hier kann bereits ein versehentlicher Klick auf eine Werbefläche, wie sie sich häufig in kostenlosen Apps findet, in die Abofalle führen. Wer sich bereits im Vorfeld schützen will, kann bei seinem Handyanbieter kostenlos eine sogenannte Drittanbietersperre einrichten lassen.

Indizien für versteckt kostenpflichtige Angebote

- aufwändige **Registrierung** erforderlich (Frage, wozu – wenn nicht zur Rechnungsstellung – braucht der Betreiber die gewünschten Daten?)
- viel **Fließtext** etwa am Homepagerand
- „auffällig unauffällige" **Textpassagen** – eventuell farblich gestaltet (farbige Schrift auf farbigem Untergrund)

Ist man in eine Abofalle oder Kostenfalle getappt und zahlt die beigelegte Rechnung nicht, drohen die Betreiber oft mit rechtlichen Schritten oder der Übergabe an ein Inkasso-Unternehmen. Dabei wird auf Gerichtsurteile hingewiesen, um den Druck auf den Verbraucher zu erhöhen.

Was tun, wenn die Falle zugeschnappt ist?

- **Ruhe bewahren und niemals sofort bezahlen.**
  Oft sind die gesetzlich vorgegebenen Grundlagen vom Anbieter nicht eingehalten worden. Der Vertrag ist damit nicht rechtsgültig zustande gekommen und der Nutzer braucht nicht zu zahlen.

- **Nicht einschüchtern lassen.**
  Meist versuchen die Anbieter, den vermeintlichen Vertragspartner mit Druck zum Zahlen zu bringen.

- **Den Anbieter anschreiben.**
  Den Anbieter darauf hinweisen, dass kein Vertrag geschlossen wurde.

- **Vorsorglich den Vertrag widerrufen.**
  Neben dem Widerruf vorsorglich den Vertragsschluss wegen Irrtums und arglistiger Täuschung anfechten.

- **Alles Aufheben und Dokumentieren.**

Im Regelfall kommt kein weiteres Schreiben des Anbieters und wenn doch, sollte man sich nicht verunsichern lassen. Nur die wenigsten Anbieter versuchen, ihre Forderungen einzuklagen, denn sie kennen die einschlägigen Gesetze und Urteile. Gegebenenfalls vorsorglich Rat bei der zuständigen Verbraucherzentrale einholen! Wenn allerdings ein Mahnbescheid vom Gericht kommt, muss man unbedingt innerhalb von 14 Tagen reagieren, denn das Gericht prüft den behaupteten Anspruch im Mahnverfahren nicht.

Informationen und Hilfe im Netz

www.vis.bayern.de (mit Hinweisen auf Musterbriefe zum Download)
www.computerbetrug.de
www.verbraucherzentrale.de

Viren, Würmer, Trojaner & Co.

Schadsoftware ist fast genau so alt wie normale Software. Bereits 1982 wurde ein Virus entwickelt, der aber damals nur als „Scherz" gemeint war und keine dauerhaften Schäden verursachte.

Mittlerweile ist Schadsoftware verantwortlich für Milliarden vernichteter Datensätze und immense materielle Schäden. Waren früher einfache Viren das Maß aller Dinge, so sind es heute Würmer und andere Programme, die gezielt nach Schwachstellen im Rechner des Opfers suchen. Mittlerweile scheinen manche Programme, wie etwa der Computerwurm Stuxnet, so mächtig, dass sie sogar in der Lage sind, die Sicherheitsinfrastruktur eines Landes außer Gefecht zu setzen.

Der Otto-Normalnutzer ist in der Regel nicht Zielscheibe derartiger Programme. Der gezielte Angriff ist und bleibt die Ausnahme. Nichtsdestotrotz kann der Schaden des Einzelnen aber beträchtlich sein. Das fängt an mit dem nicht mehr funktionierenden System und reicht bis zum komplett abgeräumten Bankkonto.

Absolute Sicherheit ist in diesem Zusammenhang nicht zu erreichen. Die Virenschutzhersteller können nur auf bekannte Schädlinge reagieren. Dennoch ist ein regelmäßiges Update der Virenschutzsoftware unerlässlich, denn damit lassen sich zumindest alle bekannten Schädlinge wirksam abwehren.

