Bayerisches Staatsministerium für
Umwelt und Verbraucherschutz

GUT ZU WISSEN
VERBRAUCHERSCHUTZ IN BAYERN

# Sicher Surfen

## Chancen nutzen und Risiken erkennen

INITIATIVE D21

3. Auflage

# Inhalt

# Vorwort

Nach der industriellen Revolution im 19. Jahrhundert erleben wir mit dem digitalen Wandel der letzten Jahrzehnte die nächste große Revolution. Neben den vielen Vorteilen und Möglichkeiten, die ein modernes und vernetztes Leben bietet, dürfen die Gefahren weder verdrängt noch überbewertet werden.

Vergleichbar mit der Teilnahme am Straßenverkehr müssen wir grundsätzliche Regeln im Internet beachten. Diese Regeln zu verstehen, ist essentiell, um sich die **Chancen** der digitalisierten Welt zu erschließen **und Risiken** zu erkennen.

Im Internet ist der Nutzer nicht nur Konsument, sondern gleichzeitig Produzent von Inhalten und auch **Daten**.

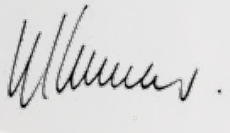
In der zunehmend digitalisierten Welt hinterlassen wir Informationen. Diese ermöglichen Rückschlüsse auf unsere Person, unsere Vorlieben, Gewohnheiten – wertvolle Informationen für Unternehmen.

Daten sind eine neue Währung und wir müssen kompetent und souverän entscheiden, wie viel wir bereit sind, für einen Dienst von uns preiszugeben.

Vor dem Überqueren einer Straße schauen wir erst nach links und rechts, bei einer roten Ampel bleiben wir stehen; einfache Regeln, um uns abzusichern.

So gilt es auch im Internet zu lernen, Risiken abzuschätzen und allgemeingültige Handlungsweisen zu entwickeln. **Medienkompetenz** ist in der digitalisierten Welt genauso eine Notwendigkeit wie das umsichtige Verhalten im Straßenverkehr.

**Ulrike Scharf MdL**
Bayerische Staatsministerin für Umwelt und Verbraucherschutz



**Hannes Schwaderer**
Präsident der Initiative D21 e.V.

# Datenschutz im Internet

Der Schutz persönlicher Daten ist vor allem in der heutigen Zeit der Digitalisierung und angesichts der Vielzahl der Daten, die jeder Nutzer hinterlassen kann, immer wichtiger. Über das Internet können schnell, einfach und sehr umfangreich Daten analysiert werden, die Auskunft über die eigene Person, den aktuellen Standort, das eigene Verhalten und Vorlieben geben. Für Unternehmen sind Daten die **neue Währung** im Zeitalter der Digitalisierung.

Daher ist es wichtig, beim Online-Einkaufen oder bei Bankgeschäften im Internet, bei der Nutzung von Sozialen Medien oder beim Versenden von E-Mails zu wissen, wie man die eigenen Daten vor unberechtigten Zugriffen schützt.

Es ist empfehlenswert für jeden Nutzer, sich bewusst zu machen, wem man welche personenbezogenen Angaben übergibt. Eine gute technische Sicherheit von Computer, Mobiltelefon und anderen Geräten sowie deren Anwendungen, aber auch das eigene Nutzerverhalten im Internet tragen zu einem **wirksamen Schutz der eigenen Daten** bei.

Lesen Sie sich daher stets die allgemeinen Datenschutzbestimmungen der Anwendungen und Internetseiten durch. Nutzen Sie Ihre Rechte in puncto Datenschutz.

Sofern Sie personenbezogene Daten hinterlassen, können Sie bei dem Anbieter jederzeit die:

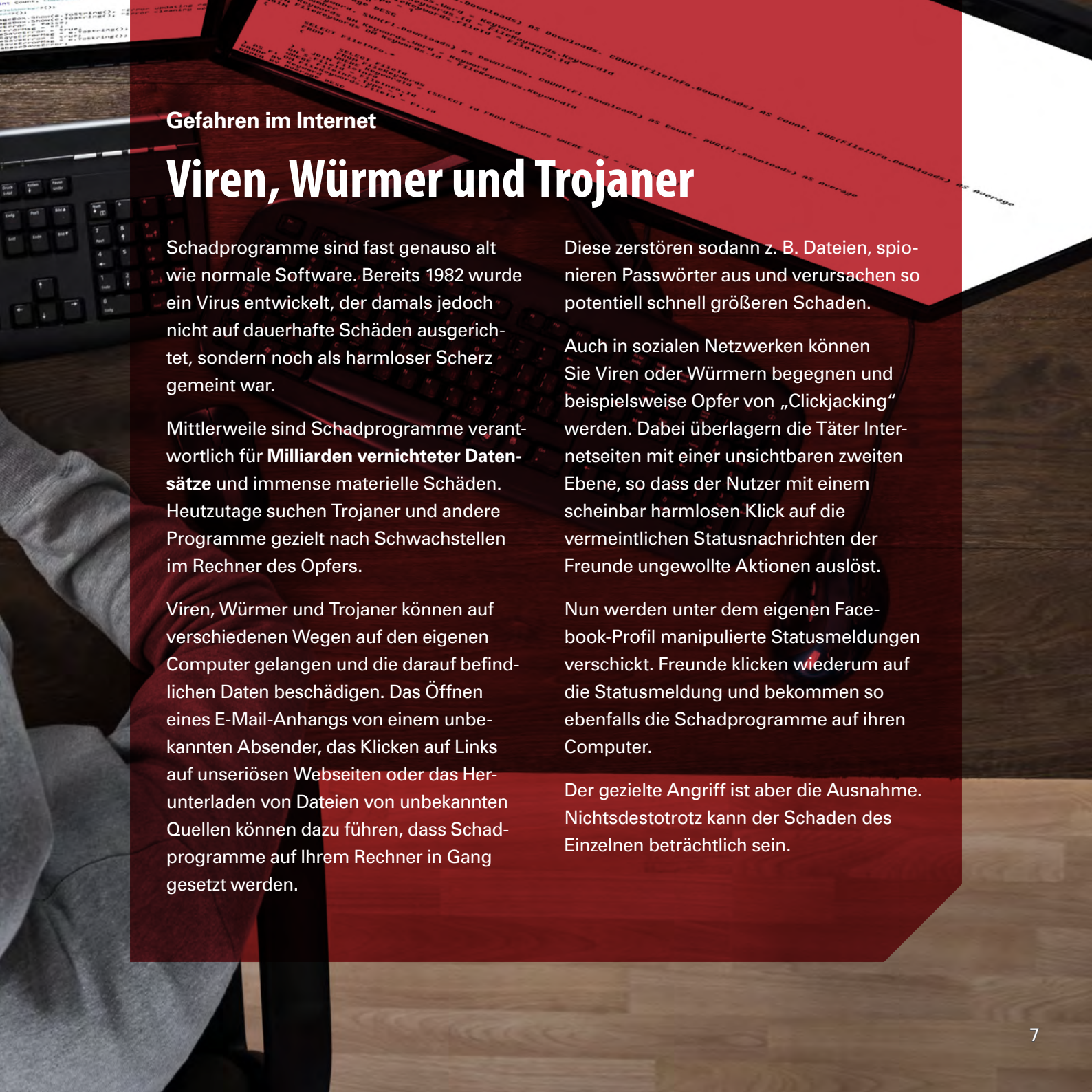
- ⇨ Löschung, Benachrichtigung, Sperrung oder Berichtigung Ihrer personenbezogenen Daten beantragen.
- ⇨ Auskunft beantragen, welche Daten über Sie erhoben wurden und wozu sie verwendet werden.

