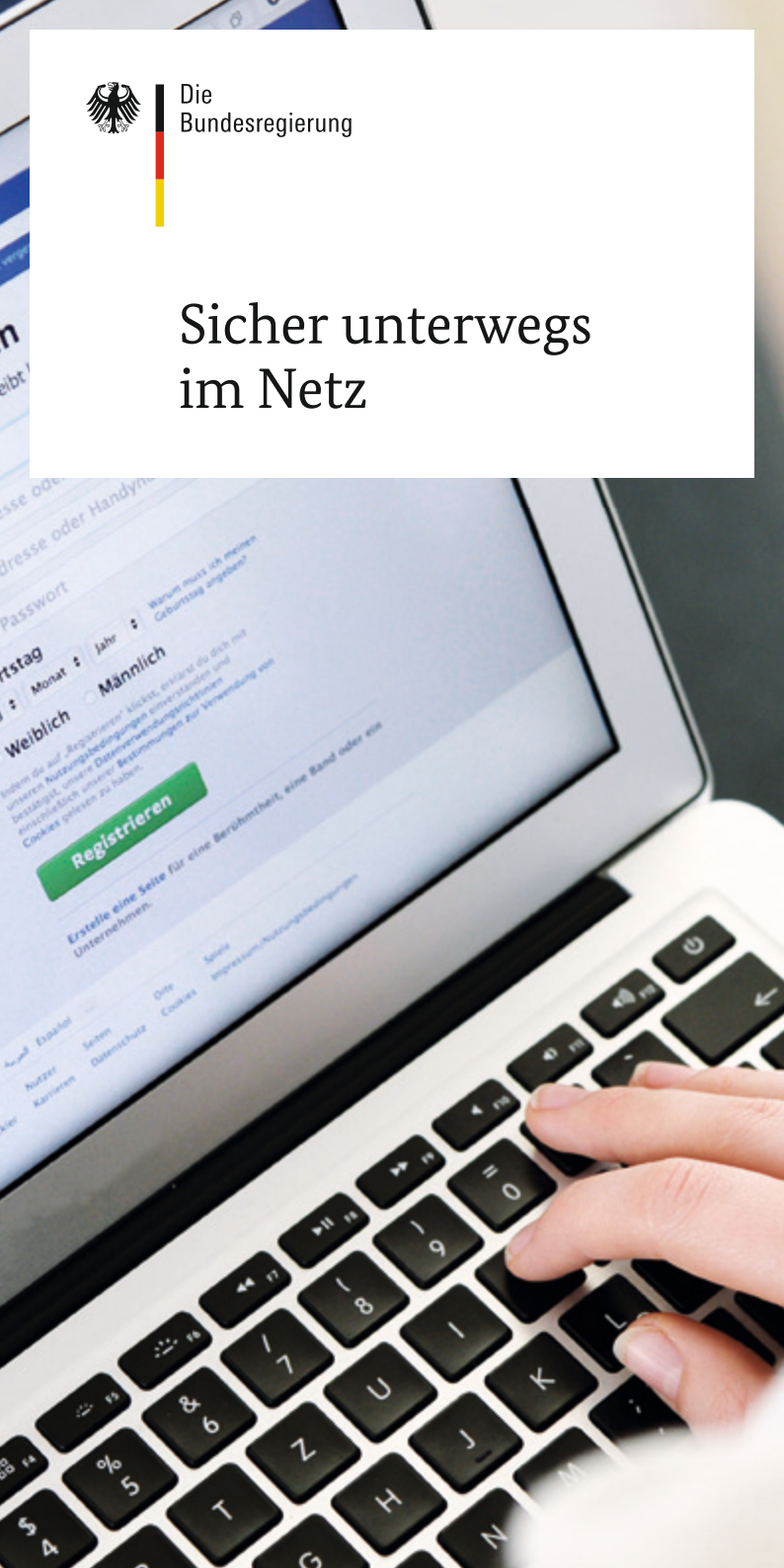
Die
Bundesregierung

Sicher unterwegs im Netz



Inhalt

1 Einleitung
2 Digitale Agenda: Verbraucherrechte im Blick
4 Mit den eigenen Daten geizen
5 Datenschutz fängt im Kopf an!
7 Datennutzung nur mit Einwilligung
8 Einfallstor „Phishing“
10 Clevere Konfiguration und sichere Software
13 Sicher mailen
15 Cookies
16 Sicher bewegen mit dem Smartphone
20 Soziale Netzwerke richtig nutzen
25 Daten endgültig löschen!
28 Weitere Informationen
Impressum

Einleitung

Jeden Tag kommunizieren Millionen von Menschen in Deutschland via Internet. Sie surfen, chatten, versenden E-Mails und Kurznachrichten.

Die meisten wissen inzwischen, dass die Informationen, die sie dabei über sich preisgeben, auch missbraucht werden können.