Schutzmaßnahmen

- **Virenscanner** und **Betriebssystem** immer auf dem neuesten Stand halten (Updatefunktion aktivieren)
- eine **Firewall** installieren/ aktivieren
- keine **unbekannten Dateien** (z.B. aus E-Mails) öffnen
- möglichst **keine fremden Datenträger** (CD-ROM, DVD, USB-Stick, etc.) verwenden

Cybermobbing

Mit dem Begriff des Cybermobbing oder auch des Cyberstalking werden verschiedene Formen der Belästigung, Bedrängung oder Nötigung anderer Personen unter Zuhilfenahme der neuen Medien bezeichnet. Das kann von einfacher Belästigung via elektronischer Nachricht bis hin zur Beleidigung oder üblen Nachrede in Foren, Chatrooms oder Netzwerken gehen.

Oftmals sind sowohl Täter als auch Opfer Kinder oder Jugendliche und in nahezu 80 Prozent der Fälle kennen sich Täter und Opfer auch aus der realen Welt. Die Online-Mobbingszenarien sind daher in vielen Fällen nur die Fortsetzung des Schulhofmobbing. Die Täter sind dabei fast zu gleichen Teilen Jungen und Mädchen.

In einer Studie des Zentrums für empirische pädagogische Forschung (zepf) an der Universität Koblenz-Landau aus dem Jahre 2009 hat jeder sechste der Befragten angegeben, schon selbst Ziel einer Mobbingattacke via Internet gewesen zu sein. Zwar verstehen die meisten Täter dies als Scherz. Ein Scherz mit jedoch oftmals ungeahnten und dramatischen Auswirkungen für das Opfer.

Die Folgen reichen von der sozialen Isolierung, massivem Stress und psychischen Problemen bis hin zum Selbstmord. Denn anders als das „normale" Schulhofmobbing endet die Schikane nicht nach Schulschluss.

Viele Länder wie etwa Bayern haben mittlerweile reagiert und Kampagnen initiiert, die Cybermobbing bekämpfen und den Opfern mit Rat und Tat zur Seite stehen. Denn anders als in anderen Bereichen, ist es beim Cybermobbing oft so, dass die Eltern dem Thema in der Regel noch hilfloser gegenüber stehen als die Kinder und Jugendlichen selbst. Insofern sind viele Länder dazu übergegangen, den Opfern jugendliche Scouts zur Seite zu stellen, die von psychologischen, juristischen und medienpädagogischen Experten ausgebildet werden. Diese raten ihnen, wie mit dem Problem am besten umzugehen ist.

Die Bayerische Staatsregierung hat 2010 den Bayerischen Medienführerschein für Schüler ins Leben gerufen. Wesentliche Bausteine des Führerscheins sind die Förderung der Daten- und Medienkompetenz sowie Hinweise für den Umgang mit Belästigungen im Netz.

Auch viele Netzwerke haben mittlerweile reagiert: Hier können Nutzer, die sich belästigt fühlen, auf einen Button auf ihrer Profilseite klicken. Der Vorgang wird dann unmittelbar dem Netzwerkbetreiber übermittelt.

Erste Hilfe

- Informieren des Netzwerkbetreibers und **Beantragung der Löschung** des diffamierenden Beitrags
- Öffentlichkeit herstellen, wenn möglich auch die Schulleitung informieren
- Bewusstsein schaffen bei Kindern und Jugendlichen
- Dokumentieren Sie die Mobbingattacken akribisch. Die Informationen können bei der Ermittlung der Täter und der Strafverfolgung helfen.

Download abgeschlossen

Im Radio ein tolles Lied gehört? Schnell in die Suchmaschine eingegeben und schon erhält man zahllose Links, wo man das Lied kostenfrei herunterladen kann. Ein Klick und die Kopie ist auf dem eigenen Computer.

Mithilfe des Internet eine Kopie von etwas zu erstellen, ist überaus einfach. Entsprechend finden sich millionenfach Musikstücke, Bilder, Videos und Filme, die illegal kopiert wurden. Das Stichwort hierbei ist jedoch: „illegal".

