BLM
Bayerische
Landeszentrale für
neue Medien

Jugendschutz
Nutzerkompetenz
Medienpädagogik

Selbstdatenschutz!

Tipps, Tricks und Klicks

Vorwort

Viele Menschen gehen gerade im Internet zu großzügig mit ihren Daten um. Teilweise passiert das bewusst – etwa in Sozialen Netzwerken, wo oft selbst Unbekannten viel Persönliches mitgeteilt wird. Teilweise geschieht es aber auch unbewusst – wenn beispielsweise beim Onlineshopping Datenschutzrichtlinien ungelesen zugestimmt wird.

Wir müssen uns darüber bewusst sein, dass unsere persönlichen Daten heute als das „Gold unserer Zeit" gehandelt werden. Internetgiganten werden zu Goldgräbern und versuchen, mit scheinbar kostenlosen Angeboten in Sozialen Netzwerken oder Apps so viel wie möglich von diesem Goldschatz zu heben. Denn unsere Daten sind die Finanzierungsquellen für ihre Unternehmenskonzepte.

Jeder Einzelne ist daher gefragt, selbst aktiv zu werden, um seine Privatsphäre entsprechend zu schützen! Nachdem klassischer Datenschutz in der globalen Welt mit schnellen Vervielfältigungs- und Weiterverbreitungsmöglichkeiten im Netz immer schwieriger durchzusetzen ist, gewinnt das Thema Selbstdatenschutz in der Öffentlichkeit immer mehr an Bedeutung.

Beim Selbstdatenschutz stehen aus dem Grund die Nutzerinnen und Nutzer im Mittelpunkt – so wie in dieser Broschüre: Wir möchten damit einen Beitrag dazu leisten, das Bewusstsein für einen verantwortungsvollen Medienumgang zu stärken, mithilfe verständlich aufbereiteter Hintergrundinformationen und alltagstauglicher Tipps.

Gerade Pädagogen und Eltern fragen bei der Landeszentrale immer wieder nach Informationen zum Schutz der Daten – ihrer eigenen, aber auch der ihrer Kinder und Schutzbefohlenen. Deshalb legen wir auf dieses Themenfeld besonderes Augenmerk: Bei jedem unserer vier Schwerpunktthemen, „Technik und Geräte",

„Kommunikation mit mobilen Geräten", „Surfen, Web 2.0 und Cloud-Dienste" sowie „Einkaufen und Bezahlen" findet sich ein Abschnitt zu den besonderen Handlungsoptionen in Elternhaus und Schule.

Hinweisen möchten wir Sie in diesem Zusammenhang auch auf unseren über www.blm.de abrufbaren Online-Ratgeber für Mediennutzer „total digital", in dem relevante Begriffe zu Radio, Fernsehen, Internet und Mobilfunk verständlich, kurz und nutzernah erklärt werden.

Im Sinne eines kompetenten und selbstbestimmten Umgangs mit den eigenen Daten wünsche ich Ihnen eine informative Lektüre. Viel Erfolg bei der Umsetzung der vielen praktischen Anregungen!

Siegfried Schneider
Präsident der Bayerischen Landeszentrale
für neue Medien

Einleitung

„Ich habe doch nichts zu verbergen?“

Selbstdatenschutz – was ist das?

Kaum ein Mensch erlaubt einem Unbekannten ohne Grund Einblick in seine privaten Verhältnisse. Persönliche Notizen, Urlaubsfotos, Bankdaten – nichts davon wird Fremden oder Neugierigen einfach gezeigt.

Ganz anders erscheint das bei vielen Menschen, wenn sie im Internet unterwegs sind: Nach dem Motto **„Ich habe doch nichts zu verbergen“** werden Daten und damit große Teile der Privatsphäre freiwillig öffentlich gemacht. Überwachung und das Ausspähen von Informationen bewertet man oft nur als Kavaliersdelikt. Aber ist dieses Vorgehen wirklich harmlos? Sicherlich nicht – jedoch sind die Konsequenzen weniger offensichtlich als bei einer direkten Begegnung mit neugierigen Mitmenschen.

Der Staat und seine Institutionen sind zwar zum bestmöglichen Schutz der Bürgerinnen und Bürger verpflichtet. Ein Skandal wie die NSA-Abhöraffäre sowie die fragwürdigen Datensammlungen großer Konzerne zeigen jedoch: Es besteht auf vielen gesellschaftlichen Ebenen Handlungsbedarf.

Begriffe wie „Selbstdatenschutz“ und „Digitale Selbstverteidigung“ bedeuten: **Wir alle können und müssen selbst etwas für den Schutz unserer Daten tun.** Selbst wenn die digitale Welt nicht ganz ohne die Preisgabe persönlicher Daten funktioniert, so sind wir als Mediennutzer nicht völlig wehrlos.

Diese Broschüre möchte Sie in einigen wichtigen Punkten für den Selbstdatenschutz sensibilisieren. Sie erhalten Tipps, wie Sie bei der Nutzung digitaler Medien – zumindest teilweise – die Kontrolle über Ihre Daten behalten können.

Mit „* “ gekennzeichnete Begriffe werden am Ende der Broschüre in einem Glossar erläutert.

Gründe für den Selbstdatenschutz

Der Bürger als „gläserner Mensch"?
Mit der Verbreitung des Internets hat der Zugriff auf persönliche Daten eine völlig neue Größenordnung erreicht. Doch schon vorher gab es Auseinandersetzungen um den Schutz der Privatsphäre: Das „Recht auf informationelle Selbstbestimmung" wurde 1983 vom Bundesverfassungsgericht im Zusammenhang mit der Volkszählung festgeschrieben.

Volkszählungsurteil

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß."

„Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus."
(BVerfGE 65, 1 – Volkszählung)

Das Recht auf informationelle Selbstbestimmung ist aus dem allgemeinen Persönlichkeitsrecht abgeleitet (Art. 1 und 2 Grundgesetz) und kann nur durch Gesetze eingeschränkt werden. Dies betrifft beispielsweise die „Vorratsdatenspeicherung", also die Speicherung personenbezogener Verbindungsdaten, damit Ermittlungsbehörden Straftaten besser verfolgen können.

Das Recht auf informationelle Selbstbestimmung zu gewährleisten, ist somit auch eine Aufgabe des Staates. Daher gibt es das Bundesdatenschutzgesetz sowie die einzelnen Landesdatenschutzgesetze. Doch der Begriff der „Selbstbestimmung" verweist in einer freiheitlich-demokratischen Grundordnung ebenso auf die notwendige Eigeninitiative der Bürgerinnen und Bürger.

Eigeninitiative zeigen!

Datensparsamkeit
Was kann man tun, um nicht zum „gläsernen Menschen" zu werden? Sicherlich möchte niemand, dass von ihm unwissentlich Daten gesammelt und verfügbar gemacht werden: von jedem Bezahlvorgang mit Kunden-, Kredit- oder EC-Karte, von jedem Schritt durch GPS-Daten und von jedem Gedanken durch Mitteilungen in Sozialen Netzwerken.

„Konto gehackt?“

Sie haben nicht viel eingekauft und trotzdem leert sich Ihr Bankkonto? Konto- und Kreditkarten-Daten können durch Leichtsinn oder gezielte Hacker-Angriffe in falsche Hände geraten. Dann werden z.B. Zahlungen umgeleitet oder Bestellungen auf anderer Leute Kosten getätigt. Schauen Sie also genau hin, bevor Sie Ihre Konto- und Kreditkarten-Daten im Internet verwenden und überprüfen Sie Ihre Kontoauszüge.

Nur so viele Daten wie nötig und so wenige Daten wie möglich von sich preisgeben

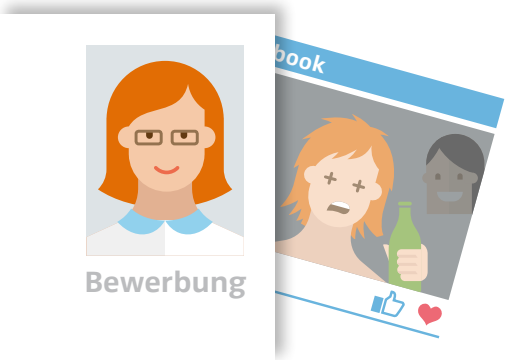
Sobald Daten – insbesondere in Verbindung mit dem Internet – gesammelt werden, gibt es keinen absoluten Schutz vor Zugriffen mehr. Das richtige Verhalten lässt sich daher auf eine einfache Grundformel bringen: **Geben Sie nur so viele Daten wie nötig und so wenige Daten wie möglich von sich preis.**

Beispiele für persönliche bzw. personenbezogene Daten

- Name, Alter, Familienstand, Geburtsdatum
- Anschrift, Telefonnummer, E-Mail-Adresse
- Konto-, Kreditkartennummer
- Kraftfahrzeugnummer, Kfz-Kennzeichen
- Personalausweisnummer
- Sozialversicherungsnummer
- Vorstrafen
- genetische Daten und Krankendaten
- Werturteile (z.B. Zeugnisse)
- Kundendaten
- Personaldaten

Quelle: Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Oftmals geben wir unsere Daten bei einer Anmeldung freiwillig preis – daher sollten wir uns auch selbst verstärkt um den Verbleib und um den Schutz unserer Daten kümmern. Beispielsweise ist es gar nicht immer erforderlich, bestimmte Angaben zur eigenen Person zu machen, wenn man dazu aufgefordert wird. Unterscheiden Sie zwischen Pflichtangaben und freiwilligen Angaben.



„Zugespamt?“

Ihr Briefkasten enthält plötzlich viel mehr Werbesendungen und auch Ihr E-Mail-Konto wird „zugespamt“? Möglicherweise haben Sie ein Kundenkonto bei einem unseriösen Online-Händler eröffnet und Ihre Daten wurden weiterverkauft.

„Schlechten Eindruck hinterlassen?“

Sie bewerben sich für eine Stelle oder einen Ausbildungsplatz – welchen Eindruck möchten Sie hinterlassen? Denken Sie daran: Immer mehr Arbeitgeber recherchieren Informationen über neue Mitarbeiter auch im Internet.

Nicht alle Inhalte, die man im Internet teilen möchte, müssen für jedermann sichtbar sein. Dies betrifft oft auch Dritte. Wenn man beispielsweise Fotos, auf denen andere Personen abgebildet sind, online stellt, muss man diese um Erlaubnis fragen. Daher sollte man in den Privatsphäre-Einstellungen, statt alles „öffentlich“ zu machen, für bestimmte Inhalte besser „privat“ wählen.

Man sollte selbst entscheiden, welche Informationen etwa der zukünftige Arbeitgeber nicht nur aus Bewerbungsunterlagen, sondern auch über Soziale Netzwerke bezieht.

Privatsphäre-Einstellungen prüfen

„Meine Daten gehören mir!“

Fragen Sie sich, ob Sie für bestimmte Bonus-Angebote von Supermärkten und Online-Shops mit den eigenen Daten bezahlen wollen, die für gezielte Werbesendungen eingesetzt werden?

Es ist nicht abzusehen, was die umfassenden Datensammlungen und Auswertungen mittels Algorithmen von heute für zukünftige Konsequenzen haben. Sie können Vor- und Nachteile mit sich bringen (Big Data*). Die Vergangenheit hat allerdings gezeigt: Die wahren Beweggründe für bestimmte Entwicklungen werden der breiten Öffentlichkeit oftmals verschwiegen. Wichtig ist daher: Die eigenen persönlichen Daten und Fotos sowie die Daten anderer Menschen (z.B. von Partnern, Kindern oder Freunden) sind als persönliches „Kapital“ zu verstehen, mit dem man nicht verschwenderisch, sondern sparsam umgeht. **„Meine Daten gehören mir!“** – Das ist ein Slogan, der immer wichtiger wird.