In dieser Broschüre finden Sie zahlreiche Tipps, wie Sie sich vor Datenmissbrauch schützen können.

Digitale Agenda: Verbraucherrechte im Blick

Verbraucher sollen sich selbstbestimmt auf den digitalen Märkten bewegen können. Hierzu ist Vertrauen in die digitale Technik und Dienste ebenso notwendig wie der kompetente Umgang damit. Deshalb steht auch der Verbraucherschutz für die Bundesregierung im Mittelpunkt der Digitalen Agenda:

- Die neue EU-Datenschutz-Grundverordnung soll ab 2018 europaweit und einheitlich vor allem dreierlei leisten: Private Daten schützen und die Voraussetzungen dafür schaffen, dass jeder seine Daten auch eigenverantwortlich schützen kann. Dabei werden die hohen deutschen Standards gewahrt bleiben.

- Marktwächter bei den Verbraucherzentralen beobachten die digitalen Produkte und Dienste, um Missstände frühzeitig zu identifizieren und Abhilfe zu schaffen.

- Wettbewerbsregeln für Internetriesen sollen verschärft, Internetplattformen mit großer Marktmacht kontrolliert und transparenter werden.

- Besonders datenschutzfreundliche Anbieter können eine Zertifizierung von einer dafür akkreditierten Stelle bekommen.

- Verbraucherschutzverbände können neuerdings Unternehmen wegen unzulässiger Erhebung, Verarbeitung und Nutzung personenbezogener Daten abmahnen und verklagen.

- Um eine stabile Rechtsgrundlage für den Datentransfer zwischen privaten Datenverarbeitern in der EU und den USA zu schaffen, arbeiten die EU und die USA derzeit an einer Nachfolgeregelung für den vom Europäischen Gerichtshof für unwirksam erklärten „Safe Harbor"-Mechanismus. Die Europäische Kommission veröffentlichte am 29. Februar 2016 den Entwurf einer solchen Regelung („Privacy Shield"), der derzeit geprüft wird.

www.digitale-agenda.de

Mit den eigenen Daten geizen

Etwas bequem im Internet nachschlagen, online einkaufen, in Sozialen Netzwerken chatten oder einfach eine E-Mail senden: Jeder Klick hinterlässt Spuren im Netz.

Einzelne Daten scheinen für sich genommen wenig wert. Interessant werden sie erst in der Kombination: Dritte können so Persönlichkeitsprofile für ganz unterschiedliche Zwecke zusammenstellen, Betrüger damit Unheil anrichten.

Viele haben sich schon einmal über unerbetene Werbung zu einem bestimmten Thema gewundert, nachdem sie zuvor dazu im Netz gesurft hatten. Es gibt Firmen, die anhand eines Facebook-Auftritts Risikobewertungen für die Kreditvergabe durchführen. Und: Bewegungsprofile, die bereits durch die mobile Nutzung von Internetdiensten anfallen, können zum Schaden des Nutzers ausgewertet werden.

Oberstes Gebot ist deshalb: Geben Sie nur so viel von sich preis wie unbedingt notwendig! Treffen Sie Schutzvorkehrungen. Und bedenken Sie: Das Netz vergisst in aller Regel nichts! Zumindest vorerst. 2018 kommt ein „Recht auf Vergessen". Dann kann man seine personenbezogenen Daten über das Privat- oder Berufsleben sowie Fotos im Netz löschen lassen.

Datenschutz fängt im Kopf an!

Dazu, dass persönliche Informationen auch privat bleiben, können Sie selbst eine ganze Menge beitragen:

- Informieren Sie sich in den Allgemeinen Geschäftsbedingungen (AGB) und den Datenschutzerklärungen, wie Online-Anbieter die erhobenen Daten verwenden. Widersprechen Sie der Datenweitergabe an Dritte, etwa wenn sie zu Werbezwecken erfolgen soll.

- Online-Fragebögen – vor allem bei Gewinnspielen und kostenlosen Diensten – nicht mit persönlichen Daten bis ins Detail ausfüllen.

- E-Mail-Adresse nicht sorglos weitergeben. Wenn Sie sich auf Webseiten ohne Kaufabsicht anmelden, sollten Sie sich dafür eine zweite, anonyme E-Mail-Adresse zulegen.

- Besser einen Spitznamen als Benutzernamen verwenden. Auch anhand eines Nicknamens können Profile erstellt werden. Deshalb für verschiedene Dienste unterschiedliche Spitznamen nutzen.

- Für verschiedene Anwendungen auch unterschiedliche Passwörter verwenden. Das Passwort sollte mindestens zwölf Zeichen lang sein, mit zufälliger Reihenfolge von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Ändern Sie es regelmäßig und speichern Sie es nicht auf dem PC!

- Regelmäßig ausloggen, sonst können andere Personen auf Ihre Internetkonten zugreifen.