Selbst bei ganz normalen Nutzern ist die Denkweise, „das lade ich mir mal schnell runter", überaus verbreitet. Sie wissen zwar, dass das eigentlich nicht in Ordnung sein kann, aber das eine Lied… Hinzu kommen die Nutzer, die aus Unwissenheit oder Leichtfertigkeit sogenannte Raubkopien anfertigen. Den jeweiligen Urhebern entsteht dabei ein immenser Schaden, der mit jeder Einzelkopie noch weiter zunimmt.

In diesen Fällen kann es passieren, dass man sich plötzlich hohen Schadensersatzforderungen oder gar einem strafrechtlichen Ermittlungsverfahren gegenüber sieht. Meist ist die Rechtsprechung eindeutig: Der Schädiger muss zahlen – und zwar nicht zu knapp!

Und nicht nur der eigene widerrechtliche Download kann folgenreich sein: Auch für den der Kinder oder gar für den durch unbekannte Dritte kann man haftbar sein. Als Betreiber eines WLAN-Netzes muss man dafür sorgen, dass niemand über den eigenen Anschluss widerrechtlich Dateien herunterladen kann. Dies geschieht durch eine Absicherung des Zugangs mit Kennwörtern und durch Verschlüsselung (z.B. WPA2).

Sorgen Sie dafür, dass auch Ihre Kinder nicht über Ihren Computer widerrechtlich Dateien herunterladen. Bei einigen hundert Dateien summiert sich der Schadensersatz schnell auf hohe vierstellige Beträge. Führen Sie mit Ihren Kindern dahingehende Gespräche oder lassen Sie sie – soweit erforderlich – nicht allein im Netz surfen.

Tauschbörsen

Besonders problematisch ist die aktive Teilnahme an einer Tauschbörse. Nahezu alle großen Verwerter beschäftigen Kanzleien oder Internetdetektive, die sich auf das sogenannte File-Sharing spezialisiert haben. Spüren sie Teilnehmer einer illegalen Tauschbörse auf, drohen diesen hohe Schadensersatzforderungen und teilweise auch strafrechtliche Konsequenzen.

Die Abmahnung

Dabei handelt es sich um die förmliche Aufforderung, eine bestimmte Handlung (hier das Herunterladen) künftig zu unterlassen. Sie ist eine Art außergerichtliches Einigungsangebot des Rechteinhabers, um die Sache schnell und unbürokratisch zu regeln. Im Regelfall enthält die Abmahnung mehrere Punkte: Neben der Löschung der Datei wird ein Pauschalbetrag für die Rechtsverletzung und die Kosten des Anwalts erhoben sowie die Unterzeichnung einer Unterlassungserklärung verlangt. Oftmals ist die Rechtslage so eindeutig, dass nichts weiter übrig bleibt als zu zahlen. Die beigefügten Unterlassungserklärungen gehen jedoch oft zu weit: Im Zweifel fachkundigen Rat einholen, oder – noch besser – lieber gleich die Hände weg von kostenloser Musik im Netz.

Sie haben Post!

Als Spam wird die massenhafte Übersendung von unerwünschten E-Mail-Nachrichten bezeichnet. Inhalte sind zumeist Werbung oder Phishingversuche.

Der Begriff stammt aus dem Englischen und bedeutet „Abfall". Nach Schätzungen sind beinahe 90 Prozent des gesamten weltweiten E-Mail-Aufkommens dem Spamming geschuldet. Spams verursachen einen enormen volkswirtschaftlichen Schaden und verschwenden eine Unmenge an Ressourcen.

Die rechtliche Verfolgung von Spamming ist sehr schwierig. Zwar hat der Empfänger grundsätzlich einen Unterlassungsanspruch gegenüber dem Versender, aber die Geltendmachung erweist sich in der Realität oftmals als nahezu unmöglich.