„Zu viel bezahlt?“

Sie erfahren, dass Ihre Bekannte über das Internet die gleiche Reise beim selben Anbieter gebucht, aber wesentlich weniger bezahlt hat. „Preisdiskriminierung“ ist im Internet an der Tagesordnung. Dabei geht es beispielsweise um Preiszuschläge für Nutzer teurer Geräte oder für Bewohner teurer Wohnviertel.

Teil 1: Technik und Geräte

Teil 1: Technik und Geräte

Die digitalen Geräte, die wir verwenden, werden immer zahlreicher, kleiner und vielfältiger.
Mit Spielkonsole, Tablet und Smartphone nutzen wir heute digitale Mediengeräte mobil – überall und jederzeit. Das bedeutet: Es werden immer mehr Datenspuren erzeugt und hinterlassen. Wer dies einschränken will, muss sich regelmäßig über **aktuelle Schutzmaßnahmen** informieren.

Datenschutzeinstellungen prüfen

TIPP

Sparen Sie keine Zeit an der falschen Stelle. Überprüfen Sie bei neuer Technik und neuen Geräten immer die **Datenschutzeinstellungen**. Die von den Anbietern festgelegten **Voreinstellungen** entsprechen in aller Regel nicht dem eigenen Sicherheitsbedürfnis, sondern ermöglichen häufig umfangreiche Datenerhebungen.

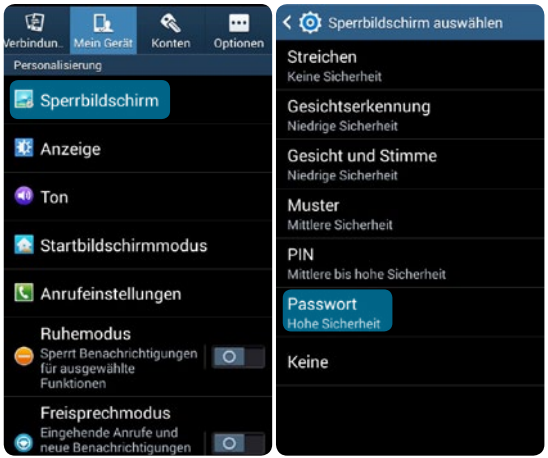
Datendiebstahl geschieht nicht nur online. Verhindern oder erschweren Sie das Aufrufen von Daten bei einem Gerätediebstahl oder bei Abwesenheit (etwa am Arbeitsplatz). Sie können nahezu alle digitalen Geräte mit einer Zugangssperre versehen.

TIPP

Richten Sie Zugangssperren ein, z.B.:

- **Boot-Sperre**
  Aktiv vor dem Hochfahren des Geräts,
  Sicherung durch PIN, Passwort oder Fingerabdruck-Scanner
- **Display-Sperre bzw. Sperrbildschirm**
  Aktiv nach dem Hochfahren und nach Inaktivität des Geräts,
  Sicherung durch PIN, Passwort oder Fingerabdruck-Scanner oder Tastatur-Muster
- **PIN-Schutz der SIM-Karte***
  Aktiv bei Entwendung der SIM-Karte aus dem Gerät,
  Sicherung durch PIN

Der Weg zur Einrichtung eines Sperrbildschirms ist je nach Gerät unterschiedlich: Zunächst „Einstellungen“ wählen und dann z.B. „Mein Gerät“ (alternativ: „Optionen“ oder „Sicherheit“) anwählen. Unter einem dieser Punkte liegt in der Regel der Menüpunkt „Sperrbildschirm“ (siehe auch *www.tutonaut.de/anleitung-android-smartphones-und-tablets-per-display-sperre-vor-fremden-zugriff-schuetzen.html*).



Display-Sperre bzw. Sperrbildschirm

Sicherheitsstufen bei Zugangssperren:

- **Geringe bis mittlere Sicherheit**
  Unterschrift auf dem Display des Handys, Muster auf dem Bildschirm streichen
- **Mittlere Sicherheit**
  Geheimzahl, PIN (Persönliche Identifikationsnummer), oft nur vierstellige Zahlenkombination
- **Höhere Sicherheit**
  Passwort/Kennwort: Buchstaben-, Zahlen- und Zeichenkombination, höhere Sicherheit bei Beachtung der Regeln für ein sicheres Passwort

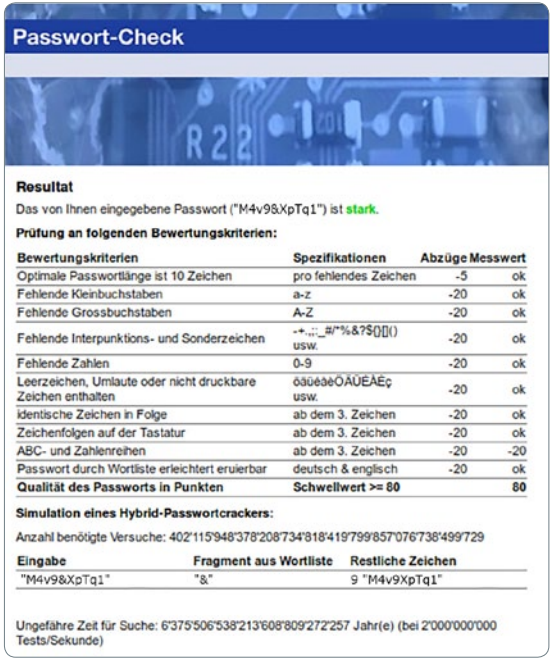
TIPP

Bei Verwendung von **Passwörtern** berücksichtigen:

- Mindestens 10 Zeichen
- Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen
- Keine Eigennamen, Geburtsdaten, Tastaturabfolgen, ABC- und Zahlenreihen verwenden
- Nicht in unbekannten Umgebungen einloggen (z.B. offene Netzwerke, Internet-Cafés)
- Passwort regelmäßig wechseln
- Passwörter nicht auf den Geräten oder im Browser speichern und nicht an andere weitergeben
- Überprüfen Sie ein Testpasswort online

Sicheres Passwort wählen

Nicht verwendete Dienste wie GPS, WLAN oder Bluetooth deaktivieren



Passwort-Check

Resultat

Das von Ihnen eingegebene Passwort ("M4v98&XpTq1") ist **stark.**

Prüfung an folgenden Bewertungskriterien:

Bewertungskriterien	Spezifikationen	Abzüge	Messwert
Optimale Passwortlänge ist 10 Zeichen	pro fehlendes Zeichen	-5	ok
Fehlende Kleinbuchstaben	a-z	-20	ok
Fehlende Grossbuchstaben	A-Z	-20	ok
Fehlende Interpunktions- und Sonderzeichen	-+.,:;_#/*%&?$()[]{} usw.	-20	ok
Fehlende Zahlen	0-9	-20	ok
Leerzeichen, Umlaute oder nicht druckbare Zeichen enthalten	öäüéàèÖÄÜÉÀÈç usw.	-20	ok
identische Zeichen in Folge	ab dem 3. Zeichen	-20	ok
Zeichenfolgen auf der Tastatur	ab dem 3. Zeichen	-20	ok
ABC- und Zahlenreihen	ab dem 3. Zeichen	-20	-20
Passwort durch Wortliste erleichtert eruierbar	deutsch & englisch	-20	ok
Qualität des Passworts in Punkten	**Schwellwert >= 80**		**80**

Simulation eines Hybrid-Passwortcrackers:

Anzahl benötigte Versuche: 402'115'948'378'208'734'818'419'799'857'076'738'499'729

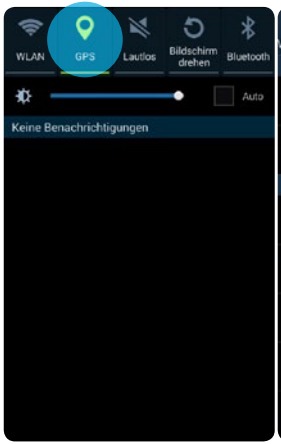
Eingabe	Fragment aus Wortliste	Restliche Zeichen
"M4v98&XpTq1"	"&"	9 "M4v9XpTq1"

Ungefähre Zeit für Suche: 6'375'506'538'213'608'809'272'257 Jahr(e) (bei 2'000'000'000 Tests/Sekunde)

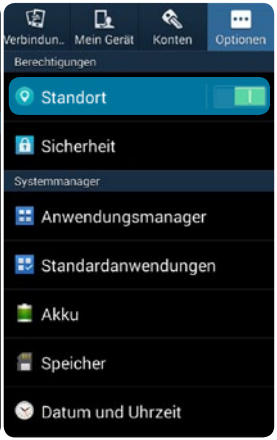
Beispiel für ein sicheres Passwort: M4v9&XpTq1. Weitere Informationen und Video unter: *www.handysektor.de/hacker-sicherheit/sichere-passwoerter.html.*

Funknetze und drahtlose Zugänge wie WLAN*, Bluetooth*und NFC* sind praktisch. Sie ermöglichen aber auch Eindringlingen den Zugriff auf Ihre Geräte bzw. Daten. Daher sollte man diese Funktionen nur für den Zugang zu verschlüsselten, sicheren Netzwerken (= passwortgeschützt, WPA2-Standard*) und für den Austausch mit bekannten Geräten aktivieren. Bei offenen Netzwerken (Hotspots) ist Vorsicht geboten – hier können die Daten leicht von Dritten mitgelesen werden.

Ein wichtiges Selbstdatenschutz-Thema ist die **Standort-Abfrage**. Ein grobes Bewegungsprofil kann immer über die Einwahl des mobilen Gerätes in die jeweiligen Funkzellen des Mobilfunknetzwerkes erstellt werden. Auch eingeschaltetes WLAN und Bluetooth ermöglichen eine Positionsbestimmung – es sei denn, das Telefon ist ausgeschaltet oder im Flugmodus. Wesentlich genauere Standortdaten liefern die Daten des Satellitennavigationssystems (GPS).



Vom oberen Displayrand nach unten wischen: Durch Antippen **WLAN**, **GPS** und **Bluetooth** aktivieren oder deaktivieren.



Unter **Einstellungen** → **Optionen** können Sie die Standort-Abfrage über einen Schalter ein- und ausschalten.

TIPP

- **GPS-Funktion**
  Überlegen Sie sich, ob Sie die GPS-Funktion immer aktiviert lassen. Bedenken Sie: Viele **Apps*** – und damit Konzerne – sammeln Ihre Standortdaten, wenn Sie den Zugriff auf diese Informationen erlauben, selbst wenn Sie die App gerade nicht verwenden.
- **WLAN, Bluetooth und NFC**
  Deaktivieren Sie nicht benötigte Dienste.
- **Internet-Router***
  Sichern Sie Ihren Router mit einem eigenen Passwort (mindestens 20 Zeichen) – behalten Sie nicht das voreingestellte Passwort des Herstellers.

Kamera und Mikrofon ausschalten

Eingebaute Kameras und Mikrofone können gehackt und zum Ausspionieren der Privatsphäre verwendet werden (z.B. Blick ins Wohnzimmer). Man kann die Kamera am Laptop mit einem Sticker überkleben, wenn man sie gar nicht braucht. Bei bestimmten Anwendungen (Video-Konferenzen, Internet-Telefonie) und im alltäglichen Gebrauch von Smartphones sind Kamera und Mikrofon aber zumeist notwendig.

Beispiel „https“ und „Schloss-Symbol“ im Firefox-Browser

Beispiel „https“ und „Schloss-Symbol“ im CM-Browser eines Smartphones (Android). Hier wird zusätzlich die Option „Privates Surfen“ verwendet, symbolisiert durch die „Maske“ (bei anderen Browsern z.B. Inkognitomodus).

Wird bei der Installation von Apps der Zugriff auf Kamera oder Mikrofon jedoch grundlos eingefordert, sollte man misstrauisch sein und darauf verzichten (→ siehe Grafik auf Seite 19).