- Auch am eigenen PC den Browser im Browserfenster so einstellen, dass beim Beenden der Sitzung die komplette Chronik und sonstige Daten gelöscht werden. Zum Beispiel über das Menü „Sicherheit“. Zu empfehlen sind auch sogenannte „Anti-Tracking-Tools“. Auch sie lassen sich über ein Häkchen im Browser („Do-not-track“-Funktion)

oder durch sogenannte Anti-Tracking-Add-Ons installieren. So können andere das eigene Surf-Verhalten und persönliche Daten nicht nachvollziehen.

- Um Werbung zu blockieren, können Sie auch sogenannte „Adblocker“ in der Browser-Erweiterung oder Smartphone-Anwendung entsprechend aktivieren.

- Personalisierte Online-Werbung kann man über www.youronlinechoices.eu, Stichwort: „Präferenzmanagement“, deaktivieren.

- Wer sogenannte „Spam“ E-Mails erhält, sollte sie sofort löschen. Auf keinen Fall darauf antworten und schon gar nicht etwaige Anhänge öffnen.

- In Hotspots – etwa am Flughafen oder in Fastfood-Ketten – werden Ihre Daten über einen fremden Server transportiert. Das heißt: Die lassen sich mit entsprechender Software mitlesen. Verbinden Sie sich deshalb nur mit vertrauenswürdigen Hotspots (bekannter Betreiber, Verschlüsselung bei WLAN, Zutritt nur mit Zugangsdaten). Als Profil für die hergestellte Verbindung zum Hotspot „öffentliches Netzwerk“ einstellen.

- Googeln Sie sich regelmäßig selbst und überprüfen Sie, was über Sie im Netz steht. Wenn Sie bestimmte Ergebnisse der Google-Suche zu Ihrem Namen als Verstoß gegen Ihre Persönlichkeitsrechte empfinden, können Sie Google dazu auffordern, diese Links zu entfernen.

Datennutzung nur mit Einwilligung

Grundsätzlich bedarf die Erhebung und Nutzung Ihrer Daten zu Werbezwecken Ihrer ausdrücklichen Einwilligung. Ausnahme: Wenn sie für die Vertragsabwicklung oder aus anderen berechtigten Gründen – etwa zur Kundenbetreuung – benötigt werden.

Nach dem Bundesdatenschutzgesetz haben Sie Anspruch darauf zu erfahren, was mit Ihren Daten geschieht. Auch die neue EU-Datenschutz-Grundverordnung sieht das vor. Haben Unternehmen dabei unzulässig gehandelt, können Sie verlangen, die Daten oder Fotos zu löschen, zu berichtigen oder zu sperren. Und Sie haben Anspruch auf Unterlassung und gar Schadensersatz.

Verbraucherschutzverbände können seit kurzem Unternehmen wegen unzulässiger Datenerhebung abmahnen und verklagen.

Einfallstor „Phishing“

Zusammengefügt aus dem „P“ aus „Password“ und „Fishing“ zielen Phishing-Attacken auf Geburtsdatum, Passwörter, Kontoverbindungen. Denn das sind lohnende Informationen für Betrüger. Sie versenden gefälschte E-Mails und tarnen sich dabei als seriöse, meist den Nutzern auch bekannte Firmen. In diesen E-Mails fordern sie die Empfänger auf, einem Link zu folgen. Der führt zu einer täuschend echt nachgebauten Internetseite oder einem Formular. Dort soll der Kunde vertrauliche Daten wie Passwörter, Zugangsnummern oder Kreditkartennummern eingeben. Angeblich, weil das Passwort erneuert werden muss, die Kreditkarte abläuft oder aus Sicherheitsgründen Kontoinformationen zu bestätigen sind.

Wer eine solche Nachricht bekommt, sollte nicht vorschnell reagieren und stattdessen beim vermeintlichen Absender nachfragen. Eine seriöse Bank etwa fordert ihre Kundschaft niemals per E-Mail auf, persönliche Daten wie PINs (persönliche Identifikationsnummern) und TANs (Transaktionsnummern) oder Kreditkartennummern einzugeben.

Woran erkennen Sie Phishing?
Darauf sollten Sie achten

- E-Mails im HTML-Format zeigen einen „offiziellen Link“ an. Dahinter verbirgt sich aber ein ganz anderer Link. Um ihn zu entdecken, muss man den Quelltext der HTML-Mail lesen. Dazu mit der rechten Maustaste im Nachrichtenfeld klicken und den Menüpunkt „Quelltext anzeigen“ wählen.