# Tipps

- ⇨ Seien Sie grundsätzlich umsichtig im Umgang mit personenbezogenen Daten.
- ⇨ Gehen Sie mit besonders sensiblen personenbezogenen Daten (z. B. Ihren Gesundheitsdaten) sorgsam um.
- ⇨ Vermeiden Sie es, Anwendungen zu verknüpfen, bei denen Sie bereits eine Vielzahl von Daten hinterlassen haben (bspw. Amazon-Konto mit Facebook-Konto).
- ⇨ Löschen Sie in regelmäßigen Abständen in den Browsereinstellungen die Cookies, um die Erfassung Ihres Nutzerverhaltens zu reduzieren.
- ⇨ Überprüfen Sie bei Ihren Endgerät, welche Daten (z. B. Ortungsfunktion, Zugriff auf Telefonbuch) die voreingestellten Datenschutzfunktionen erlauben (in „Einstellungen“ zu finden).
- ⇨ Ihre Standortdaten schützen Sie, indem Sie den Zugriff von Anwendungen (Apps) auf die GPS-Funktion in Ihrem Handy vermeiden (in „Einstellungen“ zu finden).

# Wichtige Schutzmaßnahmen

- **Grundsätzlich:** Eine **Firewall** installieren und auch aktivieren!
- Installieren Sie einen **Virenschutz** und überprüfen Sie Ihren Computer regelmäßig mit dem Programm.
- Halten Sie Virenscanner und Betriebssystem immer auf dem neuesten Stand (automatische Updatefunktion aktivieren).
- Öffnen Sie grundsätzlich keine Dateien und klicken Sie nicht auf Links, wenn Ihnen die Quelle unbekannt ist (z. B. Werbe-E-Mails).
- Verwenden Sie keine **Datenträger unbekannter Quelle** (z. B. gefundene CD-ROMs oder USB-Sticks).
- Sollten Sie in sozialen Netzwerken wie Facebook auf Spam geklickt haben, überprüfen und löschen Sie ggf. dadurch installierte Anwendungen und informieren Sie Ihre Kontakte.



Gefahren im Internet

# Viren, Würmer und Trojaner

Schadprogramme sind fast genauso alt wie normale Software. Bereits 1982 wurde ein Virus entwickelt, der damals jedoch nicht auf dauerhafte Schäden ausgerichtet, sondern noch als harmloser Scherz gemeint war.

Mittlerweile sind Schadprogramme verantwortlich für **Milliarden vernichteter Datensätze** und immense materielle Schäden. Heutzutage suchen Trojaner und andere Programme gezielt nach Schwachstellen im Rechner des Opfers.

Viren, Würmer und Trojaner können auf verschiedenen Wegen auf den eigenen Computer gelangen und die darauf befindlichen Daten beschädigen. Das Öffnen eines E-Mail-Anhangs von einem unbekannten Absender, das Klicken auf Links auf unseriösen Webseiten oder das Herunterladen von Dateien von unbekannten Quellen können dazu führen, dass Schadprogramme auf Ihrem Rechner in Gang gesetzt werden.

Diese zerstören sodann z. B. Dateien, spionieren Passwörter aus und verursachen so potentiell schnell größeren Schaden.

Auch in sozialen Netzwerken können Sie Viren oder Würmern begegnen und beispielsweise Opfer von „Clickjacking“ werden. Dabei überlagern die Täter Internetseiten mit einer unsichtbaren zweiten Ebene, so dass der Nutzer mit einem scheinbar harmlosen Klick auf die vermeintlichen Statusnachrichten der Freunde ungewollte Aktionen auslöst.

Nun werden unter dem eigenen Facebook-Profil manipulierte Statusmeldungen verschickt. Freunde klicken wiederum auf die Statusmeldung und bekommen so ebenfalls die Schadprogramme auf ihren Computer.

Der gezielte Angriff ist aber die Ausnahme. Nichtsdestotrotz kann der Schaden des Einzelnen beträchtlich sein.

Gefahren im Internet

# Identitätsdiebstahl/ -missbrauch und Phishing

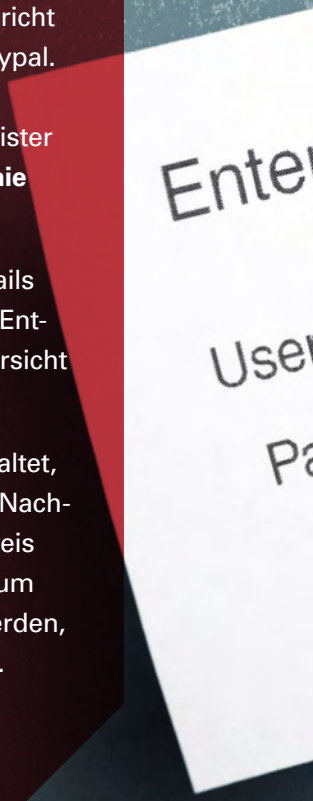
Beim Identitätsdiebstahl oder Identitätsmissbrauch gibt eine Person vor, eine andere zu sein, um auf diese Weise Waren zu bestellen ohne zu bezahlen oder um auch Personen bedrohen oder beleidigen zu können, ohne für die Konsequenzen einzustehen. Sicherheit bieten Identifikationsverfahren wie beispielsweise die Online-Ausweisfunktion des Personalausweises, die in der digitalen Welt als Identitätsnachweis verwendet werden kann.

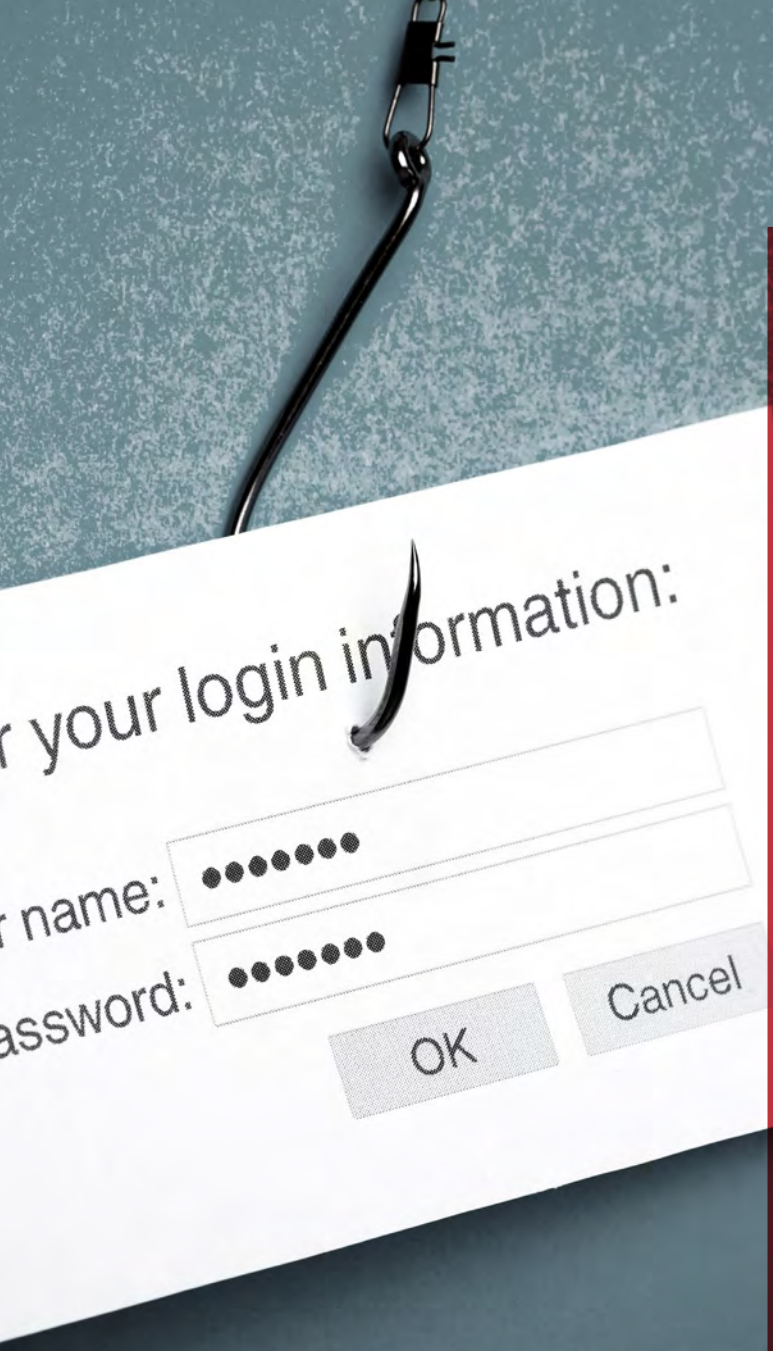
Mit Phishing ist der Versuch gemeint, Nutzer dazu zu bewegen, sicherheitsrelevante Informationen wie Kontodaten, PINs und TANs preiszugeben, indem ihnen ein vermeintlich seriöser Sachverhalt, z. B. durch eine gefälschte E-Mail, vorgespielt und der Nutzer so verleitet wird, auf bestimmte Links zu klicken. Als Absender der E-Mail werden meistens seriöse Institutionen wie Bankinstitute oder Kommunikationsanbieter vorgegaukelt.