Eine **Verschlüsselung* von Datenleitungen** im Internet erkennt man in der Adresszeile des Browsers am Kürzel **„https://“ (Hyper Text Transfer Protocol Secure)**. Es steht für ein sicheres Hypertext-Übertragungsprotokoll (anstelle des ungesicherten „http://“). Unter „https“ werden die Daten über ein sicheres Übertragungsprotokoll, das inzwischen veraltete SSL (Secure Sockets Layer) oder das verbesserte TLS (Transport Layer Security) transportiert.

TIPP

Achten Sie insbesondere bei Bestell- und Bezahlvorgängen auf das Kürzel **„https“** mit einem Schloss-Symbol im Browser.

Über „Add-ons“ können Sie in jedem Browser die Sicherheits-Erweiterung „https-Everywhere“ installieren. Mit ihr wird immer wenn möglich automatisch die verschlüsselte Version eines Internetangebots aufgerufen.

Eine **Schutz-Software** ist Pflicht, denn es gibt ständig neue digitale Schädlinge wie Viren, Spyware, Trojaner oder Würmer. Sie können z.B. Geräte schädigen, persönliche Daten ausspionieren und zu kriminellen Zwecken verwenden.

TIPP

Installieren Sie auf allen Geräten – auch auf Ihrem Smartphone – Schutzprogramme, also eine **Anti-Viren-Software** und eine **Firewall***. Suchen Sie auf Fachportalen im Internet nach entsprechenden positiv bewerteten Programmen (*www.chip.de*, *www.heise.de/security*) und aktualisieren Sie diese stets. Durch Updates werden Sicherheitslücken regelmäßig geschlossen.

TIPP

Sie können den Zugang zum Internet zeitweise ausschalten – vor allem nachts. Wenn Sie nicht immer den Stecker des Internet-Routers ziehen möchten, können Sie beispielsweise mit einer Zeitschaltuhr arbeiten. Bestimmte Internet-Router verfügen über die Möglichkeit, eine **Nachtschaltung** zu aktivieren (z.B. FritzBox). Natürlich sind Sie selber dann ebenfalls „offline".

Auch wenn es für Sie überflüssig klingt: Machen Sie Ihre Kinder darauf aufmerksam, dass die eigenen Passwörter wirklich geheim bleiben müssen. Es ist kein Freundschaftsbeweis, Passwörter weiterzugeben.

Elternhaus und Schule

In Elternhaus und Schule gelten die genannten Schutz- und Vorsichtsmaßnahmen zum Selbstdatenschutz nicht nur für „einen selbst", sondern Eltern und Pädagogen müssen auch auf ihre jungen „Schutzbefohlenen" achten. Kinder und Jugendliche sind im Umgang mit Techniken und Geräten anzuleiten und hinsichtlich Maßnahmen zum Selbstdatenschutz zu schulen. Wo dies an Grenzen stößt, können zumindest zeitweise auch technische Zugangsbeschränkungen oder Verbote notwendig sein.

TIPP

Für Geräte sollten Sie bis zu einem Alter von ca. 12 Jahren **gemeinsame Nutzungszeiten** vereinbaren, in denen Sie Ihre Kinder unterstützen und begleiten. Vereinbaren Sie **Nutzungspausen** oder behalten Sie insbesondere nachts die internetfähigen Geräte ein, wenn Sie der Meinung sind, dass Ihre Kinder leichtfertig agieren. Weisen Sie Ihre Kinder deutlich darauf hin: Bei **Downloads und Anmeldungen** im Internet sollten Sie grundsätzlich informiert werden. Installieren Sie **technische Schutzmaßnahmen** wie Jugendschutzprogramme, „Kinder Server" und Apps, wie „Meine-Startseite", „fragFINN" oder „Surfgarten".

Nutzungszeiten vereinbaren und Unterstützung anbieten

In der Schule ist zu unterscheiden:

Die Verwendung von eigenen Geräten der Schülerinnen und Schüler

Hierzu gibt es im „Bayerischen Gesetz über das Erziehungs- und Unterrichtswesen" folgende Regelung: „Im Schulgebäude und auf dem Schulgelände sind Mobilfunktelefone und sonstige digitale Speichermedien, die nicht zu Unterrichtszwecken verwendet werden, auszuschalten. Die unterrichtende oder die außerhalb des Unterrichts Aufsicht führende Lehrkraft kann Ausnahmen gestatten. Bei Zuwiderhandlung kann ein Mobilfunktelefon oder ein sonstiges digitales Speichermedium vorübergehend einbehalten werden" (Art. 56 Abs. 5 BayEUG).

Pseudonyme verwenden

Die Nutzung von schulischer Technik und Geräten im Unterricht

Im Idealfall werden die Geräte und Software von einem Administrator der Schule gepflegt und auf dem aktuellsten Sicherheitsstand gehalten. Schulungen über Sicherheitseinstellungen erscheinen sinnvoll. WLAN ist an Schulen umstritten, da die Gefahr des unkontrollierten Zugangs besteht (und damit des Missbrauchs z.B. durch illegale Downloads).

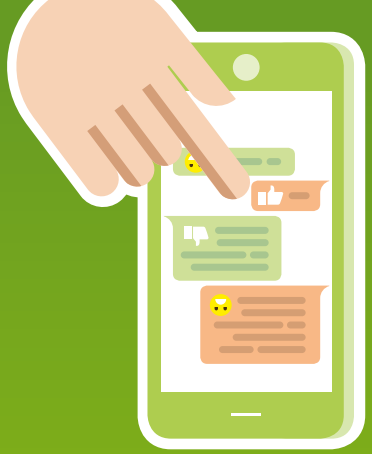
TIPP

Für die Nutzung des Internets im Unterricht gilt:

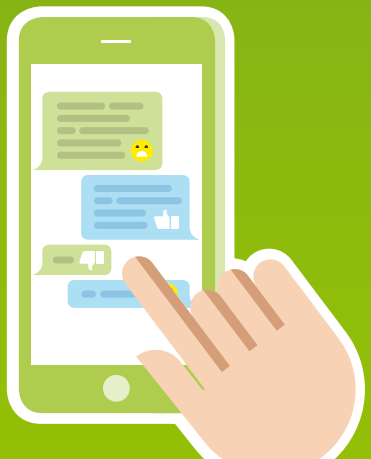
- Holen Sie die schriftliche Zustimmung **der Eltern** (und ab 14 Jahren auch der Schüler/innen) ein und klären Sie die Vorgehensweise der jeweiligen Schule ab.
- Erläutern Sie neben dem notwendigen Handlungswissen auch mögliche Gefahren. Erstellen Sie klare Regeln, deren Verstoß auch Konsequenzen hat (Risikoeinschätzung erfolgt durch die Lehrkraft).
- Arbeiten Sie – auch in Ihrem Kollegium – nach Möglichkeit in einem „gesicherten Internet" (z.B. eine eigene schulische Lernplattform, „Moodle", „lo-net²").
- Lassen Sie die Verwendung von „Nicknames" (**Pseudonymen**) statt Klarnamen zu. Dies gilt, wenn Sie mit anmeldepflichtigen Anwendungen im Internet arbeiten (externe E-Mail-Adressen, **Cloud-Dienst***)

Weiterführende Informationen

unter *www.blm.de/aktivitaeten/medienkompetenz/materialien.cfm*



Teil 2: Kommunikation mit mobilen Geräten



Teil 2 : Kommunikation mit mobilen Geräten

App-Diät

Einfach nur Gespräche führen mit dem Telefon – das war einmal. Heute gibt es Multifunktionsgeräte mit einer Vielzahl an Informations-, Unterhaltungs- und Kommunikationsmöglichkeiten: Telefonate sind über die normale Gesprächsfunktion oder über Internet-Telefonie mit Hilfe von Apps möglich (z.B. Skype, alternativ: Jitsi). Mit solchen Apps kann man sich zusätzlich per Video sehen und Konferenzschaltungen mit mehr als zwei Personen einrichten. Textnachrichten können über das Telefonnetz per SMS sowie über das Internet per E-Mail und mit Messenger-Apps versendet werden (z.B. WhatsApp oder Threema). Grundsätzlich gibt man bei der Installation und Nutzung aller Apps Daten von sich preis. Zugleich eröffnen sich durch Apps für Unbefugte Angriffsmöglichkeiten auf die eigenen Geräte. Klar ist: Wenn die Apps kostenfrei sind, müssen sich die Anbieter auf einem anderen Weg als über direkte Bezahlung finanzieren. Dies geschieht beispielsweise, indem Werbung angezeigt oder versendet wird, die auf Nutzerdaten beruht.

TIPP

Beachten Sie drei Schritte bei der App-Installation:

- **Vor einer Installation**
  Benötigen Sie die App wirklich?
- **Während der Installation**
  Welche Berechtigungen fordert die App? Welche Daten auf Ihrem Gerät wollen Sie für die Verwendung der App freigeben und ist dies unbedingt notwendig?
- **Nach der Installation**
  Welche Privatsphäre-Einstellungen sind voreingestellt und sind diese ausreichend? Ändern Sie die Einstellungen gegebenenfalls.

App-Diät:

Eine einfache Möglichkeit, um sich zu schützen, ist die Beschränkung auf seriöse und für Sie wirklich notwendige Apps. Seien Sie besonders kritisch bei scheinbar kostenlosen Apps – hier „bezahlen" Sie mit Werbeeinblendungen und mit Ihren Daten.

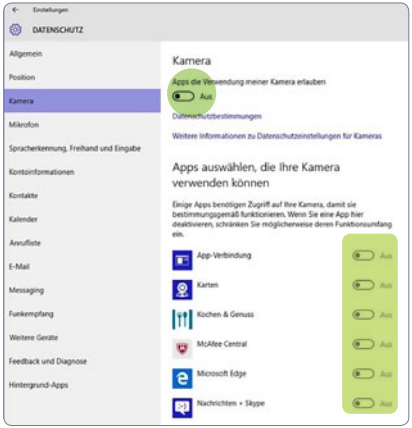
Die gängigste App für **Internet-Telefonie** ist **Skype**. Sie gilt wegen ihrer Verschlüsselung* nach außen als relativ gut geschützt vor Angreifern im Internet. Nicht jedoch vor ihrem Anbieter Microsoft: Dort verfügt man über die Zugriffsmöglichkeiten auf Daten bzw. Inhalte. Gesammelt werden die Profildaten der Nutzer, **IP-Adressen***, Zeitpunkt und Dauer der Nutzung sowie die Kontakte. Darüber hinaus werden alle Text-, Sprach- und Videonachrichten über einen gewissen Zeitraum gespeichert.

TIPP

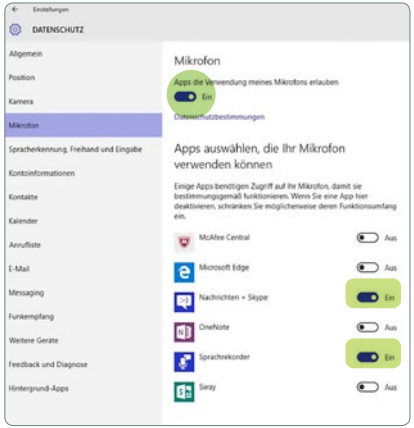
Erlauben Sie **Kommunikations-Apps** den Zugriff auf Kamera und Mikrofon auf Ihrem Gerät nur vorübergehend, wenn es für eine App bzw. Anwendung aktuell notwendig ist. Überprüfen Sie die „Privatsphäre"-Einstellungen.

Melden Sie sich mit einem **Pseudonym** an und teilen Sie dieses nur Freunden mit, mit denen Sie in Kontakt treten möchten. Eine Alternative zu Skype ist **Jitsi**.

Bei vielen Laptops und Tablets lassen sich unter „Einstellungen" → „Datenschutz" die Kamera und das Mikrofon ein- und ausschalten.