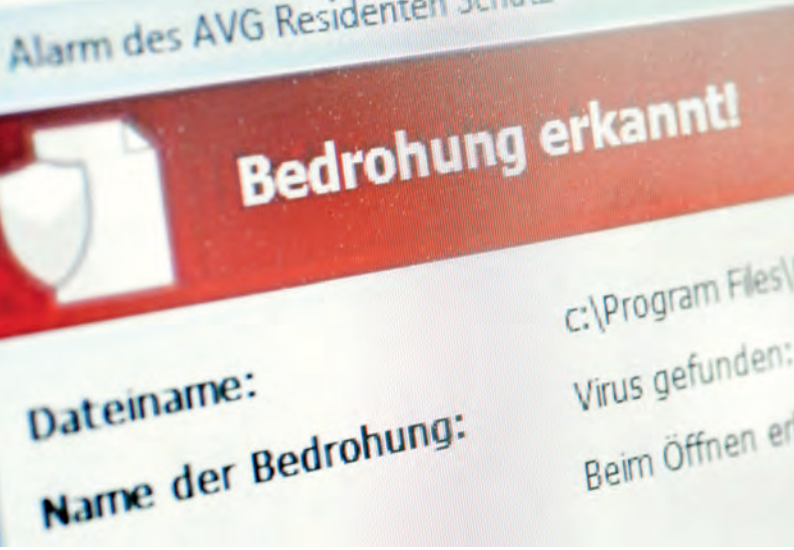
- Das Log-in dauert ungewohnt lange.

- Es werden mehr Informationen abgefragt als nötig, etwa ein zusätzlicher Nachweis oder unnötige persönliche Informationen.

- Im Browser fehlt das Schloss-Symbol: Seriöse Webseiten, die vertrauliche Informationen abfragen, verschlüsseln die Seite mit dem Netzwerkprotokoll „Secure Sockets Layer“ (SSL), angezeigt durch das Schloss-Symbol.

- Fragwürdigen Links nicht folgen, sondern Adresse eines Unternehmens oder eines Kreditinstituts direkt in den Browser eingeben oder selbst gespeicherte Lesezeichen verwenden. Beginnt die Adresse mit „https://“, ist das ein Indiz für eine geschützte Seite.

- Und: Löschen Sie fadenscheinige E-Mails mit Web-Links oder anderen Anhängen sofort! Entfernen Sie die Mail so schnell wie möglich von Ihrem Rechner.



Clevere Konfiguration und sichere Software

Schadprogramme, wie sogenannte Trojaner, verschaffen sich harmlos getarnt Zugang zum Computer und zu persönlichen Informationen. Häufig sind sie in Phishing-Mails eingebettet. Sie installieren sich dann automatisch mit einem Klick auf die Links in der E-Mail oder auf die Datei.

Oder es werden Auftragsdaten gefälscht und umgeleitet: Führt man etwa eine Überweisung durch, fängt das Schadprogramm die Auftragsdaten ab, verändert Betrag und Kontonummer des Empfängers und leitet die manipulierten Daten an die Bank weiter. Erst der Blick auf den nächsten Kontoauszug macht den Schaden sichtbar.

Die meisten Schadprogramme verfügen inzwischen über mehrere Schadfunktionen: Ein Trojanisches Pferd kann auch sogenannte Backdoor- und Spyware-Funktionen haben. Das sind heimliche Programme, die auf einen Fernzugriff abzielen. Sie können unbemerkt die Eingaben des Benutzers am Computer protokollieren.

Ausgenutzt werden hierzu Sicherheitslücken in Webbrowsern wie Internet Explorer, Mozilla Firefox oder in installierten Zusatzkomponenten (Plug-ins).

Gegen derlei Bedrohungen gibt es Softwarelösungen. Unternehmen bieten sie im Internet für Privatanwender überwiegend kostenlos an:

- Firewalls schützen vor unberechtigtem Zugriff von außen,
- Kryptografie-Programme verschlüsseln Daten,
- Digitale Signaturen ermöglichen bei elektronischen Rechtsakten, die Echtheit der Identität zu prüfen,
- Antiviren-Schutzprogramme filtern Viren aus und spüren Trojanische Pferde auf,
- Spamfilter fischen unerwünschte Werbung aus dem Posteingang.

Generell gilt für den Zugriff auf das Internet: Man sollte sich ausschließlich mit dem Benutzerkonto mit eingeschränkten Rechten, keinesfalls aber mit einem Administratorkonto anmelden.

Dringende Empfehlung: Für jede der Gefahren Sicherheitsvorkehrungen treffen, nicht nur für eine! Wichtig sind auch **regelmäßige** Updates der Software, die auf dem Rechner installiert ist, insbesondere der Antiviren-Schutzprogramme und des Betriebssystems. Denn täglich treten neue Varianten von Schädlingen auf. Die meisten Betriebssysteme und Sicherheitslösungen bieten eine automatische Aktualisierung schon als Voreinstellung an. Diese Funktion können Sie meist unter dem Menüpunkt „Optionen“ oder „Einstellungen“ aktivieren.