Schutzmaßnahmen

- Einsatz von Spam-Filtern/ Nutzung von Blacklists
- Verwendung von „Wegwerf-Adressen"/ Sparsamkeit bei der Bekanntgabe der eigenen Mailadresse
- niemals auf Spam antworten, jede Spam-Mail löschen
- Eintrag in die Robinson-Liste (**www.robinsonliste.de**)

Weitere Informationen im Netz

- **Verbraucherportal VIS Bayern** mit aktuellen Informationen der Bayerischen Staatsregierung zu allen wichtigen Verbraucherthemen wie Verbraucherrechte, Ernährung, technische Produkte, Finanzen & Versicherungen und Energie. Die Sicherheit im Netz bildet im Bereich Daten und Medien einen neuen Schwerpunkt.
  www.vis.bayern.de

- **Verbraucherservice der Bundesnetzagentur**, zentrale Anlaufstelle für Endkunden, die Schwierigkeiten mit ihren Telekommunikationsanbietern haben (auch Spam und Rufnummernmissbrauch)
  http://www.bundesnetzagentur.de

  Schicken Sie die erhaltenen Werbemails mit einer kurzen Sachverhaltsdarstellung und der Bitte um Einschreiten der BNetzA an die Fax-Nummer 06321 934-111 oder die E-Mail-Adresse: rufnummernmissbrauch@bnetza.de

- **BSI für Bürger**, das Bundesamt für Sicherheit in der Informationstechnik informiert über Risiken, Gefahren und Befürchtungen beim Einsatz der Informationstechnik und versucht Lösungen dafür zu finden.
  https://www.bsi-fuer-buerger.de

- Mit der Webseite **Internet-Beschwerdestelle.de** bieten die Organisatoren eco und fsm Nutzern die Möglichkeit, sich an einer Stelle über verschiedene Aspekte zur Förderung des sichereren Umgangs mit dem Internet zu informieren und Beschwerden einzureichen.
  www.internet-beschwerdestelle.de

- Der Verein **„Deutschland sicher im Netz“** hat das Ziel, bei Verbrauchern und in Unternehmen ein Bewusstsein für einen sicheren Umgang mit Internet und IT zu fördern.
  https://www.sicher-im-netz.de

- Umfangreiche **Hinweise der Technischen Universität Berlin** zu IT-Sicherheit, sicherer Nutzung des Internet und zum Schutz vor Viren.
  http://hoax-info.tubit.tu-berlin.de/software/antivirus.shtml

- »**Verbraucher sicher online**« ist ein vom Bundesverbraucherschutzministerium gefördertes Projekt der TU Berlin. Ziel ist es, Verbraucher über die sichere Internetnutzung, den sicheren Umgang mit Computern, Barrierefreiheit sowie den Zugang zu digitalen Inhalten und Informationen umfassend und verständlich zu informieren.
  www.verbraucher-sicher-online.de

- **Sicherheitsportal des Heise-Verlages**, Informationsangebot zu allen Belangen der IT-Sicherheit. „Browser-Check" und „E-Mail-Check" ermöglichen Nutzern alle gängigen Internet-Produkte auf Schwachstellen zu prüfen.
  www.heise.de/security/

- **Informationsseite des Bundesverbandes Digitale Wirtschaft** rund um das Thema Cookies.
  www.meine-cookies.org

- **Verbraucher haben Rechte** ist eine Aufklärungskampagne des Verbraucherzentrale Bundesverbandes (vzbv) mit dem Ziel, Verbraucher zu befähigen, sich sicher im Internet zu bewegen und aktiv zu partizipieren.
  www.surfer-haben-rechte.de

- **Webseite des Bundesdatenschutzbeauftragten** mit zahlreichen Hinweisen rund um das Thema Datenschutz im Netz, auch mit kostenlosem Selbsttest „Datenklau – sind Sie ausreichend geschützt?" www.bfdi.bund.de

- Bei **klicksafe.de** findet man u.a. eine Anleitung, wie man seinen PC schützt und Kindersicherungen einbaut.
  https://www.klicksafe.de

- Das **Internet-ABC** bietet Kindern und Erwachsenen Infos, Tipps und Tricks rund um das Internet - ob für Anfänger oder Fortgeschrittene. www.internet-abc.de

- **Verbraucherzentrale Bayern e.V.**
  www.verbraucherzentrale-bayern.de

- **VerbraucherService Bayern im KDFB e.V.**
  www.verbraucherservice-bayern.de

- Das **Landesamt für Datenschutzaufsicht** informiert über aktuelle Fragen des Datenschutzes und überwacht die Einhaltung der datenschutzrechtlichen Vorschriften im nichtöffentlichen Bereich. www.datenschutzaufsicht.bayern.de