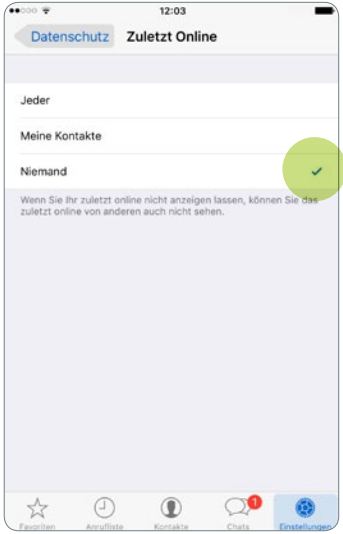
Kamera ist deaktiviert, daher ist sie auch für alle Apps deaktiviert.



Mikrofon ist aktiviert und kann daher gezielt für bestimmte Apps ein- und ausgeschaltet werden.

Textnachrichten bzw. **SMS** können von den Mobilfunkanbietern gespeichert werden – was sie angeblich nicht tun. Der polizeilich relevanten Vorratsdatenspeicherung unterliegen lediglich die Verbindungsdaten. Fraglich ist jedoch, ob eine Trennung von Verbindungsdaten und Inhalt tatsächlich eingehalten wird.

Über **Messenger-Dienste** (z.B. WhatsApp) können neben Textnachrichten auch Sprachdateien, Fotos und Videos versendet und Gruppenchats eingerichtet werden. Die neueste WhatsApp-Version verschlüsselt alle gesendeten Daten angeblich so, dass sie (auch vom Anbieter) nicht mitgelesen werden können. Jedoch lassen Sie weiterhin den Zugriff auf Ihre persönliche Kontaktliste mit Telefonnummern zu, um die App zu installieren und zu nutzen – und diese Daten werden beim Anbieter gespeichert.



TIPP

Überlegen Sie sich, ob Sie eine **Messenger-App** wirklich benötigen. Informieren Sie sich über mögliche Alternativen zu WhatsApp, die ebenfalls eine **Ende-zu-Ende-Verschlüsselung** bieten. Bedenken Sie: Dann müssen auch alle Ihre Kontakte diese Alternative verwenden (z.B. Open Whisper Systems, Threema, Signal).
Informationen unter: *www.handysektor.de*.

TIPP

Überprüfen Sie immer die Privatsphäre-Einstellungen (z.B. Synchronisation, Online-Status, Konto löschen). **Schalten Sie den Online-Status aus.**

Änderung der Sichtbarkeit des Online-Status bei WhatsApp über „Menüleiste am unteren Rand" → „Einstellungen" → „Account" → „Datenschutz" → Option „Niemand" auswählen.

TIPP

- **Senden Sie E-Mails auf einem verschlüsselten Übertragungsweg.** Selbst bei einer verschlüsselten Datenleitung können jedoch Sicherheitslücken am Gerät z.B. beim Senden und Empfangen bestehen. Bei der Nutzung eines eigenen E-Mail-Programms (z.B. Outlook/Thunderbird) auf Ihrem Gerät sollten Sie bei den Server-Einstellungen eine verschlüsselte Verbindung (Verschlüsselungsprotokolle veraltet: SSL/verbessert: TLS) und eine Authentifizierung mit Passwort auswählen.
  Freemail-Anbieter im Internet (z.B. Gmail, GMX, Yahoo, Web.de) verwenden verschlüsselte Datenleitungen, analysieren aber Ihre E-Mail-Inhalte für Werbeeinblendungen und das Ausfiltern von Spam.

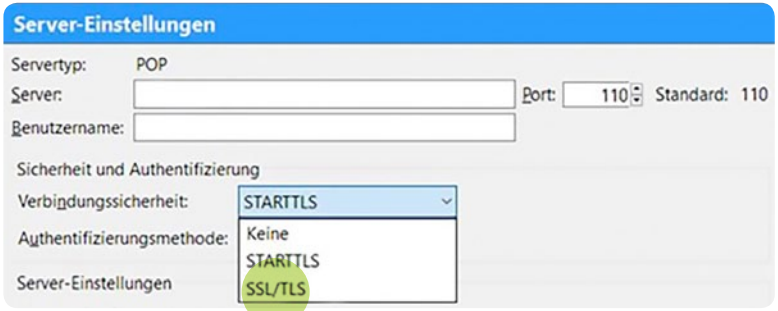
Verschlüsselung wählen

Auch bei **E-Mails** gilt das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis, welche nach Artikel 10 Absatz 1 des Grundgesetzes unverletzlich sind. Doch in der Praxis sind E-Mails gegen das „Mitlesen" durch Unbefugte nur sehr schwer zu schützen. Ein Versuch, dies zu ändern, ist die von der Bundesregierung unterstützte Einführung der „De-Mail". Dieser staatlich geprüfte E-Mail-Dienst soll in Zukunft eine rechtssichere Kommunikation in der Verwaltung ermöglichen.

TIPP

- **Auch der Inhalt der E-Mail sollte verschlüsselt werden.** Hierfür ist eine Reihe von Schritten notwendig. Eine Anleitung finden Sie z.B. unter: *www.bsi-fuer-buerger.de* oder unter: *www.verbraucher-sicher-online.de/artikel/e-mail-verschluesselung*.

Verschlüsselte Verbindung im E-Mail-Client des Smartphones einstellen:
→ „Einstellungen“
→ „Kontoeinstellungen“
→ „Weitere Einstellungen“
→ „Eingangsserver/ Ausgangsserver“



Verschlüsselte Verbindung im E-Mail-Programm eines Laptops (z.B. Thunderbird) unter → „Extras“ → „Konten-Einstellungen“ → „Server-Einstellungen“

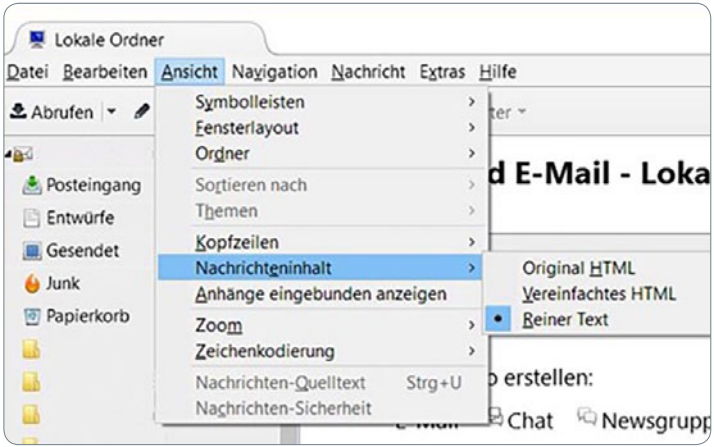
Vorsicht auch beim E-Mail-Empfang:
Über E-Mails wird nicht nur lästige Werbung, sondern werden auch gefährliche Schadprogramme verbreitet. Schädliche Viren- und betrügerische **Phishing-Mails*** zum „Abfischen“ persönlicher (Bank-)Daten werden immer professioneller. Die Zeiten, in denen man sie an schlecht gefälschten Firmenlogos und vielen Recht-schreibfehlern eindeutig erkennen konnte, sind vorbei.

TIPP

Öffnen Sie keine **Anhänge** oder **Links** in E-Mails von Unbekannten.

Deaktivieren Sie ggf. die **HTML-Ansicht** in Ihrem E-Mail-Programm. Damit werden die in einer E-Mail eingebetteten Inhalte, die gefährlich sind, deaktiviert. Versenden Sie keine persönlichen Daten und erst recht niemals Bankdaten, selbst wenn Sie dazu aufgefordert werden, weil dies angeblich „Ihrer Sicherheit" dient.

Legen Sie sich neben einer seriösen **E-Mail-Adresse** (für Arbeits- und Geschäftsleben) auch mindestens eine anonymisierte E-Mail-Adresse unter einem Pseudonym zu. Damit können Sie z.B. Newsletter abonnieren oder eine Anmeldung bei einem Angebot im Internet ausprobieren, ohne dass Ihre seriöse E-Mail-Adresse weiterverkauft und mit Spam (E-Mail-Abfall, unerwünschte Werbung) überschüttet wird.



Deaktivierung der HTML-Ansicht im E-Mail-Programm Thunderbird: → „Ansicht" → „Nachrichteninhalt" → „Reiner Text"

Kommunikation im Internet ist niemals ganz sicher – dies müssen wir bei wichtigen privaten oder beruflichen Angelegenheiten immer bedenken.

Kommunikation im Internet ist niemals ganz sicher

Elternhaus und Schule

Sprechen Sie mit Ihren Kindern sowohl über Risiken (z.B. Datenmissbrauch, Mobbing, falsche Freunde) als auch über Chancen der Internet-Kommunikation (z.B. Zusammenhalt, Austausch und Vernetzung, Information, Spaß). Die Nutzung von Kommunikationsdiensten gehört zum Alltag von Kindern und Jugendlichen dazu. Viele sind zwar kompetent in der Handhabung von Geräten und Apps, aber oftmals unbedacht und leichtsinnig, wenn es um ihre eigene Sicherheit geht.

Bedenken Sie: Falls Ihren Schutzbefohlenen etwas misslingt, schaffen Schuldzuweisungen und Verbote kein Vertrauen.

Schuldzuweisung und Verbote vermeiden

TIPP

Bieten Sie Ihre Unterstützung an. Achten Sie dabei auch auf die Privatsphäre Ihrer „Schützlinge".

Je nach Alter nehmen Sie Downloads und Anmeldungen bei Apps nach Möglichkeit gemeinsam mit Ihren Kindern vor. Überprüfen Sie gemeinsam die Privatsphäre-Einstellungen.

Machen Sie Ihre Kinder darauf aufmerksam: **Nachname, Adresse, Geburtsdatum und Telefonnummern werden nicht an Unbekannte weitergegeben.** Besprechen und erproben Sie die Möglichkeit einer anonymen Anmeldung bei einem Internet-Angebot.

Die Nutzung von **WhatsApp** ist laut den „Allgemeinen Geschäftsbedingungen" erst ab 16 Jahren erlaubt. Neugierde und Gruppendruck treiben jedoch auch schon Kinder und jüngere Jugendliche zu WhatsApp. Ein Verbot der Installation auf dem Gerät wäre möglich, ist aber mit einer dauerhaften Kontrolle verbunden und daher kaum durchführbar.

TIPP

Weisen Sie auf die kritischen Punkte bei der Nutzung von **WhatsApp** hin (Übertragung der Kontaktdaten, Online-Status, Mobbing-Gefahr, Kettenbriefe, Erreichbarkeitsdruck, Zugriffsberechtigungen). Zeigen Sie Alternativen auf und besprechen Sie Handlungsoptionen.

Weitere Informationen finden Sie beim Internet-ABC e.V., online unter: *www.internet-abc.de/eltern/familie-medien/kommunikation-handy-whatsapp-facebook/whatsapp/whatsapp-fuer-kinder-und-jugendliche*.

Internet-Kommunikationswege sind heute grundlegend für Ausbildung sowie Berufsleben und daher zentrale Elemente der **Medienbildung in der Schule**. Sie müssen daher schon im schulischen Kontext eingeübt und kompetent verwendet werden. Einsatzmöglichkeiten sind – in Ergänzung zur mündlichen Verständigung im Unterricht – beispielsweise der schriftliche Austausch über Termine und Inhalte (Wissen, Lernmaterialien, Aufgaben). Dies kann ortsunabhängig und sowohl gleichzeitig (per Gruppenchat) als auch zeitversetzt (per E-Mail) geschehen, gerade auch im Krankheitsfall.

TIPP

Die gängigsten Anwendungen bzw. Apps sind selten auch die datenschutzfreundlichsten. Gehen Sie mit gutem Beispiel voran und versuchen Sie, für Unterricht und Klassenkommunikation **alternative Angebote** zu nutzen. Möglicherweise ist dies mit Kosten verbunden.