Wenn Sie merken oder vermuten, dass Ihr Gerät mit einem Schadprogramm infiziert wurde, sollten Sie die Arbeit am Gerät schnell aber ohne Panik beenden. Schalten Sie das Gerät aus. Holen Sie sich gegebenenfalls Expertenhilfe. Haben Sie Zugriff auf einen von Schadprogrammen freien Computer, sollten Sie versuchen, darüber alle Ihre im Internet angewendeten Passwörter zu ändern. Prüfen Sie Ihre Kontoauszüge. Was Sie bei einer Infektion Ihres Computers tun sollten, finden Sie im Detail unter www.bsi-fuer-buerger.de; Stichworte: Risiken > Schadprogramme > Infektionsbeseitigung.

Hilfestellung bietet auch das Service-Center des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Telefon 0800 2741000 von Montag bis Freitag von 8:00 bis 18:00 Uhr, kostenlos aus dem deutschen Fest- und Mobilfunknetz.

Oder schicken Sie eine E-Mail an:
mail@bsi-fuer-buerger.de

Sicher Mailen

Bei Mails sollte man sich sicher sein können, dass die Nachricht tatsächlich vom angegebenen Absender stammt. Unbefugte sollten zudem eine E-Mail nicht mitlesen und nicht verändern können.

Wer De-Mail nutzt, um eine Nachricht zu versenden, kann sicher sein, dass der Versand verschlüsselt und signiert ist. Die Mail erhält nämlich einen virtuellen Umschlag wie ein Brief. Unbefugte können sie nicht einsehen oder manipulieren. Außerdem hat sie einen eindeutigen Absender, denn für De-Mail müssen sich alle Kommunikationspartner einmal bei ihrem De-Mail-Anbieter identifizieren lassen.

Mit De-Mail lassen sich sowohl die Identität der Kommunikationspartner als auch der Versand und der Eingang von De-Mails zweifelsfrei nachweisen.

Neben der bei De-Mail bereits standardmäßig durchgeführten Transportverschlüsselung können Sie besonders sensible Nachrichten zusätzlich auch noch Ende-zu-Ende, d.h. lückenlos zwischen Absender und Empfänger, verschlüsseln. Hierfür benötigen Sie ebenso wie der Empfänger Ihrer

Nachricht entsprechende Verschlüsselungssoftware, die auf den eigenen Rechnern installiert sein muss.

Mit dieser Software verschlüsseln Sie Ihre De-Mail persönlich vor dem Versand. Entschlüsselt wird sie erst durch den Empfänger auf dessen Rechner. Die sonst übliche automatische Prüfung auf Schadprogramme durch den De-Mail-Anbieter kann bei Ende-zu Ende-Verschlüsselung technisch nicht erfolgen. Hierfür muss der Empfänger durch sein eigenes Virenschutzprogramm Sorge tragen.

Mittlerweile bieten verschiedene Dienste De-Mail auch kostenlos an. Unabhängig davon, welchen De-Mail-Anbieter Sie wählen: Das De-Mail-Gesetz gewährleistet ein einheitliches und geprüftes Sicherheitsniveau. Ebenso können Sie alle De-Mail-Nutzer bei allen anderen De-Mail-Anbietern erreichen.

Nähere Informationen zu De-Mail finden Sie auf der Webseite des Beauftragten der Bundesregierung für Informationstechnik **www.de-mail.de**

Weitere Empfehlungen zur Verschlüsselung Ihrer Nachricht im Netz finden Sie auf der Internetseite **www.bsi-fuer-buerger.de**

Rat zu Browser-Einstellungen und E-Mail-Anbietern sowie Verschlüsselungen gibt das (vom Bundesverbraucherschutzministerium geförderte) Angebot **www.verbraucher-sicher-online.de**

Cookies

Cookies sind kleine Dateien, die sich beim Besuch einer Internetseite auf dem PC ablegen. Sie helfen, den Rechner beziehungsweise Nutzer „wiederzuerkennen“: So findet man schnell eine vertraute Internet-Umgebung wieder und muss einmal eingegebene Angaben nicht wiederholen. Damit kann man etwa auf den Seiten eines Online-Shops den Warenkorb füllen und sich anschließend weiterbewegen – ohne die getroffene Vorauswahl zu verlieren. Diese sogenannten „Session Cookies“ sind unproblematisch: In der Regel verschwinden sie nach dem Schließen des Browsers.

Anders die sogenannten persistenten Cookies: Sie nisten sich im PC ein und spähen gezielt Daten aus. Sperren Sie deshalb persistente Cookies über die Browsereinstellung. Einen Wegweiser hierzu finden Sie etwa unter www.meine-cookies.org .

Sicher bewegen mit dem Smartphone

Besonders bei Mobiltelefonen sind die Sicherheitsrisiken nicht zu unterschätzen. Hier gilt ebenso wie beim häuslichen PC: Geizen Sie mit Ihren privaten Daten.

Viren, die sich insbesondere bei dem Betriebssystem Android über den Download von Klingeltönen, Logos, Bildschirmschonern, Musikstücken und Handyspielen ausbreiten, können erhebliche Kosten verursachen.