Es gibt jedoch Anzeichen, dass die Nachricht nicht vom angegebenen Absender stammen könnte. So wird als Anrede oft nur die Floskel „Sehr geehrter Kunde“ verwendet und die E-Mail-Adresse entspricht nicht der offiziellen Endung (z.B. @paypal.com). Zudem gilt als Faustregel, dass Banken und Kommunikationsdienstleister **Kundendaten sowie PINs und TANs nie per E-Mail abfragen** werden.

Häufig finden sich in den Phishing-Mails Grammatik- oder Rechtschreibfehler. Entdeckt man solche, ist in jedem Fall Vorsicht geboten.

Teilweise sind Phishing-Mails so gestaltet, dass bereits das Anklicken des in der Nachricht enthaltenen Links (z. B. mit Hinweis auf eine Telefonrechnung) ausreicht, um mit Schadprogrammen infiziert zu werden, z. B. einem Virus oder einem Trojaner.






# Wichtige Schutzmaßnahmen

- **Grundsätzlich:** Haben Sie ein **gesundes Misstrauen** und hinterfragen Sie die Identität und den angegebenen Absender bei elektronischer Kommunikation kritisch.
- Öffnen Sie E-Mails von unbekannten Absendern, wenn überhaupt, nur im Textmodus und öffnen Sie keine Anhänge und klicken nicht auf Links.
- Übermitteln Sie sensible und geheime Informationen möglichst nur verschlüsselt oder nutzen Sie in der Kommunikation die DE-Mail der Deutschen Post.
- Wenn Sie Opfer eines Identitätsdiebstahls geworden sind, dann ändern Sie Ihre Passwörter und informieren Sie ggf. den Anbieter über den Missbrauch. Setzen Sie auch Ihre Nachbarn und Bekannte in Kenntnis, dass Sie keine Paketsendungen von Ihnen annehmen sollen. Sollte eine Straftat vorliegen, erstatten Sie Anzeige oder suchen Sie anwaltliche Hilfe auf.

# Erste Hilfe Cybermobbing

- ⇨ Informieren Sie den Netzwerkbetreiber (z. B. Facebook) und beantragen Sie die Löschung des diffamierenden Beitrags.
- ⇨ Stellen Sie Öffentlichkeit her und informieren Sie Lehrer und Schulleitung.
- ⇨ Für eine Strafverfolgung mit Hilfe der Polizei ist eine **akribische Dokumentation** (z. B. über Screenshots der Seiten, Protokollieren der Vorfälle) der Mobbingattacken notwendig. Jede Information kann bei der Ermittlung der Täter und der Strafverfolgung helfen.
- ⇨ Reden Sie mit Kindern und Jugendlichen über das Thema Cybermobbing und deren Folgen.

Gefahren im Internet

# Cybermobbing

Mit dem Begriff des Cybermobbings oder auch des Cyberstalkings 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 Täter wie Opfer Kinder oder Jugendliche und in nahezu 80 Prozent der Fälle kennen sich Täter und Opfer auch aus der analogen Welt.

Die Online-Mobbingszenarien sind daher in vielen Fällen die Fortsetzung des Schulhofmobbings, wobei Jungen und Mädchen fast zu gleichen Teilen die Täter sind und entsprechende Aktionen meist als Scherz gemeint sind. Ein Scherz mit jedoch oftmals ungeahnten und dramatischen Auswirkungen für das Opfer. Die Folgen reichen von der sozialen Isolierung, massivem Stress bis zu psychischen Problemen. Denn anders als das „normale“ Schulhofmobbing endet die Schikane nicht nach Schulschluss.

Dem Thema Cybermobbing stehen die Eltern in der Regel noch hilfloser gegenüber als die Kinder und Jugendlichen selbst. Bayern und andere Länder haben reagiert und Kampagnen initiiert, die Cybermobbing bekämpfen und den Opfern mit Rat und Tat zur Seite stehen (z. B. **www.klicksafe.de**). Den Opfern werden jugendliche Scouts zur Seite gestellt, die von psychologischen, juristischen und medienpädagogischen Experten ausgebildet werden. Diese raten dann, wie mit dem Problem am besten umzugehen ist.

Die Bayerische Staatsregierung hat zudem 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.



# Sexting

Der Begriff Sexting stammt aus dem Englischen und leitet sich von „Sex“ und „texting“ (= Schreiben von Kurznachrichten) ab. Jugendliche machen dabei erotische oder pornografische Bilder bzw. Videos von sich und verschicken sie per Handy oder Smartphone an andere.

Die Gründe sind unterschiedlich: Teilweise möchten Jugendliche herausfinden, wie interessant oder begehrenswert sie auf andere wirken. Andere verschicken innerhalb einer Beziehung entsprechende Fotos im Vertrauen der Geheimhaltung, wieder andere wollen sich schlicht beweisen und versenden sie als Mutprobe innerhalb der Clique.

Jugendliche können bei der Versendung derartiger Fotos schnell Opfer von Cybermobbing werden. Ist die Versendung in einer Beziehung vielleicht noch unbedenklich, können, etwa aus Rache nach der Beendigung der Beziehung, entsprechende Fotos zum Alptraum werden.

Wenn die Fotos und Aufnahmen an andere Personen weitergegeben werden, könnte den abgebildeten Personen **Erpressung oder Diffamierung drohen**. Die Fotos können außerdem an Fremde mit pädophilen Neigungen gelangen.