- **Telefon- und Video-Konferenzen**
  Jitsi statt Skype
- **Messenger**
  Threema statt WhatsApp
- **E-Mail**
  Schuleigenes Web-Hosting mit eigenen E-Mail-Adressen statt Freemail-Angebote
- **Gesamtlösungen**
  Plattformen wie „lo-net²“ und „Moodle“ mit individuell einstellbaren Kommunikationsmöglichkeiten
- **Altersgrenzen**
  Bei allen Angeboten auf die Altersgrenzen für die Nutzung achten und die Zustimmung der Eltern einholen

Weiterführende Informationen
unter *www.blm.de/aktivitaeten/medienkompetenz/materialien.cfm*

Teil 3: Surfen, Web 2.0 und Cloud-Dienste

Teil 3 : Surfen, Web 2.0 und Cloud-Dienste

Bei jedem Aufruf einer Internetseite geben wir Persönliches von uns preis

Je mehr wir das Internet für unseren Alltag nutzen, desto mehr lässt sich hier etwas über uns erfahren. Bei jedem Aufruf einer Internetseite geben wir Persönliches von uns preis. Besonders gern ausspioniert wird unser gesamtes Surf- und Suchverhalten, weil sich die Datenspuren hier zu einem umfassenden Bild von uns verdichten lassen.

Auch die Dinge, die wir im Social Web ganz offen von uns zeigen oder in der **Cloud** für uns hinterlegen, sind nicht nur für diejenigen interessant, für die wir unsere Daten online stellen oder vorhalten. Ob Geheimdienste, professionelle Datenspione der Wirtschaft oder Kriminelle, die unsere Daten für ihre Zwecke missbrauchen wollen – alle suchen gezielt das Netz ab.

Doch wie behalte ich beim Surfen, im Social Web sowie in der Cloud ein Mindestmaß an Kontrolle über meine Daten? Kann ich überhaupt verhindern, dass ich bei der Nutzung des Internets ausspioniert werde? Auch hierfür gibt es nicht das eine Erfolgskonzept. Bereits mit der Auswahl von Browser und **Suchmaschine***, geänderten Einstellungen von den genutzten Angeboten und Diensten sowie mit zusätzlichen Tools lässt sich ein Abgreifen unserer Daten durch Dritte zumindest begrenzen.

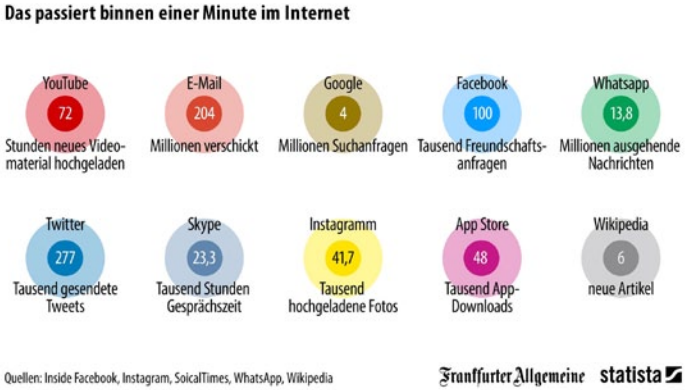
Bereits die **IP-Adresse*** verrät einiges über uns. Sie wird bei jeder Seiten- oder Suchanfrage übermittelt, damit die Server im Netz wissen, wohin sie das angefragte Angebot verschicken. Sie gibt Auskunft darüber, von wo aus man sich für das Angebot interessiert, welcher Provider genutzt wird und auch, ob man gerade mit einem internetfähigen Fernseher oder mobilen Endgerät (Smartphone, Tablet) online ist.

TIPP

- Rufen Sie die Internetseite eines **Lokalisierungstools** auf (z.B. *www.utrace.de*), um sich anzeigen zu lassen, welcher Region und welchem Provider Ihre aktuelle IP-Adresse zugeordnet ist.
- Mit der Nutzung von Proxyservern und speziellen Diensten (z.B. *www.anonymizer.com*) können Sie sich hinter einer anderen IP-Adresse „verstecken" und weitgehend anonym im Netz surfen.

Die IP-Adresse gehört zu den personenbezogenen Daten. Sie ermöglicht eine Zuordnung zu einer bestimmten Person. Auf sie kann aber bei der Internetnutzung nicht verzichtet werden. Ebenso kann sie nicht vollständig unterdrückt oder anonymisiert werden. Immerhin lässt sich so umgekehrt leicht herausfinden, was die eigene aktuelle IP-Adresse anderen verrät. Und es gibt Möglichkeiten, die Zugriffsmöglichkeiten darauf einzuschränken.

Auch der **Browser*** übermittelt Informationen. Auslesbar ist hier nicht nur, ob man gerade mit Firefox, Safari, Internet Explorer etc. surft, sondern auch die Version, die gewählte Bildschirm- und die Spracheinstellung.



Quelle: © FAZ.NET/Statista – Das passiert binnen einer Minute im Internet – *www.faz.net/aktuell/wirtschaft/wirtschaft-in-zahlen/grafik-des-tages-was-binnen-einer-minute-im-internet-passiert-13459083.html* (abgerufen am 17.Mai 2016) – Lizenz: CC BY-ND 3.0

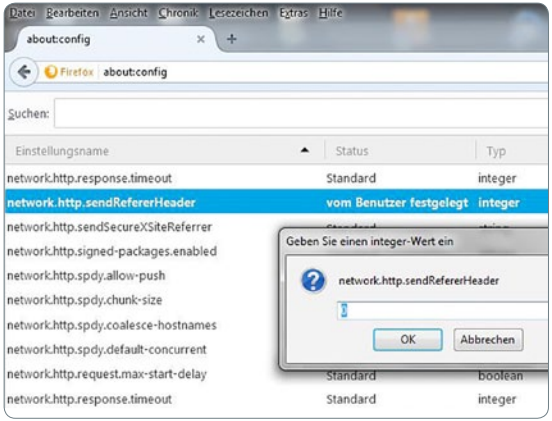
Deshalb erscheinen z.B. Werbeinhalte gleich optimiert und in Ihrer Sprache. Ist der **Referrer*** nicht deaktiviert, verrät der Browser zudem, welche Webseite zuvor besucht wurde. Beliebtes Angriffsziel ist die Browser-Chronik, in der alle Seitenbesuche hinterlegt werden.

TIPP

Mit **regelmäßigen Updates** erhöhen Sie nicht nur die Performance Ihres Browsers, sondern schließen auch Sicherheitslücken.

Unter *www.zendas.de/service/browserdaten.html* werden die aktuell von Ihrem Browser übermittelten Daten angezeigt.

Die **Browser-Chronik** lässt sich deaktivieren (unter „Einstellungen" → „Datenschutz" → „Chronik" → „niemals anlegen" wählen). Alternativ deaktivieren Sie den zuständigen „Referrer"* in Firefox folgendermaßen: Eingabe „about:config" in die Adressleiste des Browsers → „network.http.sendReferer-Header" in „Suchen" eingeben → Doppelklicken der nun erscheinenden, gleichlautenden Zeile → im sich öffnenden Fenster den Wert von „2" auf „0" ändern.



Browser-Chronik deaktivieren

Cookies löschen

Auf vielen Webseiten kommen standardmäßig **Cookies*** und **Zählpixel*** (Web-Bugs) zum Einsatz. Ihnen lässt sich entnehmen, was sich die Nutzer auf welcher Webseite wie lange anschauen, was sie wie oft anklicken und ob sie erstmalig die Seite nutzen. Bei Inhalten eingesetzt, die über viele Webseiten gestreut werden (z.B. Werbung), machen Cookies und Zählpixel Ihren Weg durch das Internet für andere nachvollziehbar.

TIPP

Mit der Anpassung der Einstellungen Ihres Browsers können Sie die Speicherung von **Cookies** verhindern (unter „Datenschutz“).

Surfen im **Privat-Modus** verhindert das Speichern von Cookies, Chronik, Suchanfragen und temporären Dateien.

Angezeigt und deaktiviert werden können **Zählpixel** als unliebsame **„Tracker“** mit Browser-Erweiterungen (Add-ons) wie „Ghostery“. Wer Sie aktuell gerade „beobachtet“, zeigt Ihnen das Add-on „Lightbeam“.

TIPP

Wer auf Adobe Flash beim Surfen nicht verzichten will, sollte regelmäßig den **Flash Player** (Programm zur Darstellung multimedialer sowie interaktiver Inhalte) aktualisieren, da auch so Sicherheitslücken geschlossen werden.

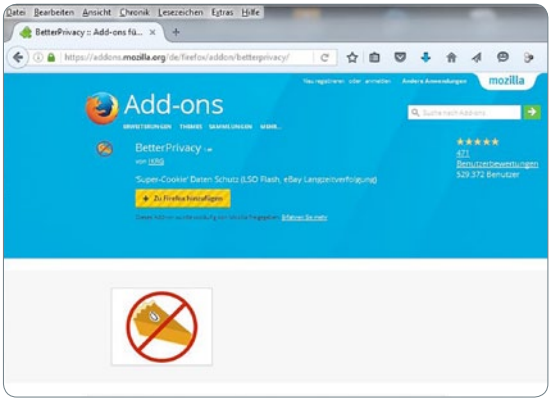
Über ein vom Flash Player bereitgestelltes Interface (Softwareschnittstelle) lassen sich Flash-Cookies webseitenbezogen löschen, seitenübergreifend geht dies nur auf der Adobe-Website.

Bei Firefox können Sie mit dem Add-on „BetterPrivacy“ unliebsame Flash Cookies automatisch bei jedem Start des Browsers löschen.

Flash-Cookies webseitenbezogen löschen durch Rechtsklick auf das Video:
→ „Einstellungen“
→ „lokaler Speicher“
→ „verweigern“ wählen

Rasant im Internet verbreitet haben sich auch **Flash-Cookies***. Sie nisten sich unabhängig von den Einstellungen des Browsers über den Adobe Flash Player auf Ihrem Computer ein. Schnell sammeln sich unbemerkt hunderte kleine Spione an und erfassen nahezu unbegrenzt die Aktivitäten der Nutzer, um von bestimmten Anbietern ausgelesen und ausgewertet zu werden.

Da für multimediale und interaktive Anwendungen von Webseiten häufig auf die Adobe Flash Plattform zurückgegriffen wird, ist der Flash Player oft notwendig, um die eingebundenen Animationen sowie Sound- und Videodateien korrekt dargestellt zu bekommen.



BetterPrivacy im Browser hinzufügen:
→ „Extras“
→ „Add-ons“
→ „Add-ons suchen“

oder direkt über den Link:
addons.mozilla.org/de/firefox/addon/betterprivacy/?src=ss.

Alternative Suchmaschinen verwenden

Umfangreiche Datenspuren hinterlassen wir bei der Nutzung von **Suchmaschinen**. Je mehr Dienste der entsprechende Anbieter unter seinem Dach hat, desto mehr kann er über uns herausfinden. Der Global Player **Google** verfügt über weitere populäre Dienste, z.B. YouTube, Gmail, Google Drive, Google+. Durch die Verknüpfung der hier erfassten Daten mit Suchanfragen weiß Google schnell sehr viel über uns – egal von welchem Endgerät (PC, Smartphone, Tablet etc.) wir die Dienste nutzen: Kommunikationsverhalten, Medienvorlieben und persönliche Interessen.

TIPP

Achten Sie auch bei der Websuche auf Ihre Privatsphäre. Sie können z.B. die Metasuchmaschine „**Ixquick**" nutzen. Eine weitere alternative Suchmaschine ist „**DuckDuckGo**". Mit der Nutzung von **Startpage** erhalten Sie anonymisierte Google-Ergebnisse.

Wenn Sie bei Google-Diensten angemeldet sind und einen Eindruck vom Netzwerk Ihrer Daten bekommen möchten, schauen Sie sich das Dashboard an (Anmeldung unter google.com/dashboard).

Mit Hilfe von **Cloud-Diensten** überall, jederzeit und unabhängig vom Endgerät auf seine Daten zugreifen zu können, ist sehr praktisch. Doch wie sicher sind **Google Drive**, **Dropbox**, **iCloud** & Co.? Wie kann ich verhindern, dass der Anbieter des Online-Speichers meine hinterlegten Daten einsehen kann oder die privaten Dokumente, Bilder, Videos etc. nach einem Hacker-Angriff im Netz landen? Einige Stars waren in den letzten Jahren Opfer solcher Attacken und mussten feststellen, dass z.B. Nacktaufnahmen von ihnen im Netz kursierten.