- Der Internetauftritt der Bayerischen Staatsregierung zur Jugendmedienschutzkampagne **„Was spielt mein Kind?"** informiert über die Bedeutung des Jugendmedienschutzes im Hinblick auf Computer- und Konsolenspiele und klärt vor allem Eltern über den richtigen Umgang mit den Spielgewohnheiten ihrer Kinder auf.
  www.was-spielt-mein-kind.de

- Neben Informationen zum Thema Jugendschutz ist es der **Aktion Jugendschutz, Landesarbeitsstelle Bayern e.V.** ein wichtiges Anliegen, medienpädagogische Materialien und Angebote zu entwickeln und so zu einem positiven und konstruktiven Medienumgang bei Kindern und Jugendlichen beizutragen. www.bayern.jugendschutz.de

- **ELTERNTALK** steht für: Fachgespräche von Eltern für Eltern. Eltern treffen sich im privaten Rahmen zu einem Erfahrungsaustausch über Erziehungsfragen in der Familie. Im Mittelpunkt stehen die Themen Medien, Konsum und Suchtvorbeugung. www.elterntalk.net

- **www.webhelm.de** ist die Werkstatt-Community für Daten, Rechte und Persönlichkeit. Hier findet man Informationen zum Thema Web 2.0 und Tipps für den Umgang mit dem Internet. Pädagoginnen und Pädagogen finden im Bereich „Materialpaket" Hintergrundinformationen und Anregungen für ihre Arbeit. www.webhelm.de

- Ziel des **Medienführerscheins Bayern** ist es, Kinder, Jugendliche und Erwachsene in ihrer Medienkompetenz zu stärken. Als Portfolio konzipiert, bietet er Informationen und Materialien, die eine auf die Bedürfnisse unterschiedlicher Zielgruppen zugeschnittene Auseinandersetzung mit relevanten Medienthemen ermöglicht.
  www.medienfuehrerschein.bayern.de

- Im **Portal der polizeilichen Kriminalprävention des Bundes und der Länder** finden sich umfassende Informationen zu Gefahren im Internet und zur Medienkompetenz. Auch Infomaterialen sind abrufbar. www.polizei-beratung.de

Herausgeber
Initiative D21 e.V. und
Bayerisches Staatsministerium
der Justiz und für Verbraucherschutz

Redaktion
Martin Falenski (Initiative D21) – V.i.S.d.P.

Gestaltung
Gordon Albrecht, mail@newww.de

Druck
ARIADNE MEDIENAGENTUR
www.ariadne-medienagentur.de

Kontakt
Initiative D21, Reinhardtstraße 38, 10117 Berlin
kontakt@initiatived21.de, **www.initiatived21.de**

Bayerisches Staatsministerium der Justiz und für Verbraucherschutz,
Prielmayerstraße 7, 80335 München
poststelle@stmjv.bayern.de, **www.justiz.bayern.de**

Auch wenn im Text nicht immer explizit ausgeschrieben, beziehen sich alle personenbezogenen Formulierungen auf weibliche und männliche Personen.

Aufbruch Bayern

Bildnachweise

Seite 1	Safe Internet @ slobo - iStockphoto.com
Seite 2, 4	Woman Shopping Online @ Brainsil - iStockphoto.com
Seite 2, 8	Padlock @ sodafish - iStockphoto.com
Seite 2, 14	Using laptop © vm - iStockphoto.com
Seite 2, 22	Identity Theft @ fredpal - iStockphoto.com
Seite 2, 24	Flying Envelopes @ eyeidea - iStockphoto.com
Seite 5	Https secure @ OneO2 - iStockphoto.com
Seite 16	„Bezahlen"-Button © entwurfsmaschine - Fotolia.com
Seite 16	Abo Falle 1 © illuminator - Fotolia.com
Seite 18	Datenschutz © Aamon - Fotolia.com
Seite 20	Cyber Bullying @ Rivendellstudios - iStockphoto.com