Sicherheits-Apps helfen; meist sind sie vom Hersteller bereits eingebaut. Damit kann man sein Smartphone außerdem wiederfinden oder bei Diebstahl sperren lassen. Außerdem lohnt es sich auch hier, beim Browser regelmäßig Sicherheits-Updates durchzuführen, um Schadprogramme abzuwehren.

Für Smartphones von Kindern gibt es spezielle Suchmaschinen. Gerade bei Kindern gilt zudem: Nicht alles was im Netz steht, gehört auf deren Smartphone.

Sicherer Umgang mit dem Smartphone
für junge Menschen:
www.sicher-im-netz.de
www.fragfinn.de
www.schau-hin.info

Die wichtigsten Sicherheitshinweise für mobiles Telefonieren und mobiles Internet:

- Keine unbekannten Rufnummern zurückrufen. Bei Bedarf unerwünschte Rufnummern zu teuren „Mehrwertdiensten" von Ihrem Netzbetreiber sperren lassen.

- Keine Gespräche mit vertraulichem Inhalt übers Handy: Das Telefonieren über GSM (Standard zur mobilen Sprach- und Datenübertragung) ist nicht abhörsicher.

- Die Tastatursperre sowie den Gerätesperrcode nutzen und stets die SIM / USIM-PIN aktivieren. Zusätzlich, wenn möglich, eine Display-Sperre aktivieren.

- Deaktivieren Sie drahtlose Schnittstellen (zum Beispiel WLAN und Bluetooth), wenn Sie diese nicht nutzen. Koppeln Sie externe Geräte mit Ihrem Mobilfunkgerät (etwa über Bluetooth) nur in gesicherter Umgebung. Und vergessen Sie nicht, die Verbindung wieder zu deaktivieren.

- Apps nur aus vertrauenswürdigen Quellen beziehen. Falls der App-Anbieter unbekannt ist, informieren Sie sich vor der Installation im Internet. Überprüfen Sie auch, welche genauen Zugriffsrechte eine App vorsieht. Denn: Eine Spiele-App muss nicht Ihren Standort erfassen, eine Taschenlampen-Funktion nicht Ihre Verbindungsdaten.

- Bei Verlust Ihres mobilen Gerätes die SIM-Karte unverzüglich sperren lassen. Hat Ihr Gerät eine Remote-Wipe-Funktion, kann man das Gerät aus der Ferne zurücksetzen und sperren.

- Betreiber von Funknetzwerken und manche App-Anbieter können den Aufenthaltsort von Mobilfunkgeräten – und damit ihrer Besitzer – jederzeit ermitteln. Seien Sie deshalb mit der Weitergabe Ihrer Positionsdaten sehr zurückhaltend. Meiden Sie Lokalisierungsdienste und speichern Sie keine Ortsdaten in Fotos, die Sie ins Internet laden. Schalten Sie die GPS- und die WLAN-Funktion nur ein, solange Sie sie wirklich brauchen.

- Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht und wenn, dann über eine gesicherte Verbindung (https). Online-Banking und andere sensible Anwendungen sollten Sie in offenen Netzwerken vermeiden. Achten Sie darauf, öffentliches WLAN nur mit dem Verschlüsselungsstandard WPA 2 zu nutzen.

- Führen Sie regelmäßig Sicherheits-Updates durch. Verwenden Sie hierfür Firmenware Ihres Gerätes, die etwa auf der jeweiligen Internetseite zu finden ist.

- Halten Sie mobile Geräte stets unter Aufsicht.

Weitere Informationen rund um die Sicherheit Ihres Handys oder Smartphones finden Sie unter: **www.bsi-fuer-buerger.de**; siehe unter „Empfehlungen“: „Basisschutz für Computer und Smartphone“.

Oder bei der vom Bundesministerium der Justiz und für Verbraucherschutz geförderten Webseite: **www.mobilsicher.de**

Zum Thema Smartphones fernlöschen, orten und sperren: **www.tecchannel.de**

Soziale Netzwerke richtig nutzen

So reizvoll der Austausch auf Sozialen Netzwerken ist, so gefährlich kann er auch sein. Soziale Netzwerke zu nutzen, ist nur auf den ersten Blick kostenlos. Man bezahlt zwar nicht mit Geld, aber mit seinen Daten – Daten, die die Netzbetreiber teuer an Dritte verkaufen.

Darauf beruht das Geschäftsmodell der Netzwerkbetreiber. Sie sind keine Wohlfahrtsorganisationen. Insofern ist das Wort „sozial“ im Grunde irreführend.

Fair mit Mindeststandards

Die Bundesregierung hat sich in den Verhandlungen zur Datenschutz-Grundverordnung dafür eingesetzt, dass auch die Betreiber von Sozialen Netzwerken vollständig, verständlich und gut sichtbar über ihre Nutzungsbedingungen informieren. Für den Nutzer muss klar sein, auf welche personenbezogenen Daten die Betreiber zugreifen und wie sie sie auswerten. Nutzer müssen hierin wirksam eingewilligt haben – und zwar vor der ersten Anwendung.