# Wichtige Schutzmaßnahmen

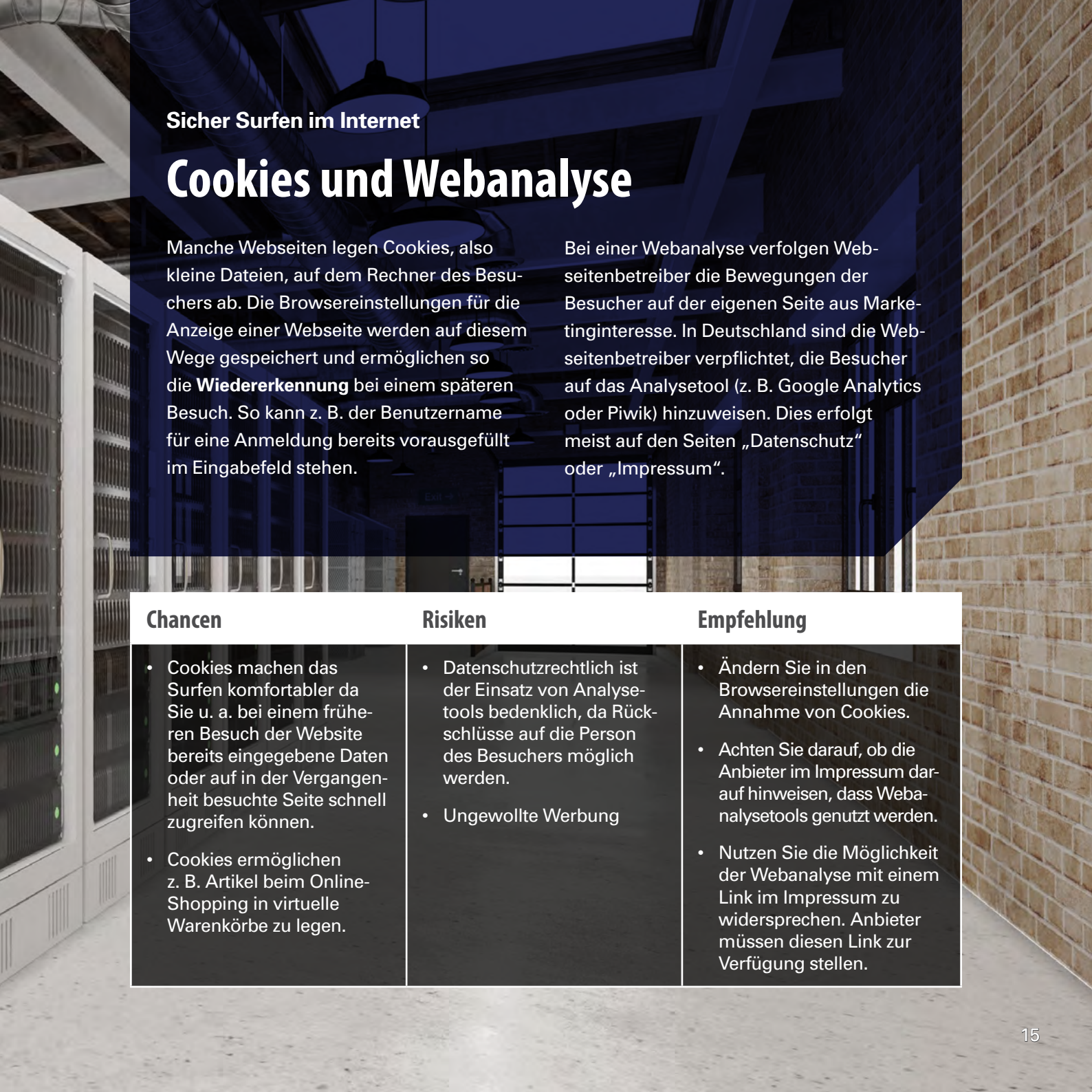
- ⇨ **Grundsätzlich**: Eltern und Lehrer sollten Kinder für die Folgen der Veröffentlichung gerade digitaler Bilder **sensibilisieren** und offen über das Thema sprechen.
- ⇨ Seien Sie achtsam, mit wem sich ihr Kind austauscht und seien Sie gesprächsbereit.
- ⇨ Vereinbaren Sie mit Ihrem Kind Verhaltensregeln im Umgang mit Diensten (z. B. auf Herausgabe persönlicher Bilder und auf Weiterleitung von Bildern der Freunde möglichst verzichten, bei Bildern oder Kontaktaufnahmen von fremden Personen stets wachsam sein).
- ⇨ Melden Sie Belästigungen jeder Art umgehend bei **www.jugendschutz.net** oder **www.i-kiz.de**. In schweren Fällen kontaktieren Sie umgehend die Polizei.
- ⇨ Dokumentieren Sie die Vorfälle für die weitere Aufklärung.

Sicher Surfen im Internet

# Cloud-Computing

Cloud-Computing bedeutet, dass ein Teil der Hard- oder der Software vom Nutzer nicht mehr selbst betrieben, sondern bei einem oder mehreren Anbietern als Dienst gemietet wird. Die Anwendungen und Daten befinden sich dann nicht mehr auf dem lokalen Rechner, sie befinden sich in der sogenannten „Cloud“ (engl. für Wolke). Der Zugriff erfolgt über das Internet. Die Spannbreite der Angebote ist riesig und reicht vom Versand von Nachrichten über einen webbasierten E-Mail-Dienst, über **Web-Speichermöglichkeiten** für Fotos bis zu hochkomplexen Anwendungen für Unternehmen und Organisationen. Entsprechende Dienste sind zum Beispiel web.de oder gmx.de für E-Mails und Dropbox oder One Drive als Online-Speicher.

| Chancen | Risiken | Empfehlung |
|---|---|---|
| • Einsparen von Speicherplatz auf lokalem Rechner, da Daten oder Anwendungen ausgelagert sind<br>• Der Nutzer kann von überall auf seine Daten und Software zugreifen, egal ob über Smartphone, Notebook oder Tablet. | • Viele Cloud-Dienste haben ihren Sitz in den USA, Rechte bei Verstößen gegen den Datenschutz sind möglicherweise nur schwer durchsetzbar.<br>• Vertragliche Haftungsausschlüsse bei Datenverlust | • Überprüfen Sie die Datenschutzhinweise hinsichtlich Datenverlust oder -diebstahl.<br>• Wählen Sie zertifizierte Anbieter, z. B. nach Kriterien des Bundesamtes für Sicherheit in der Informationstechnik (BSI).<br>• Vorsicht mit personenbezogenen und sensiblen Daten, keine Speicherung von persönlichen Passwörtern und Bankdaten<br>• Je nach Sensibilität der Daten besser auf europäische Cloud-Anbieter zurückgreifen. |



Sicher Surfen im Internet

# Cookies und Webanalyse

Manche Webseiten legen Cookies, also kleine Dateien, auf dem Rechner des Besuchers ab. Die Browsereinstellungen für die Anzeige einer Webseite werden auf diesem Wege gespeichert und ermöglichen so die **Wiedererkennung** bei einem späteren Besuch. So kann z. B. der Benutzername für eine Anmeldung bereits vorausgefüllt im Eingabefeld stehen.

Bei einer Webanalyse verfolgen Webseitenbetreiber die Bewegungen der Besucher auf der eigenen Seite aus Marketinginteresse. In Deutschland sind die Webseitenbetreiber verpflichtet, die Besucher auf das Analysetool (z. B. Google Analytics oder Piwik) hinzuweisen. Dies erfolgt meist auf den Seiten „Datenschutz“ oder „Impressum“.

| Chancen | Risiken | Empfehlung |
|---|---|---|
| • Cookies machen das Surfen komfortabler da Sie u. a. bei einem früheren Besuch der Website bereits eingegebene Daten oder auf in der Vergangenheit besuchte Seite schnell zugreifen können.<br>• Cookies ermöglichen z. B. Artikel beim Online-Shopping in virtuelle Warenkörbe zu legen. | • Datenschutzrechtlich ist der Einsatz von Analysetools bedenklich, da Rückschlüsse auf die Person des Besuchers möglich werden.<br>• Ungewollte Werbung | • Ändern Sie in den Browsereinstellungen die Annahme von Cookies.<br>• Achten Sie darauf, ob die Anbieter im Impressum darauf hinweisen, dass Webanalysetools genutzt werden.<br>• Nutzen Sie die Möglichkeit der Webanalyse mit einem Link im Impressum zu widersprechen. Anbieter müssen diesen Link zur Verfügung stellen. |

Sicher Surfen im Internet

# Gaming – Computerspiele

Mit der Verbreitung von Smartphones und Tablets ist auch das Angebot an Spiele-Apps in den letzten Jahren stark angestiegen. Gerade hier hat sich die Zielgruppe auf den **Querschnitt der Gesellschaft** ausgeweitet. Eltern sind bei dem Thema Computerspiele zunehmend verunsichert, denn die Risiken, die mit Computerspielen einhergehen, stehen verstärkt im medialen Fokus.

| Chancen | Risiken | Empfehlung |
|---|---|---|
| • Computer- und Videospiele können die Hand-Augen-Koordination verbessern oder das Gedächtnis durch entsprechende Quiz- und Denkspiele (z. B. Sudoku) trainieren.<br>• Für Kinder und Jugendliche gibt es viele Angebote mit pädagogischem Hintergrund zum spielerischen Lernen von z. B. Lesen, Rechnen und physikalischen Grundgesetzen. | • Computer und Videospiele können zur Sucht werden und Kinder und Jugendliche in der Folge sozial isolieren.<br>• Gewaltverherrlichende Spiele haben das Potenzial die Wahrnehmung im realen Leben zu verzerren.<br>• Versteckte Abo-Kosten, mangelnder Datenschutz sowie die Gefahr von Schadprogrammen besonders bei Online-Spielen (Browserspiele). | • Eltern sollten mit Kindern gemeinsam über potentielle Risiken sprechen.<br>• Achten Sie auf das gesunde Maß beim Computerspielen. Je nach Alter wird eine maximale Spieldauer von 20 bis 120 Minuten pro Tag empfohlen.<br>• Jüngere Kinder zwischen 4 und 6 Jahren sollten nur im Beisein der Eltern spielen.<br>• Nutzen Sie Spiele, die für die jeweilige Altersgruppe geeignet sind (achten Sie auf die Altersangaben **www.usk.de**).<br>• Begeistern Sie für Spiele, die für innovative, kulturelle und pädagogische Werte stehen (**www.deutscher-computerspielpreis.de**). |