TIPP

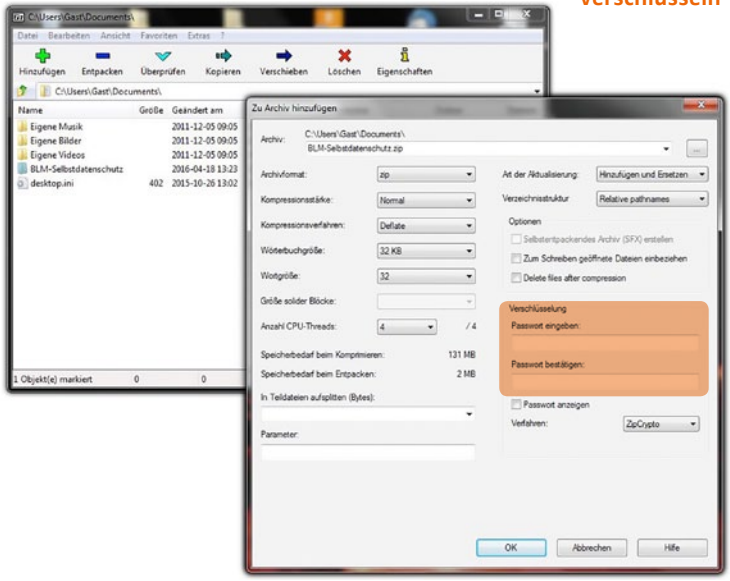
Wer den Sicherheitsstandards der **Cloud**-Anbieter nicht vollends vertraut, verschlüsselt seine Daten. Schnell erstellt sind passwortgeschützte Dateien-Archive mit freier Software wie 7-Zip (Windows/Linux) und iZip (OS X).

TIPP

Die Verschlüsselung von Datei-Archiven mit 7-Zip und iZip ist einfach:

- Installieren Sie 7-Zip (Windows/Linux) bzw. iZip (OS X) auf Ihrem Computer.
- Erstellen Sie ein Dateien-Archiv (Ordner) mit den zu verschlüsselnden Dateien.
- Öffnen Sie 7-Zip bzw. iZip, gehen Sie auf das erstellte Dateien-Archiv (Ordner) und klicken Sie auf „Hinzufügen".
- In dem geöffneten zweiten Fenster (siehe Bild) vergeben Sie nun ein Passwort und bestätigen mit „OK". Über den Windows-Explorer gelangen Sie zu diesem Fenster auch direkt über einen Rechtsklick mit der Maus → „7-Zip" → „Zu einem Archiv hinzufügen".
- Das so erstellte Zip-Archiv ist nun passwortgeschützt und kann speicherplatzsparend in der Cloud abgelegt werden.
- Zum Öffnen der Dateien oder Entpacken des gesamten Archives ist die Eingabe Ihres Passworts erforderlich.

In Cloud-Diensten gespeicherte Dateien verschlüsseln



Verschlüsselung von Datei-Archiven

Elternhaus und Schule

Das **Web 2.0*** bietet viele Möglichkeiten, selbst aktiv zu werden. Mit Postings auf **Facebook**, Fotos auf **Instagram** und Videos auf **YouTube** geben die User oft sehr viel Persönliches von sich preis. Vor allem junge Menschen agieren im **„Mitmachnetz"** unbefangen: Es geht ihnen um Spaß und Unterhaltung, Vernetzung und kreativen Selbstausdruck; weniger um Vorsicht und Zurückhaltung, auch was persönliche Daten anbetrifft. Elternhaus und Schule, Erziehende und Pädagogen sind hier besonders gefragt.

Die Rechte der Anderen im Netz achten

Die populären Dienste der Facebook Inc. (Facebook, WhatsApp, Instagram) sind bei jungen Menschen besonders beliebt. Doch gerade hier ist Vorsicht geboten und Selbstdatenschutz gefragt. Zwar wissen die meisten, dass ihre Daten die Basis der Finanzierung solcher Angebote sind. Doch was gespeichert, übermittelt und analysiert wird, das bleibt in den – umfangreichen und teils englischsprachigen – Datenschutzrichtlinien und Allgemeinen Geschäftsbedingungen nebulös.

Für die alltägliche Kommunikation wird heute zwar lieber WhatsApp genutzt, für den Austausch im „größeren Rahmen" hat **Facebook** aber noch immer eine besondere Relevanz. Mit den geposteten Texten, Bildern und Videos zeigen sie, was sie selbst machen. Und sie schauen, kommentieren und bewerten das, was andere so treiben. Zwar fühlen sich die wenigsten hinsichtlich des Schutzes ihrer Daten in den Netzwerken sicher. Oft geben sie hier trotzdem viel von sich und anderen preis.

TIPP

Achten Sie darauf, dass Ihre „Schützlinge" in Texten, Bildern oder Videos nicht zu viel Persönliches von sich in den **„Sozialen" Netzwerken** einstellen. Wie das Internet allgemein, „vergisst" auch Facebook nichts.

Noch unerfahrene Heranwachsende müssen dafür sensibilisiert werden, dass sie Daten oder Bilder von anderen (z.B. ihren Freunden, Lehrern und Eltern) nicht ohne deren Erlaubnis posten dürfen. Dies folgt aus dem **Recht am eigenen Bild.** Umgekehrt sollten sich Heranwachsende bewusst machen, dass ihre auf privaten Seiten eingestellten eigenen Daten oder Bilder von anderen missbräuchlich ohne Einholung einer entsprechenden Erlaubnis öffentlich gemacht werden können.

Wählen Sie für Profilinformationen und Beiträge **restriktive Privatsphäre-Einstellungen** (Anleitung unter: www.klicksafe.de).

TIPP

Ihre Selbstdarstellung im Netz sollten Schulen mit einem Auftritt auf einer eigenen Webseite realisieren.

Zur Verbreitung schulischer Informationen und Materialien sollten Schulen bzw. Lehrkräfte Lernplattformen wie Moodle und lo-net² nutzen. Gemäß Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus vom 24. Oktober 2012 (Az.: III.4-5 S 1356-3.18 725) ist von einer unterrichtlichen Nutzung Sozialer Netzwerke abzusehen.

Der „Leitfaden für Beschäftigte der Staatsverwaltung zum Umgang mit Sozialen Medien" sensibilisiert Lehrkräfte für die Eigenheiten Sozialer Netzwerke und empfiehlt bei der privaten Kommunikation mit Schülern und Eltern ein verantwortungsvolles Handeln (*www.social-media-lehrperson.info/wp-content/uploads/2013/09/Leitfaden-Social-Media-Web.pdf*).

Aus Gründen des Selbstdatenschutzes sollte die Nutzung von **Facebook im schulischen Kontext** eigentlich tabu sein. Lehrkräfte sollten Facebook-Gruppen nicht für schulische Zwecke nutzen. Wer Stundenpläne, Arbeitsblätter, Noten etc. nur (noch) hier bekannt gibt, zwingt (einzelne) Schüler zur Facebook-Nutzung und kann unter Umständen eine Vermischung schulischer und privater Informationen nicht vermeiden.

Mit weltweit 1 Mrd. Nutzern ist auch Googles **YouTube** ein Schwergewicht. Eine besondere Bedeutung hat die Videoplattform für junge Menschen – hierzulande ist sie sogar das beliebteste Internetangebot Jugendlicher: Die meisten nutzen es täglich, um sich Videos, Clips oder zeitversetzt Fernsehinhalte anzusehen. Angemeldet im persönlichen Konto werden die mit Cookies nachverfolgten Spuren mit den Daten der anderen Google-Dienste zusammengeführt.

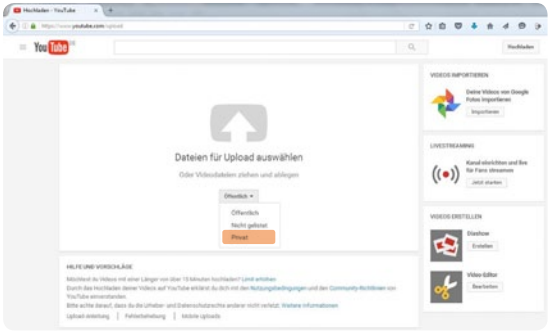
Diejenigen, die selbst Videos einstellen, sollten bewusst entscheiden, ob sie diese öffentlich und damit für alle sichtbar einstellen.

Hochgeladene Videos nicht für alle sichtbar machen

TIPP

Auch beim **Einstellen von Videos** ist darauf zu achten, dass

- keine persönlichen Informationen veröffentlicht werden (Name, Adresse, Telefonnummer etc.),
- Minderjährige nicht sexualitätsbezogen dargestellt sind,
- keine Dritten ohne deren Erlaubnis abgebildet sind (Recht am eigenen Bild) und
- keine urheberrechtlich geschützten Musik- oder Filmaufnahmen verwendet werden.



Veröffentlichungsoptionen für das Hochladen von Videos bei YouTube, abrufbar unter: *www.youtube.com/upload*

TIPP

Erläutern Sie die Vor- und Nachteile von personalisierter und **anonymisierter Nutzung**. Wenn Sie oder Ihre Kinder bei **YouTube** weitgehend anonym Videos sehen wollen, melden Sie sich nicht an und nutzen Sie die beschriebenen Browser-Einstellungen und -erweiterungen, um Cookies zu unterbinden.

Weisen Sie auf die Veröffentlichungsoptionen beim Hochladen von Videos auf YouTube hin (siehe Grafik). Eingestellte Videos (standardmäßig: „Öffentlich“) können auch nachträglich „Privat“ gestellt werden. Hierfür unter „Video-Manager“ → Option „Bearbeiten“ wählen, → „Öffentlich“ anklicken → **„Privat“** auswählen.

Weiterführende Informationen

unter *www.blm.de/aktivitaeten/medienkompetenz/materialien.cfm*

Teil 4: Einkaufen und Bezahlen

Teil 4: Einkaufen und Bezahlen

Beim Einkauf im Netz werden sensible Daten hinterlassen

Das Internet wird auch für den Erwerb von Produkten und Dienstleistungen sowie für die Abwicklung von Bezahlvorgängen und Bankgeschäften immer wichtiger. Fast jeder fünfte Internet-User tätigt hierzulande mindestens einmal pro Woche online Einkäufe, jeder Dritte nutzt das Onlinebanking. Onlineshopping bietet im Vergleich zum Einkauf im Einzelhandel Vorteile wie den Zugriff auf eine breite Angebots- und Produktpalette bequem von zu Hause aus, die Nutzung von Preisvorteilen, einfach zum Ziel führende Suchmöglichkeiten, mühelose Vergleichsoptionen und die schnelle Abwicklung von Bestellung und Bezahlung.

TIPP

- Nutzen Sie nur die geprüften, mit **Gütesiegel** gekennzeichneten Onlineshops.
- Bestellen Sie nur von Ihrem eigenen, gesicherten Gerät aus.
- Achten Sie bei Bestellvorgängen auf eine verschlüsselte Datenübertragung **„https://"** bzw. **„Schloss-Symbol"** (→ siehe Seite 14).

Gemäß dem Motto „Bei uns finden Sie alles!" bieten große Online-Verkaufsplattformen ihren Nutzern Vorteile, für die man in der Offline-Welt lange unterwegs wäre. Einmal ein Kundenkonto angelegt, ist der Kauf schnell abgewickelt.

Gerade beim Einkaufen und Bezahlen im Netz hinterlassen wir aber sensible Daten, die besonderen Schutz benötigen. Ohne vollständigen Namen, korrekte Adresse sowie Bankverbindung oder Kreditkartennummer geht kaum etwas. Verschiedene Dienstleister versprechen zwar weitgehende Datensicherheit, doch sollten wir uns darauf nicht verlassen. Schutzmechanismen bei Hardware und Internetzugang sind hier nur ein erster Schritt.