Auswertung persönlicher Daten verhindern

Wer nicht zum gläsernen Menschen werden will, kann beim Nutzen Sozialer Netzwerke verhindern, dass seine persönlichen Informationen ausgewertet werden.

Die persönlichen Aussagen in den Sozialen Netzwerken und beim „Instant Messaging“ zu Vorlieben und Denkweisen geben eine perfekte Grundlage, um Nutzerprofile zu erstellen. Nutzer sollten deswegen gut überlegen, wie offen sie ihre Seite überhaupt einrichten wollen.

- Vorsicht! Sich im Internet über Live-Stream-Foren zu präsentieren, offenbart alles, was die Kamera einfängt.

- Es ist stets ratsam, sich in offenen Foren eher mit persönlichen Aussagen zurückzuhalten – sei es im Text oder im Bild. Datenschutzrechtlich Sensibles hat in Sozialen Netzwerken nichts verloren! Eine unüberlegte Aussage oder nachteilige Äußerung über Dritte kann selbst nach Jahren zu einem ernsten Problem werden.

- Wer öffentlich preisgibt, welche Musik, welche Urlaubsziele, welche Restaurants er mag, muss immer damit rechnen, dass Fremde ihre eigenen Schlüsse daraus ziehen. Man zeichnet mehr oder weniger unbewusst ein Bild von sich, das andere Menschen voreingenommen machen kann.

- Vorsicht ist auch geboten beim Trend, immer mehr Geräte mit dem Internet zu verbinden. Wenn ein Nutzer es hierbei unterlässt, zumindest ein schützendes Passwort und regelmäßige Updates vorzusehen, können Unbefugte auf die Daten zugreifen und Schaden anrichten. Ungesicherte Webcams etwa können so im Internet Einblicke in Privaträume freigeben.

- Unter den vielen Anbietern von Online-Diensten gilt es, denjenigen zu wählen, der ein hohes Datenschutzniveau sichert. Im Zweifel besser auf einen Online-Dienst verzichten.

- Man sollte sich darüber im Klaren sein, dass Online-Dienste indirekt auf die eigenen Daten zugreifen können. Dabei muss man die Dienste nicht einmal selbst in Anspruch nehmen. Es reicht, wenn das ein anderer Nutzer tut, mit dem man über ein Netzwerk in Verbindung steht.

- Oft bieten Online-Shops an, sich über ein Soziales Netzwerk anzumelden. Das ist zwar bequem, aber auch gefährlich, denn so erfährt das Netzwerk mehr über Sie, als Ihnen wahrscheinlich lieb ist. Deshalb sollten Sie sich bei jedem Online-Shop individuell anmelden – möglichst mit verschiedenen Passwörtern.

Werbung filtern

Erscheint im Sozialen Netzwerk eine Anzeige auf dem Bildschirm, kann man sie mit einem Klick entfernen: Mit der Maus über die Anzeige gehen, das in einer Ecke auftauchende Kreuz anklicken und die Werbung generell oder auch Werbung von einem Anbieter verbannen.

Texte und Fotos löschen

Wer einen ins Soziale Netz eingestellten Text oder ein Foto löschen will, kann sich direkt an den Dienste-Anbieter, den Betreiber eines Forums oder auch an die Freunde, auf deren Seite die betreffende Datei zu sehen ist, wenden. Dazu ist es nötig, den Text oder das Foto zu identifizieren. Meistens funktioniert das auch. Gegebenenfalls noch einmal nachhaken. Eine Löschung bedeutet: Der Text bzw. das Foto ist nicht mehr sichtbar. Gelöscht wird jedoch nur die Speicheradresse, die Datei selbst nicht. Damit kann man auch Agenturen beauftragen. Allerdings kostet das Geld und ist nicht unbedingt erfolgversprechender.

Gesichtserkennung in Sozialen Netzwerken

Gesichtserkennung in Sozialen Netzwerken ist nicht unproblematisch, da sie in hohem Maße die schutzwürdigen Interessen Betroffener berührt. Um Gesichtserkennung und Profilbildung durch „Taggen“ (das heißt Markieren oder Etikettieren) zu verhindern, empfiehlt es sich, mit Angaben zu Person, Ort und Datum zurückhaltend zu sein. Im Übrigen ähnlich wie beim Löschen eines Fotos vorgehen.

Fremdnutzung von eigenen Fotos und „Gefällt mir“-Angaben verhindern

Die Verwendung von Fotos und „Gefällt mir“-Angaben für Werbezwecke durch Anbieter von Sozialen Netzwerken können Nutzer abstellen. Dazu unter Einstellungen Stichwort: „Werbeanzeigen“ entsprechend anklicken und speichern.