# Grundsätzliches zum Thema Online-Gaming

- ⇨ Sorgen Sie dafür, dass die genutzte Hardware (PC, Tablet, Smartphone, etc.) durch ein Virenschutzprogramm sowie eine Firewall gesichert ist.
- ⇨ Seriosität des Anbieters: Vergewissern Sie sich, ob der Anbieter alle rechtlich relevanten Informationen, wie zum Beispiel das Impressum oder verständliche AGB, bereithält.
- ⇨ Achten Sie darauf, welche Daten Sie in Registrierungsformularen angeben. Prüfen Sie die Datenschutzerklärungen des Anbieters und nutzen Sie **sichere Passwörter** (Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen).
- ⇨ Viele Internetspiele werden kostenpflichtig angeboten. Hier sollten immer mehrere Zahlungsarten angeboten werden. Ein Kriterium für Seriosität und sicheren Zahlungsverkehr kann das Vorhandensein eines anerkannten **Internet-Gütesiegels** sein (**www.internet-guetesiegel.de**).
- ⇨ Achten Sie besonders bei Onlinespielen auf Kostenfallen wie Abonnements. Einige Spiele, die auf den ersten Blick kostenlos sind, bieten Kaufoptionen im Spiel an, so genannte In-App oder In-Game Käufe. Lesen Sie daher immer die Nutzungsbedingungen und verschaffen Sie sich ein Überblick über die Gesamtkosten.
- ⇨ Nutzen Sie einen Jugendschutzfilter. Mehr dazu erfahren Sie auf **www.klicksafe.de**.

Sicher Surfen im Internet

# Fitnessapps – Tracking von Vitalfunktionen

Fitnessapps, Wearables oder „Self-Tracking": Hinter diesen Begriffen steckt ein seit 2012 in Deutschland aufkommender neuer Trend. Wearables (englisch für Tragbares) sind tragbare Computersysteme, die als Armband getragen werden und stetig **Bewegungs- und Gesundheitsdaten** wie Schritte und verbrauchte Kalorien sammeln (sog. tracking). „Self-Tracking" Geräte bieten eine gute Orientierung für den eigenen Gesundheitszustand, ersetzen allerdings keinen Arzt bei gesundheitlichen Problemen.

| Chancen | Risiken | Empfehlung |
|---|---|---|
| • Anhand der gesammelten Daten erhalten Nutzer einen Überblick über die eigenen Gesundheitsdaten.<br>• Der direkte Vergleich der Daten mit anderen Nutzern kann Motivation zur Verbesserung der Werte sein. | • Gesundheitsdaten sind „besonders sensible personenbezogene Daten".<br>• Anbieter von Wearables und Fitness-Apps haben großes Interesse an der Auswertung und am Verkauf der Daten an Dritte (bspw. für Versicherungen oder Werbezwecke). | • Überprüfen, ob der Anbieter die Weitergabe der Daten ausschließt.<br>• Achten Sie bei den Sicherheitsangaben auf eine verschlüsselte Übertragung. |

Sicher Surfen im Internet

# Messenger-Dienste

Messaging ist eine Kommunikationsmethode, die häufig auch Instant Messaging (englisch für sofortige Nachrichtenübermittlung) genannt wird.

Nutzer von Messenger-Diensten können **Textnachrichten**, zum Teil auch Bilder, Ton- und Videoaufnahmen untereinander über das Internet verschicken.

Dafür werden Programme oder auch Apps für Smartphones genutzt.

Die Nutzung der Messenger-Dienste ist in den letzten Jahren enorm gestiegen. Der bekannteste Messenger-Dienst ist „WhatsApp“. In 2013 nutzten über 600 Millionen Menschen weltweit WhatsApp.

| Chancen | Risiken | Empfehlung |
|---|---|---|
| • Einfaches und schnelles Kontakthalten durch Versenden von Nachrichten, Bildern und Videos ohne zusätzliche Übertragungskosten wie dies bei SMS der Fall ist. | • Es bestehen datenschutzrechtliche Risiken, denn einige Dienste sammeln per se Daten, wie die Kontaktdaten aus dem Adressbuch.<br>• Hinsichtlich der IT-Sicherheit können Nachrichten bei der unverschlüsselten Versendung potenziell abgefangen bzw. mitgelesen werden und liefern Informationen über den Nutzer. | • Überprüfen Sie die Datenschutzeinstellungen auf Ihrem Smartphone und beschränken Sie den Zugriff des Dienstes auf die eigenen Telefonkontakte, Standort und Fotos.<br>• Blockieren Sie ungewollte Kontaktanfragen zum Schutz vor Viren und Belästigungen.<br>• Nutzen Sie Messenger-Dienste mit höheren Datenschutz- und IT-Sicherheitsanforderungen, z. B. Threema. |

# On-Demand- bzw. Streaming-Dienste

On-Demand-Dienste setzen sich in den letzten Jahren immer mehr durch. Hier kann über Webseiten oder auch Apps auf Audio- oder Videodateien (z. B. Musik, Hörbücher, Filme, Serien u.ä.) nach Bedarf zugegriffen werden.

In der Regel wird das Nutzungsrecht der Inhalte durch ein kostenpflichtiges Abonnement/Flatrate gewährleistet.

Streaming bedeutet, dass die Dateien über das Internet auf ein Endgerät übertragen werden, ohne dauerhaft auf der Festplatte gespeichert zu werden.

Musik-Streaming und Video-on-Demand ist quasi eine **Audio- und Videothek im Netz.**

| Chancen | Risiken | Empfehlung |
|---|---|---|
| • Aktuelle Inhalte wie Musik und Videos sind bei bestehender Internetverbindung immer und überall verfügbar.<br>• Geringe Abonnementkosten ermöglichen die Nutzung vieler medialer Inhalte unabhängig von Sendeterminen und Werbeunterbrechungen. | • Kinder und Jugendliche erhalten einfachen Zugriff auf Medieninhalte, die nicht altersgerecht sind.<br>• Der Streaminganbieter erhält personenbezogene Angaben über Ihr Mediennutzungsverhalten.<br>• Streaming über Handy verursacht ein hohes Datenvolumen und kann je nach Datentarif zu hohen Kosten führen. | • Nutzen Sie die kostenlosen Probeformate um sich einen Überblick zu verschaffen.<br>• Lesen Sie vor Vertragsabschluss die AGB und informieren Sie sich, wann und wie Sie das Abo wieder kündigen können<br>• Vermeiden Sie eine Verknüpfung der Streamingdienste mit eigenen Social-Media-Profilen wie Facebook. |

Sicher Surfen im Internet

# Online-Banking

Beim Online-Banking hat der Bankkunde über das Internet direkten Zugriff auf den Bankrechner und kann z. B. vom heimischen PC aus Bankgeschäfte erledigen. Die Aufträge werden mithilfe einer **elektronischen Authentifikation,** bspw. einer TAN-Nummer, „unterschrieben". Mit der Einführung der iTan oder der mobilen Tan ist das Risiko beim Online-Banking 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.

Wenn Ihnen eine falsche oder missbräuchliche Buchung auffällt, können Sie innerhalb einer Acht-Wochen-Frist der Abbuchung von ihrem Konto widersprechen. Bei nicht-autorisierten Zahlungen gilt ein Rückbuchungsanspruch, der innerhalb von 13 Monaten geltend zu machen ist.

Prüfen Sie daher regelmäßig ihre Kontoauszüge und kontaktieren Sie bei Unregelmäßigkeiten umgehend Ihre Bank.

Bei Abbuchung völlig fremder Firmen ist es wichtig, Ihre Bank schriftlich zu informieren und eine Frist zu setzen, die falsche Buchung wieder rückgängig zu machen.