Weiterführende Informationen zu Gütesiegeln für sichere Shops:
www.verbraucher-sicher-online.de/artikel/online-einkaufen-sichere-schnaeppchenjagd-per-mausklick

Online-Versandhändler wie Amazon bestimmen mit ihrer Produktpalette, Preispolitik und Kaufabwicklung nicht nur den Verkaufsmarkt, sondern auch technische Standards des Handels. Daher ähneln sich viele Angebote sowohl optisch als auch hinsichtlich der Erfassung, Speicherung und Verwendung sensibler Kundendaten.

Wer sich nicht nur informieren, sondern Produkte auch erwerben will, kommt bei vielen Online-Händlern an einer Registrierung nicht vorbei. Im **Kundenkonto** dauerhaft gespeichert werden in aller Regel Name, Adresse, E-Mail und Bank- oder Kreditkartenverbindung. Um sich später als Kunde zu authentifizieren, ist ein Kennwort erforderlich. So angemeldet, wird dann nicht nur nachverfolgt, was den Kunden gerade interessiert, sondern dies auch mit den hinterlegten Daten verknüpft. Das ist der Grund, weshalb Werbung dann persönlich auf Sie zugeschnitten ist.

TIPP

Falls ein Einkauf auch ohne Kundenkonto möglich ist, nutzen Sie diese Option. Ihre Daten werden dann nur für die jeweilige Kaufabwicklung gespeichert.

Wenn eine Bestellung nur für registrierte Kunden möglich ist, geben Sie nur die Daten an, die zur Nutzung unbedingt erforderlich sind (**„Pflichtangaben"**).

Verwenden Sie für Ihr Kundenkonto unbedingt ein **sicheres Passwort** (→ siehe Seite 11).

Bestellungen ohne Kundenkonto

Einige Onlineshops ermöglichen die Kaufabwicklung über spezielle Online-Bezahlsysteme wie ClickandBuy, Sofortüberweisung oder das bis Mitte letzten Jahres zu Ebay gehörende PayPal.

TIPP

Wie sicher und komfortabel Online-Bezahlsysteme im Einzelnen sind, erfahren Sie z.B. in den **Testberichten** von bekannten Computerzeitschriften.

Auch die bereits angeführten Gütesiegel für „sichere Onlineshops" berücksichtigen die hier genannten Bezahlsysteme (→ siehe Seite 38).

Webseiten zum Onlinebanking nicht über Suchmaschinen aufrufen

Seit Jahren nutzen immer mehr Deutsche auch **Onlinebanking**. Obwohl sie Sicherheit und Datenschutz höher gewichten als Schnelligkeit, Bequemlichkeit und Unabhängigkeit von Ort und Zeit, halten sie Meldungen zu Sicherheitsproblemen nicht davon ab. Eine 100-prozentige Sicherheit gibt es jedenfalls beim Onlinebanking nicht. Wie beim Geldabheben am Automaten oder Kartenlesegerät im Geschäft können Kriminelle auch bei unseren Online-Bankgeschäften via PC, Laptop oder mobilen Endgerät die Zugangsdaten ausspähen, um Zugriff auf unser Konto zu erhalten. Tatsächlich werden jährlich tausende Betrugsfälle zur Anzeige gebracht. Der Gesamtschaden addiert sich auf mehrere Millionen Euro.

Die **Zugangsdaten** haben beim Banking nach wie vor eine besondere Bedeutung. Die vierstellige Persönliche Identifikationsnummer (PIN), die von den Kreditinstituten für die Nutzung der EC- oder Kreditkarte vergeben wird, gehört zu den sensibelsten Daten überhaupt. Ebenso die selbstgewählte fünfstellige PIN für das Onlinebanking. Bereits hier gelten besondere Anforderungen an die Aufbewahrung und Nutzung.

TIPP

EC- und Kreditkarten-PIN nie ungeschützt aufbewahren oder speichern, keinesfalls an Dritte weitergeben und bei der Eingabe am Automaten oder Kartenterminal immer verdecken.

Nutzen Sie fürs **Onlinebanking** nur die eigenen Endgeräte und das eigene Netzwerk (bei WLAN eine WAP2-verschlüsselte Verbindung). Beachten Sie bei der Wahl der PIN für den Zugang zum Onlinebanking auch die Anforderungen an ein sicheres Passwort (→ siehe Seite 11 und 12).

Geben Sie die Web-Adresse per Hand ein (Vorsicht **Phishing**-Seiten: kein Aufruf der Bankseiten über Suchmaschinen).

Achten Sie auf eine verschlüsselte Datenübertragung „https://“ bzw. „Schloss-Symbol“ (→ siehe Seite 14).

Für das Onlinebanking stehen heute unterschiedliche Verfahren zur Verfügung. Nach erfolgreicher Anmeldung im Account (Nutzerkonto) wird meistens für jedes Bankgeschäft (Überweisung, Einrichtung eines Dauerauftrages etc.) die Eingabe einer separaten Transaktionsnummer (TAN) verlangt. Ein bereits früh eingesetztes Verfahren zur Autorisierung einer Transaktion im Onlinebanking ist die Eingabe einer mit Positionsnummer gekennzeichneten **iTAN**. Diese findet der Nutzer auf einer Liste, die ihm von der Bank per Post zugesandt wird. Haben Dritte Ihre Zugangsdaten zum Onlinebanking und Zugriff auf die iTAN-Liste, können sie auch auf Ihr Konto zugreifen.

TIPP

Bewahren Sie **iTAN-Listen** an einem sicheren, nur Ihnen bekannten Ort auf.

Da sich in der Vergangenheit einige Sicherheitsmängel dieser Listen offenbarten, bieten viele Kreditinstitute heute alternative, vermeintlich sichere Verfahren an. Mit den spezifischen Funktionsweisen und verschiedenen Bezeichnungen (z. B. mobileTAN, pushTAN, chipTAN, Sm@rt-TANplus) ist der Markt allerdings sehr unübersichtlich geworden. Eine schon weit verbreitete Alternative zur herkömmlichen iTAN ist **mTAN** (die mobile TAN). Sie wird im mTAN-Verfahren für jede anstehende Transaktion unter Einbezug der Auftragsdaten neu erzeugt und dann per SMS an die Mobilfunknummer geschickt, die Sie vorher bei der Bank registriert haben müssen. Die höchste Sicherheit beim Onlinebanking bietet aktuell das kostenpflichtige **HBCI** (Homebanking Computer Interface) mit Kartenlesegerät und spezieller Software.

TIPP

Nutzen Sie Ihr Smartphone nicht gleichzeitig zum **Onlinebanking** und Empfang der mTAN und überprüfen Sie Ihre Auftragsdaten in der SMS.

Machen Sie sich mit weiteren alternativen TAN-Verfahren vertraut, die von Ihrer Bank angeboten werden (Übersicht unter: *www.verbraucher-sicher-online.de/artikel/uebersicht-tan-verfahren-ausgewaehlter-banken*).

Wenn Sie das HBCI-Verfahren nutzen möchten, sollten Sie sich bei der Anschaffung der Software an Ihre Bank richten. Nähere Informationen finden Sie unter *www.hbci-zka.de*.

Kontoabbuchungen kontrollieren

Elternhaus und Schule

Jugendliche und sogar Kinder können heute ganz regulär in Geschäften bargeldlos bezahlen, am Automaten Geld abheben und online shoppen gehen. Wegen ihrer beschränkten Geschäftsfähigkeit und ihres besonderen Schutzbedarfs gibt es spezielle Angebote, bei denen einige Risiken von vornherein ausgeschlossen sind. Richten Eltern ihren Kindern ein eigenes Konto ein, mit dem auch Onlinebanking möglich ist, sollten den Minderjährigen die besonderen Anforderungen an Sicherheit und Datenschutz erläutert werden.

Schon bevor die eigenen Kinder in die Schule gehen, ist es Eltern bei vielen Kreditinstituten möglich, für sie ein Sparbuch oder Girokonto anzulegen. Die Konditionen hierfür sind durchaus attraktiv, da Kinder und Jugendliche mit der gestiegenen Kaufkraft der letzten Jahre längst eine attraktive Zielgruppe von Banken sind. Zum kostenlosen Konto gibt es deshalb nicht selten weitere Extras dazu.

Ein **Girokonto für Kinder** dürfen Eltern bereits für Neugeborene einrichten. Eine eigene Bankkarte, die auch das Abheben von Geld ermöglicht, geben die Banken frühestens für Kinder ab 7 Jahren heraus. Ab diesem Alter sind abgeschlossene Verträge nach dem sog. Taschengeldparagraphen (§ 110 Bürgerliches Gesetzbuch) wirksam, sofern die Eltern ihren Kindern den Erwerb bestimmter Waren und Dienstleistungen nicht ausdrücklich verbieten und die Kinder den Einkauf mit dem Taschengeld bezahlt haben. Auch wenn Kinder heute meist schon im Grundschulalter Erfahrungen im Umgang mit Geld sammeln, ist das Erlernen eines selbständigen Umgangs mit einem eigenen Konto oft erst später sinnvoll.

TIPP

Wenn Sie für Ihr Kind ein **eigenes Konto** möchten, eröffnen Sie ein Kinderkonto ohne Überziehungsmöglichkeit und Dispositionskredit. Eine sinnvolle Option sind auch eingeschränkte Geldkarten, die mit einem Guthaben aufgeladen werden müssen.

Mittlerweile können Kinder sogar eine **Prepaid-Kreditkarte** nutzen. Im Prinzip funktioniert das wie bei den aufladbaren Handykarten: Es kann nur mit einem vorhandenen Guthaben bezahlt werden. Damit sind zwar eine Kontoüberziehung und Verschuldung der Kinder ausgeschlossen und ist das kreditorische Missbrauchsrisiko reduziert. Die speziellen Anforderungen zum Schutz persönlicher Daten beim Einsatz in Geschäften, an Automaten und im Internet bleiben aber bestehen.

TIPP

Klären Sie Ihre Kinder auf, dass die Daten einer Prepaid-Kreditkarte wie die eines Kinderkontos **höchstpersönliche Daten** sind, die nicht an Dritte weitergegeben werden dürfen und auch online zu schützen sind.

Selbst Anschaffungen tätigen und abwickeln können ist für Kinder noch in einem anderen Bereich wichtig: In der Welt der Apps. Die beliebten Plattformen, allen voran Google Play Store und der Apple App Store, bieten Vielzahl und Vielfalt in einem – wirklich umsonst ist hier allerdings nichts. Auch wenn viele Apps an sich kostenlos sind, lauern oft doch versteckte Kosten. Die persönlichen Daten der minderjährigen User sind die Währung, mit der die Nutzung ermöglicht wird.

Obwohl kostenpflichtige Apps und **In-App-Käufe** in aller Regel kein Vermögen kosten, können vor allem jüngere Nutzer bei den (vielen) kleineren Beträgen schnell die Übersicht verlieren.

Im Google Play Store werden Apps mit In-App-Kaufoption nicht mehr mit „free“ gekennzeichnet. Im App Store steht der Hinweis auf die Kaufmöglichkeiten inzwischen schon in der Beschreibung.

Vor dem App-Kauf Zugriffsberechtigung prüfen

TIPP

Mit **Prepaid-Gutscheinen** für die Stores limitieren Eltern nicht nur die Kosten für Apps und In-App-Käufe, sondern verhindern auch die Übermittlung von persönlichen Daten.

Eltern können mit Einstellungen in den Betriebssystemen der Geräte ihrer Kinder die Kontrolle über **App-Käufe** und **In-App-Käufe** behalten (*www.klicksafe.de/themen/kommunizieren/smartphones/apps-abzocke/s/inapp/*).