Das BSI gibt Anleitungen für die beliebtesten Sozialen Netzwerke unter **www.bsi-fuer-buerger.de**

Eine Alternative für Kinder bietet das vom Bundesjugendministerium geförderte Portal **www.blinde-kuh.de/sicherheit/** sowie **www.schau-hin.info**

Anleitung gibt auch **www.chatten-ohne-risiko.net**

Daten endgültig löschen!

Einfaches Anklicken der Löschtaste verlagert Daten nur in den Papierkorb. Auch das Leeren des Papierkorbs löscht nur die Verweise, wo die Dateien gespeichert sind und gibt den Speicherplatz zum erneuten Überschreiben frei. Solange auf demselben Speicherort nichts erneut gespeichert wird, bleibt das zuvor Gespeicherte weiterhin lesbar. Um das zu verhindern, muss also der Speicherort komplett überschrieben werden. Auch das Neuformatieren oder auch Zurücksetzen des Speichers löscht nur das Inhaltsverzeichnis, die Daten jedoch nicht.

Deswegen: Sensible Daten unwiederbringlich löschen! Im Zweifel das Gerät / die Festplatte physisch zerstören. Achtung: Alle weiter benötigten Daten zuvor anderweitig sichern.

Daten auf dem PC löschen

- Intakte Festplatten mit spezieller Software bis zu siebenfach komplett überschreiben lassen! Das BSI empfiehlt Programme, die von einem bootfähigen Medium, zum Beispiel CD oder USB-Stick, zu starten sind.

- Moderne Festplatten zusätzlich mit dem „Secure Erase“-Befehl zum Löschen auffordern!

- Für Windows-betriebene PCs ist das Löschen etwa mit den kostenlosen Programmen „Disk Wipe“ und „Eraser“ möglich. Auch Daten auf Speicherkarten oder USB-Sticks lassen sich damit zuverlässig löschen.

Daten auf dem Smartphone und Tablet löschen

- Für iPhones eignen sich die Secure Wipe iPhone-App und die iErase iPhone-App. Beide löschen und überschreiben Speicher mehrfach. Die sicherste Methode, um Daten endgültig zu löschen.

- Für mobile Geräte mit Android-Betriebssystem empfiehlt es sich, seine Daten zunächst zu verschlüsseln und dann erst das Gerät zurückzusetzen. Wiederherstellbare Daten sind damit ohne Entschlüsselung nicht lesbar. Um die Wiederherstellung zu erschweren, den Speicher überschreiben, am besten mit großen Mengen an unsinnigen Daten. Sodann das Gerät erneut zurücksetzen. Um ganz sicher zu gehen, diese Schritte mehrfach wiederholen.

- Die SIM-Karte entfernen und – falls sie nicht weiterverwendet werden soll – mechanisch zerstören!

Wie das Löschen bei Smartphones funktioniert, ist für viele Modelle auch auf dem vom Bundesministerium der Justiz und für Verbraucherschutz geförderten Portal **www.mobilsicher.de** beschrieben.

Ihre Notizen

Weitere Informationen finden Sie unter folgenden Links:

www.bundesregierung.de
Stichwort: „Tipps für Verbraucher“

www.verbraucher-sicher-online.de
www.schau-hin.info
www.mobilsicher.de
www.bsi-fuer-buerger.de
www.klicksafe.de
www.blinde-kuh.de/sicherheit/
www.bfdi.bund.de
www.bundesnetzagentur.de
www.cio.bund.de

Anti-Botnet-Beratungszentrum:
www.botfrei.de

Informationen zum Cloud-Computing:
www.cloud.irights.info

Bestellmöglichkeiten für Publikationen

Internet: www.bundesregierung.de (Stichwort Infomaterial)
E-Mail: publikationen@bundesregierung.de
Telefon: 030 18 272 272 1
Fax: 030 18 10 272 272 1

Impressum

Herausgeber
Presse- und Informationsamt
der Bundesregierung
11044 Berlin

Stand
März 2016

Druck
Silber Druck oHG
34266 Niestetal

Gestaltung
adlerschmidt
kommunikationsdesign gmbh

Bildnachweis
Bundesregierung / Stutterheim: Titel, Seite 17
CE / Reporters: Seite 2
ddp images / Wolfilser: Seite 4
imago / Westend61: Seite 22, 23
Marco Laux: Seite 10
photothek.net / Grabowsky: Seite 20
picture-alliance / dpa / Marks: Seite 25
picture-alliance / dpa / Spata: Seite 1
picture-alliance / dpa / Warnecke: Seite 15
Reuters / Langsdon: Seite 8
ullstein bild – imageBROKER / Tack: Seite 7
picture-alliance / cromeorange: Seite 13

Ausführliche Informationen zu allen Themen unter
www.bundesregierung.de

Die Bundesregierung auf Facebook
www.facebook.com/Bundesregierung

Folgen Sie dem Regierungssprecher auf Twitter
www.twitter.com/regsprecher

Die Regierungs-App kostenlos zum Herunterladen

Google Play Store (Android)

App Store (iOS)