Sie können bei der Bank zudem darauf bestehen, dass sie die Einzugsermächtigung für die Abbuchung vorlegen soll. Liegt keine Einzugsermächtigung vor, muss die Abbuchung rückgängig gemacht werden.

| Chancen | Risiken | Empfehlung |
| --- | --- | --- |
| • Zu jeder Zeit unabhängig von Öffnungszeiten des Bankinstitutes Bankgeschäfte abwickeln.<br>• Immer eine aktuelle Kontoübersicht. | • Mithilfe von Schadprogrammen können Daten während des Online-Bankings ausspioniert werden.<br>• Online-Banking bietet Nährboden für die meisten professionellen Phishing-Attacken. | • Prüfen Sie genau die Internetseiten von Banken, auf der die eigenen Bankdaten eingegeben werden können. Achten Sie darauf, dass die Internetadresse mit **„https“** beginnt und damit ein sicheres Hypertext-Übertragungsprotokoll ist.<br>• Nutzen Sie Online-Banking nur mit einem aktuellen Virenschutzprogramm und einer Firewall.<br>• Tipps für sicheres Online-Banking unter **www.bankenverband.de**<br>• **Prüfen Sie regelmäßig (mindestens einmal im Monat) Ihre Bankbuchungen.** |

Sicher Surfen im Internet

# Soziale Netzwerke

Soziale Netzwerke wie Facebook und Instagram bilden für ihre Mitglieder einen öffentlichen Raum und leben von der Interaktion ihrer Nutzer.

Diese können über die Webseite oder eine App jederzeit und von überall Inhalte hochladen oder diese abrufen.

Führender Anbieter bei den Social Networks ist „Facebook“ mit über einer Milliarde Nutzer weltweit. Der Zugang zu Facebook ist altersbeschränkt.

**Ab 13 Jahre** dürfen Kinder und Jugendliche einen Facebook-Account mit Einverständnis der Eltern einrichten.

Für Kinder und Jugendliche haben die sozialen Netzwerke einen besonderen Reiz, da sie mit ihren Freunden chatten können und schnell Zugang zu interessanten Bildern und Videos erhalten.

Allerdings ist bei ihnen besonderer Schutz geboten, da sie sich oft über die Konsequenzen im Umgang mit persönlichen Daten noch nicht bewusst sind und stärker der Gefahr ausgesetzt sind, Opfer von Cybermobbing zu werden.

| Chancen | Risiken | Empfehlung |
|---|---|---|
| • Einfaches Kontakthalten, Kennenlernen und Vernetzen weltweit zu jedem Zeitpunkt ohne Zusatzkosten.<br>• Präsentieren und mit „Freunden“ und „Fans“ oder „Followern“ (englisch für Anhänger) ohne viel Aufwand in Kontakt treten und bleiben.<br>• Automatisch über Neuigkeiten favorisierter Menschen, Firmen, Events usw. informiert werden.<br>• Alles Dargestellte teilen und kommentieren. | • Nicht nur „Freunde“ interessieren sich für die Inhalte. Zu Werbezwecken werden Daten aus unterschiedlichen Quellen verknüpft, Profile erstellt und ausgewertet.<br>• Auch Personalentscheider, Kollegen und Kunden werfen häufig einen Blick ins Profil des Bewerbers, kompromittierende Fotos oder Pinnwandeinträge sollten besser nicht zu finden sein.<br>• Eigene Profile und Kommentare können für Cybermobbingattacken genutzt werden.<br>• Authentizität der Profile wird nicht überprüft, deshalb gibt es zahlreiche frei erfundene Personen mit gefälschten Profilen, zum Teil mit kriminellem Hintergrund. | • Angaben in Geschäftsbedingungen und Datenschutzerklärung des Anbieters sorgfältig lesen und in regelmäßigen Abständen überprüfen.<br>• Nur ausgewählten Personen Zugriff auf eigenes Profil und darin enthaltene Informationen gestatten.<br>• **Private Angaben auf das Nötigste beschränken** und Verknüpfungen mit anderen Nutzerdaten und Accounts vermeiden.<br>• Einmal Veröffentlichtes ist nur sehr schwer wieder zu entfernen, **das Netz vergisst nicht!** – Erst denken, dann schreiben!<br>• Klären Sie Kinder und Jugendliche im Umgang mit Sozialen Netzwerken auf und sensibilisieren Sie über die Folgen.<br>• **www.schau-hin.info** bietet eine Übersicht von sozialen Netzwerken und eine Einschätzung, inwiefern diese für Kinder geeignet sind. |

Sicher Einkaufen im Internet

# Widerrufsrecht, Checkliste Versandshop

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 bei Bestellungen im Internet mit der nötigen Aufmerksamkeit vorgegangen werden.

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 vermitteln einen ersten Eindruck.

## Information:

Der Händler ist 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 durch ein Widerrufsrecht geschützt. Hierzu gibt es allerdings für den Verbraucher seit dem 13.6.2014 neue Rechte und Pflichten:

- ⇨ Der Verkäufer ist seitdem nicht mehr verpflichtet, die Rücksendekosten zu tragen. Es zeigt sich aber, dass viele Unternehmen weiterhin freiwillig die Rücksendekosten übernehmen.

- Die **Widerrufsfrist von 14 Tagen**, innerhalb derer der Käufer die Waren zurücksenden muss, bleibt erhalten. Sie beginnt mit Zusendung der Ware. Fehlt eine ordnungsgemäße Belehrung über das Widerrufsrecht, endet die (nach früherer Rechtslage unbegrenzte) Widerrufsfrist nunmehr nach zwölf Monaten und 14 Tagen nach Eingang der Ware beim Verbraucher.
- Downloads als Einkäufe können vom Widerrufsrecht ausgeschlossen werden, wenn der Verbraucher darauf hingewiesen und ausdrücklich eingewilligt hat (Häkchen gesetzt)
- Der Widerruf kann nun auch telefonisch erfolgen und muss nicht mehr zwingend als Textform beim Verkäufer vorliegen (allerdings ist die Textform aus Beweisgründen vorteilhaft). Der Widerruf muss vom Kunden ausdrücklich erklärt werden. Eine kommentarlose Rücksendung ist nicht mehr möglich. Hierfür muss vom Unternehmen ein Formular zum Widerruf zur Verfügung stehen.
- Außerdem muss mindestens eine gängige, kostenfreie Zahlungsmöglichkeit angeboten werden.

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.

Bei Bestellungen bei ausländischen Anbietern ist zu beachten, dass eine etwaige Verfolgung der eigenen Verbraucherrechte erschwert sein kann. Allerdings können Sie Ihre Rechte in der Regel auch vor einem deutschen Gericht einklagen, wenn ein im Ausland niedergelassener Unternehmer seine Leistungen auf dem deutschen Markt anbietet.

Zu berücksichtigen sind auch mögliche Zusatzkosten (höhere Versandgebühren, Steuern und Zölle, Bankgebühren). Diese zusätzlichen Kosten lassen vermeintliche Schnäppchen schnell teurer werden, als vergleichbare Angebote im Inland.

# Widerrufsrecht, Checkliste Versandshop

Anbieter müssen zudem durch die Bezeichnung auf „Bestell“-Buttons eindeutig erkennbar machen, dass bei einem Klick ein zahlungspflichtiger Bestellvorgang ausgelöst wird.

Auf folgende Bezeichnungen sollten Sie daher achten:

- ⇨ Zahlungspflichtig bestellen
- ⇨ Kostenpflichtig bestellen
- ⇨ Kaufen
- ⇨ Zahlungspflichtigen Vertrag abschließen

Die Bezeichnungen „Bestellung“ oder „weiter“ sind demnach keine zulässigen Formulierungen mehr.


Die Änderungen sollen insbesondere vor Abo-Fallen im Internet schützen. Zudem müssen die Onlineshops vor der Bestellung zusätzliche Informationen klar und verständlich in hervorgehobener Weise zur Verfügung stellen.

Zusätzliche Informationen sind:

- ⇨ Die wesentlichen Eigenschaften der Ware oder Dienstleistung,
- ⇨ der Gesamtpreis inklusive aller Steuern und Abgaben, zusätzlich anfallender Fracht-, Liefer- oder Zustellkosten sowie aller sonstiger Kosten,
- ⇨ bei Dauerschuldverhältnissen deren Laufzeit und die Kündigungsmodalitäten,
- ⇨ gegebenenfalls die Mindestdauer der Verpflichtungen, die der Verbraucher mit dem Vertrag eingeht.