Die Welt der Apps stellt eine besondere Herausforderung an den Schutz der persönlichen Daten erwachsener wie auch junger Nutzer: Um ihre Funktionen ausführen zu können, fordern Apps bei den Endgeräten Berechtigungen für den Zugriff auf bestimmte Datenbereiche (→ siehe Seiten 18 und 19). Mit dem Herunterladen akzeptieren nicht nur junge Nutzer dann oft den Zugriff auf beispielsweise die eigenen Kontakte, persönliche Nachrichten und den Standort.

Den Ratgeber der Stiftung Medienpädagogik Bayern **„Apps sicher nutzen – Mobile Geräte in Kinderhand"** finden Sie unter: *www.stiftung-medienpaedagogik-bayern.de* in der Rubrik „Materialien"

TIPP

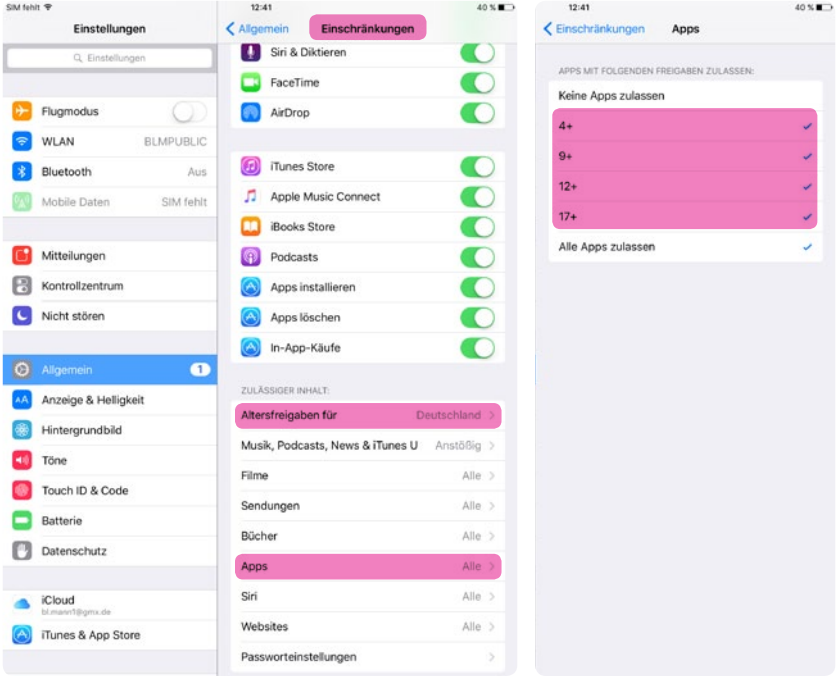
Eltern jüngerer Kinder sollten sich mit ihnen gemeinsam die geforderten Zugriffsberechtigungen ansehen.

Ältere Kinder sollten von ihren Eltern für die Datenschutzgefahren, die mit **Berechtigungen** verbunden sind, sensibilisiert werden.

Mit Datenschutz-Apps wie AppGuard (Android) oder Einstellungen im Betriebssystem (iOS) können einige Zugriffe auch beschränkt werden.

Weiterführende Informationen

unter *www.blm.de/aktivitaeten/medienkompetenz/materialien.cfm*



Altersfreigaben im Betriebssystem iOS verwalten

Glossar

App
Kurzform von *engl. application* (dt.: Anwendung) vor allem für typische Kleinprogramme von Smartphones und Tablets. Für ihre Funktionalität fordern die Apps bei der Installation die Zustimmung zum Zugriff auf die Daten des jeweiligen Geräts – nicht selten viel mehr, als eigentlich für die Funktion notwendig.

Big Data
Big Data (dt.: große Datenmengen) bezeichnet die Verfüg- und Verwertbarkeit ständig wachsender Datenmengen im Internet. Big Data wird einerseits als Chance gesehen, um z.B. durch Datenauswertung medizinische Behandlungen zu verbessern. Andererseits steigt das Risiko des Missbrauchs großer Datenmengen, z.B. durch die Erstellung von Bewegungsprofilen und damit zur Überwachung von Personen.

Bluetooth
Funkstandard für Datenübertragung zwischen Geräten im Nahbereich (bis 10 Meter). Die austauschenden Geräte müssen vom jeweiligen Besitzer „gekoppelt" werden.

Browser
Programme, die notwendig sind, damit Internetseiten mit den verschiedenen Endgeräten (PC, Laptop, Smartphone, Tablet etc.) aufgerufen und angezeigt werden können. Die aktuell am häufigsten genutzten Browser sind mit zusammen fast 90 Prozent Marktanteil: Firefox, Google Chrome, Safari und Internet Explorer.

Cloud(-Dienste)
Externer Speicherort für Dateien (Dokumente, Bilder, Videos etc.) und Dateienarchive. Diese werden auf einem Rechner abgelegt, auf den mittels des Internets (oder mittels eines anderen Computernetzwerks) zugegriffen werden kann. So kann man unabhängig vom aktuell genutzten Endgerät auf alle seine in der Cloud abgelegten Daten zugreifen.

Cookies
Kleine Dateien, die beim Besuch auf der Webseite auf dem Rechner gespeichert werden, damit zum Beispiel persönliche Einstellungen nicht verloren gehen. Im Gegensatz zu Session-Cookies, die mit dem Schließen des Browsers automatisch gelöscht werden, gibt es auch Cookies, die die Informationen unter ihrer ID dauerhaft speichern. Unabhängig vom Browser können sich bei Nutzung von Flash Playern zum Abruf von Multimediaeinbindungen (z.B. Videos) auf Webseiten auch Flash-Cookies in zentralen Ordnern des Computers einnisten und von dort aus die Aktivitäten der Nutzer ausspähen. Diese Cookies haben nicht nur eine längere Verweildauer, sondern können auch größere Datenmengen erfassen.

Firewall
Eine Firewall (dt. Schutzwall) ist ein Sicherungssystem zwischen Internet und eigenem Netzwerk bzw. Geräten: Unerwünschte Zugriffe werden blockiert und nur erwünschte Verbindungen zugelassen. Die Blockaderegeln können vom Nutzer vorgegeben werden.

Internet-Router
Vermittlungsgerät für den Internet-Anschluss, der die Verbindung zu den eigenen Endgeräten herstellt und steuert.

IP-Adresse
Das Internetprotokoll (IP) legt fest, welche Daten zwischen Computern ausgetauscht werden. Für den Datenaustausch im Internet werden den verschiedenen Computern und Servern im Netz IP-Adressen zugewiesen, anhand derer der jeweilige Computer bzw. Server eindeutig identifizierbar ist. Die Adressen stellen sicher, dass die angefragten bzw. ausgegebenen Daten an das richtige Gerät geschickt werden.

NFC
Near Field Communication (NFC, dt.: Nahfeldkommunikation) ist eine Funktechnik zur Datenübertragung auf kürzester Distanz (ca. 10 cm). Sie soll in Zukunft insbesondere bei Bezahl-Terminals eingesetzt werden.

Phishing
Der englische Begriff für *password-fishing* – das betrügerische „Abfischen" von Daten bzw. Passwörtern mit Hilfe von gefälschten E-Mails oder Internetseiten.

Provider (auch Internetprovider/-anbieter)
Anbieter von Diensten, Inhalten und technischen Infrastrukturen (DSL, WLAN etc.), die für die Nutzung des Internets erforderlich sind. Mit über 12 Mio. Kunden war die Telekom 2015 der mit Abstand größte DSL-Anbieter in Deutschland.

Referrer (auch Referer)
Internetadresse der Webseite, von der man (z.B. über eine Verlinkung) auf die aktuelle Seite gekommen ist. Bei den gängigen Browsern ist voreingestellt, dass der Referrer bei Aufruf einer Webseite als Teil der HTTP-Anfrage mit an den betreffenden Webserver geschickt wird.

SIM-Karte
SIM-Karte (engl. Subscriber Identity Module), kleine Plastikkarte mit dem digitalen Teilnehmer-Identitätsmodul und Datenspeicher.

Suchmaschine
Programme zur gezielten Suche und Recherche von Daten und Dokumenten auf Computern und in Computernetzwerken. Internetsuchmaschinen durchsuchen das Netz nach relevanten Webseiten. Basis ist ein Index, in dem Informationen über die Seiten abgelegt werden. Die ausgegebenen Ergebnisse sollen für die Suchbegriffe möglichst „passende" Webseiten anzeigen und sie nach Relevanz ordnen. Mit über 90 Prozent Marktanteil ist Google in Deutschland die mit Abstand bedeutendste Suchmaschine.

Verschlüsselung (im Internet)
Übersetzung von sinnvollen, lesbaren Daten in scheinbar sinnlose, unlesbare Daten, die nur „entschlüsseln" kann, wer über den passenden Schlüssel verfügt. Bei der Verschlüsselung im Internet gibt es zwei Varianten: Die Transportwegverschlüsselung oder die Leitungsverschlüsselung (auch: Punkt zu Punkt-Verschlüsselung) zwischen den Geräten. An den sendenden und empfangenden Geräten selbst besteht keine Sicherheit. Sicherer ist die Ende zu Ende-Verschlüsselung: Der Sender verschlüsselt und der Empfänger entschlüsselt jeweils die Daten in seinem E-Mail-Programm.

Web 2.0
Betont die Aktivität der Internetnutzer. Im Web 2.0 nehmen die Nutzer nicht mehr nur Internetseiten wahr, um sich zu informieren oder unterhalten zu lassen, sondern sie stellen selbst Inhalte ein (user generated content), kommentieren und bewerten die Inhalte anderer, tauschen sich im Netz untereinander aus und vernetzen sich miteinander. Sie werden vom reinen Nutzer zum Prosumer (englischer Begriff für eine Person, die gleichzeitig Produzent und Konsument ist), der selbst Inhalte anbietet.

WLAN
WLAN, engl. Wireless Local Area Network, ist ein kabelloses, lokales Funknetzwerk für den Internetzugang.

WPA2-Standard
Bezeichnet eine besonders sichere Verschlüsselungstechnik für WLAN mit einem langen Passwort.

Zählpixel (auch Tracking-Bugs oder Web-Bugs)
Kleine, mit bloßem Auge meist unsichtbare Grafiken auf Webseiten (oder in HTML-E-Mails). Sie ermöglichen die Aufzeichnung und Analyse von Logdateien, die die Aktionen und Prozesse auf einem Computersystem protokollieren. Zählpixel werden oft für die statistische Auswertung des Nutzerverhaltens verwendet (z. B. für Werbung und Online-Marketing).

Umfassende Begriffserläuterungen finden Sie online z. B. unter:

- *www.handysektor.de*
  Ein Informationsangebot für Jugendliche zum kompetenten Umgang mit mobilen Medien
- *www.bsi-fuer-buerger.de*
  „BSI für Bürger"
  Ein Informationsangebot des Bundesamtes für Sicherheit in der Informationstechnik

Unseren Online-Ratgeber für Mediennutzer „total digital" finden Sie unter:
www.blm.de/aktivitaeten/total_digital.cfm

Diese Broschüre, weitere Literatur sowie hilfreiche Internetangebote finden Sie unter:
www.blm.de/aktivitaeten/medienkompetenz/materialien.cfm

Stichwortverzeichnis

Impressum

Herausgeber
Bayerische Landeszentrale
für neue Medien (BLM)

Verantwortlich
Verena Weigand

Redaktion
Dr. Kristina Hopf
Annalivia Becker

Autoren
Dr. Olaf Selg, Dr. Daniel Hajok
Arbeitsgemeinschaft Kindheit,
Jugend und neue Medien
(AKJM, www.akjm.de, info@akjm.de)

Layout/Illustration
Mellon Design GmbH

Druck
Senser Druck GmbH

München, 2016

Bayerische Landeszentrale für neue Medien • Rechtsfähige Anstalt des öffentlichen Rechts
Heinrich-Lübke-Straße 27 • 81737 München • Tel. +49 (0)89 63808-278 • Fax +49 (0)89 63808-290
blm@blm.de • www.blm.de