## 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
- ⇨ Klare und verständliche Datenschutzbestimmungen

Bei Rechtsstreitigkeiten mit dem Unternehmen die Online-Schlichtung nutzen:

**www.online-schlichter.de**

## Online-Schlichtung:

Wenn es mal zu Unstimmigkeiten im Online-Einkauf kommt, gibt es für Verbraucher die Möglichkeit der Schlichtung. Hierbei bleibt der langwierige und kostenintensive Weg vor Gericht erspart.

Eine Schlichtung ist eine **außergerichtliche Beilegung** eines Rechtsstreites.

Der Schlichter ist eine neutrale Person und versucht zwischen Verbraucher und Unternehmer eine Lösung unter Berücksichtigung der bestehenden Rechtslage zu vermitteln.

Das erspart Kosten, Zeit und Nerven. Derzeit können Verbraucher aus Bayern unter der Internetadresse **www.online-schlichter.de** einen Fall zur Schlichtung online einreichen.

Voraussetzung dafür ist:

- ⇨ Rechtsstreit zwischen einem Verbraucher und einem Unternehmer.
- ⇨ Es wurde ein Vertrag (Kauf, Verkauf oder Dienstleistung) im Internet geschlossen.
- ⇨ Beiden Parteien gelingt es nicht, sich selbst zu einigen und waren noch nicht vor Gericht.

**Sicher Einkaufen im Internet**

# 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, welches 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 einem konsequenten Verbraucherschutz im Netz verpflichtet (mehr unter: **www.internet-guetesiegel.de**).

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.

Sollte doch einmal etwas schiefgehen, bieten Siegelanbieter wie Trusted Shops Streitschlichtung zwischen dem Kunden und dem Internetshop oder gar die Erstattung etwaiger Auslagen an.

Trusted Shops

S@fer Shopping

EHI Geprüfter Online-Shop

internet privacy standards

Sicher Einkaufen im Internet

# Mobile Shopping

41 Millionen Deutsche haben bereits einmal im Internet eingekauft. Immer mehr Anbieter bieten dem Nutzer die Möglichkeit, über das Smartphone oder das Tablet mobil Waren und Dienstleistungen zu kaufen.

Der Verbraucher hat beim Mobile-Shopping nicht weniger Rechte als beim normalen Online Shopping. Dennoch birgt Mobile-Shopping das ungleich höhere Risiko, dass Dritte bei Verlust des mobilen Endgerätes auf Zahlungsdaten und dergleichen zugreifen können.

Insofern ist es notwendig, gerade wenn es um Zahlungs-, Bank- oder Kreditkartendaten geht, **besondere Sicherheitsmaßnahmen** vorzunehmen.

## Tipps:

- ⇨ Speichern Sie Bank- oder Kreditkartendaten im Handy/Smartphone nie unverschlüsselt und ohne Passwortschutz ab.
- ⇨ Informieren Sie sich genau, welche Sicherheitseinstellung Bezahl-Apps wie PayPal oder Apple Pay haben.

# Informationen und Hilfe im Netz

- Kampagne „Online Kaufen – mit Verstand!“: Eine Initiative von Versandhändlern und eBay für mehr Sicherheit im Onlinehandel mit Tipps für den Streitfall.

  **www.kaufenmitverstand.de**

- Verbraucherportal VIS Bayern: Das Portal des bayerischen Verbraucherministeriums mit Hinweisen, was man im Fall der Fälle tun muss.

  **www.vis.bayern.de**

- Portale der Verbraucherverbände: Die bayerischen Verbraucherverbände – Verbraucherzentrale und Verbraucherservice – leisten schnelle und direkte Unterstützung, wenn man auf ein „schwarzes Schaf“ des Online-Handels gestoßen ist:

  **www.verbraucherzentrale-bayern.de**
  **www.verbraucherservice-bayern.de**

Online Kaufen – mit Verstand!

VIS Verbraucher-Informations-System Bayern

verbraucherzentrale Bayern

Verbraucher Service Bayern

# Sichere Bezahlverfahren

Auch Bezahlmethoden sollte man mit Bedacht wählen: Vorauskasse ist immer mit dem Risiko behaftet, bei einer Insolvenz des Händlers plötzlich ohne Ware dazustehen. Zahlung per Nachnahme ist zwar ein sicheres Verfahren, kann jedoch mit zusätzlichen Kosten verbunden sein. Wählen Sie im Zweifel besser die Zahlung per Rechnung oder per Kreditkarte.

Um auf Nummer sicher zu gehen, bieten sich auch Bezahlverfahren wie PayPal oder giropay an. Hier ist das Geld geschützt, denn im Zweifelsfall wird es – wie bei einigen Kreditkartenunternehmen – sogar zurückerstattet.

Eine weitere Alternative ist die so genannte 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.

Sicher Einkaufen im Internet

# Online-Bewertungsportale

Es ist zu unterscheiden, ob es Bewertungsmöglichkeiten auf Internetseiten gibt oder es sich um Internetseiten handelt, die sich auf das Aufnehmen von Kundenrezensionen spezialisiert haben.

Letzteres wird allgemein als Bewertungsportal bezeichnet. Die Grenzen zwischen Bewertungs- und Vergleichsportalen sind fließend. Vergleichsportale wie check24.de führen eine Vielzahl von Produkten und Dienstleistungen auf.

Bewertungsportale unterstützen den Verbraucher in der Vielzahl der Angebote passende Produkte und Dienstleistungen zu finden. Sie verschaffen dem Markt zusätzliche Transparenz und ermöglichen Verbrauchern, Unternehmen als auch deren Produkte und Dienstleistungen durch Meinung Dritter zu beurteilen. Ferner wirken sich Online-Bewertungen positiv auf die Anbieter von Produkten und Dienstleistungen aus. Da diese Bewertungen öffentlich zugänglich sind, werden Unternehmen dazu angehalten ihre Leistungen kunden- bzw. verbraucherfreundlich zu gestalten. Die geschaffene **Markttransparenz** sowie die Gefahr schlechter Kundenmeinungen wirken sich positiv auf die Angebote und den Verbraucher aus. Bei der Berücksichtigung von Kundenmeinungen bei der Kaufentscheidung ist jedoch auch Vorsicht geboten.

Der Verbrauchzentrale Bundesverband (vzbv) schätzt, dass rund 20 % der Online-Bewertungen gefälscht oder vom Unternehmer erkauft werden. Verbraucher sollten daher ihre Kaufentscheidung nicht ausschließlich von einer anderen Kundenmeinung abhängig machen.

# Tipps

- ⇨ Vergleichen Sie Waren und Dienstleistungen auf unterschiedlichen Internetseiten. Wortgleiche Kommentare von Nutzern auf mehreren Internetseiten zu gleichen Produkten **deuten auf eine „unechte" Bewertung hin**.
- ⇨ Seien Sie bei zu viel und zu großem Lobgesang auf bestimmte Produkte kritisch. Umfangreiche, detaillierte und auch kritische Nutzermeinungen geben eher die Wahrheit wieder.
- ⇨ Anbieter von Vergleichsportalen bieten in ihren Bedingungen Maßnahmen oder Anlaufstellen zur Kontaktaufnahme an, wenn Zweifel an Kundenmeinungen bestehen.

Fragen und Antworten

# Gibt es Alternativen zu Google?

Google hat mit seinem Angebot das Internet verändert. Es ist mit seiner Suchmaschine für viele Nutzer eine tägliche Hilfe.

Google ist aber mit seiner Datenschutzpolitik und seinen Datenschutzbestimmungen zunehmend in die Kritik geraten.

Suchanfragen werden gespeichert, Werbung wird anhand der eigenen Suchanfragen platziert – kurzum, mit seinen täglichen Suchanfragen erhält Google ein umfassendes Bild über unsere Vorlieben und Interessen sowie weitere Profilinformationen.

Trotzdem nutzen mehr als 90 % der Bürger Google. Es gibt allerdings viele Alternativen:

- **www.duckduckgo.com -** Suchmaschine die keine persönlichen Daten sammelt
- **www.ixquick.com -** Suchmaschine aus den Niederlanden die ebenfalls auf Datensammeln verzichtet
- **www.fragfinn.de -** Suchmaschine speziell für Kinder und Jugendliche

DuckDuckGo

fragFINN.de

ixquick

**Fragen und Antworten**

# Darf ich kostenlose Dateien aus dem Internet downloaden?

Mithilfe des Internets 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".

Die Denkweise: „Das lade ich mir mal schnell runter" ist überaus verbreitet.

Ob nun bewusst oder aus Unwissenheit, 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.

Bei einigen hundert Dateien summiert sich der Schadensersatz schnell auf hohe vierstellige Beträge und meist ist die Rechtsprechung eindeutig:
Der Schädiger muss zahlen.

Und nicht nur der eigene widerrechtliche Download kann folgenreich sein. Als Betreiber eines WLAN-Netzes muss man dafür sorgen, dass niemand über den eigenen Anschluss widerrechtlich Dateien herunterladen kann. Eine Absicherung des Zugangs mit Kennwörtern und durch Verschlüsselung (z. B. WPA2) ist daher nötig.

Eltern können nach der jüngsten Rechtsprechung immer noch für illegale Downloads ihrer Kinder über das hauseigene WLAN haften, wenn sie nicht nachweisen, dass sie die Kinder über die Illegalität belehrt und ihnen eine Teilnahme an Tauchbörsen untersagt haben.

Das Herunterladen oder Bereitstellen von illegalen Dateien bleibt in jedem Fall eine Straftat, worüber Kinder und Jugendliche aufgeklärt sein sollten.

Fragen und Antworten

# 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 Sach- und Rechtslage so eindeutig, dass nichts weiter übrig bleibt, als zu zahlen. Die beigefügten Unterlassungserklärun-gen gehen jedoch oft zu weit: Im Zweifel fachkundigen Rat einholen, oder – noch besser – lieber gleich die Hände weg von vermeintlich kostenfreier Musik im Netz.

Grundsätzlich ist es zu empfehlen, dass bei Erhalt einer Abmahnung umgehend ein **Rechtsbeistand** aufgesucht wird. Achten Sie dabei auf die Fristen. Nicht jede Abmahnung ist zudem berechtigt. Auch hier gibt es leider schwarze Schafe, die die Angst der Verbraucher ausnutzen und sich an den Abmahnkosten bereichern. Der Verbraucher zahlt leider oft viel zu schnell ohne den Anspruch fundiert durch einen Rechtsbeistand prüfen zu lassen.

Wichtig zu wissen: Der Gesetzgeber hat die Abmahnkosten gedeckelt. Neben dem Schadensersatz hat der Abgemahnte auch die Anwaltsgebühren zu begleichen. Diese dürfen allerdings im Regelfall rund 155 EUR nicht überschreiten, da der Gegenstandswert gesetzlich auf 1.000 EUR begrenzt ist.

Fragen und Antworten

# Wie erkenne ich Spammails, wie gehe ich mit Spam um?

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

Der Begriff stammt aus dem Englischen, war ein Markenname für Dosenfleisch 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.

## Wichtige Schutzmaßnahmen:

- ⇨ Einsatz von Spam-Filtern und Nutzung von „Absender sperren"-Listen
- ⇨ Verwendung von „Wegwerf-Adressen"
- ⇨ Sparsamkeit bei der Bekanntgabe der eigenen Mailadresse
- ⇨ Keine Spam-Mails öffnen, niemals darauf antworten und jede Spam-E-Mail löschen
- ⇨ Eintrag in die Robinson-Liste **www.robinsonliste.de**

Fragen und Antworten

# Internet – ergibt das in meinem Alter überhaupt noch Sinn?

Computer und Internet sind unserer heutigen Gesellschaft kaum mehr wegzudenken. Auch die ältere Generation findet zunehmend Gefallen am Internet. Die so genannten „Silver Surfer“ freuen sich über die Möglichkeiten, aktiv an allen Bereichen des Lebens teilzuhaben.

Mit E-Mails oder Videotelefonie kann der Kontakt zu entfernten Familienmitgliedern problemlos gepflegt werden, mit Online Banking oder Online Shopping erspart man sich mühsame Wege. Natürlich dient das Internet auch für ältere Menschen als Informationsquelle für Nachrichten und andere Angebote. Viele ältere Menschen haben jedoch noch Berührungsängste mit der Technik und dem Internet. Freunde, Familie und Bekannte können Schritt für Schritt dabei helfen, älteren Menschen den Umgang mit dem Internet zu zeigen. Oft empfiehlt es sich, lokale Angebote zu Computer- und Internetkursen zu besuchen, die von Volkshochschulen oder Seniorentreffs organisiert werden.

Spezielle Internetseiten wie **www.50plus-treff.de**, das Netzwerk für Senioren **www.feierabend.de** oder das Soziale Netzwerk speziell für Senioren **www.seniorbook.de** helfen bei Fragen rund um das Internet und ermöglichen neue interessante Kontakte.

Informieren Sie sich auch in unserer Broschüre „Gut zu wissen! – Ran ans Internet!“ kostenlos zum downloaden unter **www.vis.bayern.de** und **www.bestellen.bayern.de**.


Gut zu wissen!
N ANS INTERNET!
Ein Ratgeber für Einsteiger

# Links

1. Verbraucherportal VIS Bayern mit aktuellen Informationen der Bayerischen Staatsregierung zu allen Verbraucherthemen wie Rechte beim Einkaufen, Ernährung, technische Produkte, Finanzen und Versicherungen sowie Energie. Die Sicherheit im Netz bildet im Bereich „Internet und digitale Welt“ einen Schwerpunkt.
   **www.vis.bayern.de**
2. Verbraucherservice der Bundesnetzagentur, Anlaufstelle für Endkunden, die Schwierigkeiten mit ihren Telekommunikationsanbietern haben (auch Spam und Rufnummernmissbrauch) 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**
3. Das Bundesamt für Sicherheit in der Informationstechnik informiert über Risiken, Gefahren und Befürchtungen beim Einsatz der Informationstechnik und versucht Lösungen dafür zu finden.
   **www.bsi-fuer-buerger.de**
4. 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 sicheren Umgangs mit dem Internet zu informieren und Beschwerden einzureichen.
   **www.internet-beschwerdestelle.de**
5. 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.
   **www.sicher-im-netz.de**
6. 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**
7. „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**
8. 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**
9. Informationsseite des Bundesverbandes Digitale Wirtschaft rund um das Thema Cookies.
   **www.meine-cookies.org**
10. 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**
11. 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**

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

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

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

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

16. Das Portal Verbraucherbildung Bayern bündelt Angebote zum kompetenten Umgang mit dem Internet. Die Palette reicht von Schulmaterialien über Terminhinweise zu Kursen und Vorträgen für Verbraucher, bis zu Fortbildungen und der Vermittlung von Referenten. **www.verbraucherbildung.bayern.de**

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

18. 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**

19. 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**

20. 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**

21. 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**

22. 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**

23. 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**


www.vis.bayern.de

| | |
|---|---|
| Herausgeber: | Bayerisches Staatsministerium für Umwelt und Verbraucherschutz,<br>Rosenkavalierplatz 2, 81925 München und<br>Initiative D21 e.V., Reinhardtstr. 38, 10117 Berlin<br>**kontakt@initiatived21.de** |
| Konzept/Text: | Björn Stecher (Initiative D21) V.i.s.d.P. |
| Gestaltung: | New Now, Kai Nicolaides & Stephan Junghanns GbR<br>Danziger Straße 167, 10407 Berlin |
| Druck: | Schmekies Medien & Druckerei, Wilde Acht 30, 54329 Konz-Könen |
| Bildnachweis: | Seite 1: © Goodluz / Shutterstock.com<br>Weitere Bilder von Fotolia.com und Shutterstock.com – Bildnachweis erfolgt im Heft. |
| Stand: | November 2015 |




**BAYERNIDIREKT** ist Ihr direkter Draht zur Bayerischen Staatsregierung. Unter Tel. 089 122220 oder per E-Mail unter direkt@bayern.de erhalten Sie Informationsmaterial und Broschüren, Auskunft zu aktuellen Themen und Internetquellen sowie Hinweise zu Behörden, zuständigen Stellen und Ansprechpartnern bei der Bayerischen Staatsregierung.

Bayern.
Die Zukunft.