Die Welt des mobilen Internets

MODUL 05

verbraucherzentrale

SMART SURFER

Fit im digitalen Alltag

Lernhilfe für aktive Onliner*innen

20 JAHRE Bayerisches Verbraucherschutzministerium

Verbraucherbildung Bayern

Bayerisches Staatsministerium für Umwelt und Verbraucherschutz

BLM

VerbraucherService Bayern im KDFB e.V.

verbraucherzentrale Bayern

Gebündelte Kompetenz rund um die Themen: Datensicherheit, Verbraucherschutz, Digitalisierung, Unterhaltung und digitale Ethik

Seit 2011 bietet das medienpädagogische Ausbildungskonzept „Silver Surfer – Sicher online im Alter“ eine digitale Grundbildung für aktive Onliner*innen. 2020 wurde das Konzept neu aufgelegt. Dafür sind einzelne Themenbereiche erheblich erweitert und einige neue hinzugefügt worden. Zusätzlich wurde auch der Titel der Lernhilfe angepasst: „Smart Surfer – Fit im digitalen Alltag“.

Die Lernhilfe „Smart Surfer – Fit im digitalen Alltag“ wurde gemeinsam von Mitarbeiter*innen der Verbraucherzentrale Rheinland-Pfalz e.V., der Medienanstalt Rheinland-Pfalz, des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz und der Stiftung MedienKompetenz Forum Südwest sowie der Clearingstelle Medienkompetenz der Deutschen Bischofskonferenz an der Katholischen Hochschule Mainz erstellt.

verbraucherzentrale Rheinland-Pfalz

medienanstalt rlp LMK

Der Landesbeauftragte für den DATENSCHUTZ und die INFORMATIONSFREIHEIT Rheinland-Pfalz

MKFS MEDIEN KOMPETENZ FORUM SÜDWEST STIFTUNG

Katholische Hochschule Mainz – Clearingstelle Medienkompetenz

Herausgeber der Lernhilfe „Smart Surfer“ in Bayern ist das Bayerische Staatsministerium für Umwelt und Verbraucherschutz in Kooperation mit der Bayerischen Landeszentrale für neue Medien, der Verbraucherzentrale Bayern e.V. und dem VerbraucherService Bayern im KDFB e.V.

Das Projekt wird gefördert durch:

RheinlandPfalz – Ministerium für Familie, Frauen, Jugend, Integration und Verbraucherschutz

Bayerisches Staatsministerium für Umwelt und Verbraucherschutz

Baden-Württemberg – Ministerium für ländlichen Raum und Verbraucherschutz

Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen

LAND BRANDENBURG – Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz

LFK: Die Medienanstalt für Baden-Württemberg

Wie Sie diese Lernhilfe benutzen

Die Lernhilfe „Smart Surfer – Fit im digitalen Alltag“ bietet viele Informationen rund um das Thema Internet. Sie soll gleichzeitig als Nachschlagewerk dienen.

Seit dem Jahr 2020 wird die Lernhilfe in digitaler Form angeboten. Sie können die PDF-Dateien zu den einzelnen Modulen über Ihren PC/Laptop sowie Ihr Tablet nutzen.

In einer PDF-Datei können Sie gezielt nach Stichwörtern suchen. Mit einem Klick auf eine Internetadresse gelangen Sie direkt auf die jeweilige Website, vorausgesetzt, Sie lesen dieses PDF über ein internetfähiges Gerät. Natürlich können Sie sich diese PDF-Datei ausdrucken. Weitere Informationen zum Thema „Wie nutze ich ein PDF?“ finden Sie unter:
www.silver-tipps.de/was-bedeutet-eigentlich-pdf

Die Lernhilfe „Smart Surfer – Fit im digitalen Alltag“ besteht aus 9 Modulen:

- Modul 1: Was ist das Internet?
- Modul 2: Wie man das Internet nutzt
- Modul 3: Unterhaltungsmöglichkeiten im Internet
- Modul 4: Wie man Risiken im Netz vermeidet
- **Modul 5: Die Welt des mobilen Internets**
- Modul 6: Datenschutz im Internet
- Modul 7: Kommunikation im Netz
- Modul 8: Soziale Medien im Netz
- Modul 9: Ein Blick in die Zukunft des Internets

Alle PDF-Dateien zum Download finden Sie unter: *www.smartsurfer.bayern.de*

Alle Informationen der Lernhilfe haben wir nach bestem Wissen und Gewissen geprüft. Wir freuen uns stets über kritische Anmerkungen, die helfen, diese Lernhilfe noch besser zu machen. Sie möchten Kritik äußern? Dann zögern Sie nicht, uns zu kontaktieren (per E-Mail an: verbraucherbildung@stmuv.bayern.de).

In der Lernhilfe finden sich unterschiedliche Symbole:

Weiterführendes: Das entsprechende Thema wird an einer anderen Stelle der Lernhilfe erneut aufgegriffen und umfangreicher dargestellt.

Silver Tipps: Auf der Onlineplattform *www.silver-tipps.de* finden sich viele weiterführende Informationen rund um das Thema Sicherheit im Internet.

Link: Über die eingefügten Links sind weiterführende Informationen und andere Internetquellen zum Thema zu finden.

Fakt: Interessante Fakten werden im Text gesondert hervorgehoben.

Paragraf: Wer sich im rechtlichen Bereich weiterführend informieren will, findet an dieser Stelle die genauen Gesetzesbezeichnungen.

Begriffe, die mit einem Pfeil (➔) markiert sind, werden im Anschluss an den Text in einem Glossar näher erläutert.

Gender-Hinweis: Gendergerechte Sprache ist ein wichtiges Thema. Deshalb wurde in der Lernhilfe mit der Gender-Schreibweise des Ministeriums für Familie, Frauen, Jugend, Integration und Verbraucherschutz Rheinland-Pfalz gearbeitet und das Gender-Sternchen (*) genutzt, um alle Leser*innen gleichermaßen anzusprechen.

Die Welt des mobilen Internets

MODUL 05

Um in die Welt des mobilen → Internets einzutauchen, steht Nutzer*innen eine Vielzahl an internetfähigen mobilen Geräten zur Auswahl. → Apps erweitern die Funktionen eines → Smartphones und Daten liegen heute in → Clouds. Diese neuen Möglichkeiten bringen neben Annehmlichkeiten auch Herausforderungen für den Daten- und Verbraucherschutz mit sich. Denn auch Mobile Payment, also das Bezahlen im Internet, gewinnt an Bedeutung. Immer wichtiger wird außerdem das Thema Datenschutz und Datensicherung. Schließlich liegen uns viele private Daten wie Verträge und Dokumente, aber auch Bilder und Videos heutzutage → digital vor.

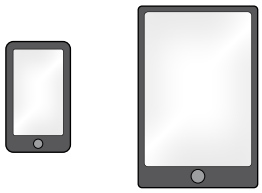
Welche Endgeräte werden auf dem Markt angeboten und was leisten diese? Welchen Stellenwert haben Benutzerkonten heute und wie organisieren Sie Ihre Datensicherung am besten? Das und mehr erfahren Sie im Modul 5. Dr. Marc Jan Eumann, Direktor der Medienanstalt Rheinland-Pfalz, erläutert zudem im Interview, wie wichtig das mobile Internet auch für die Medienvielfalt in Deutschland ist.

5.1 Die Palette smarter Endgeräte

Heutzutage werden nicht nur Uhren und Brillen „smart“, sondern auch das Internet. Smart-Technologien sollen das Leben der Menschen einfacher machen – das birgt Chancen, aber auch so manches Risiko. Verbraucher*innen können gläsern werden, wenn Daten über die Gerätenutzung unkontrolliert gesammelt und ausgewertet werden. Die massenhafte Erfassung solcher Informationen in anonymisierter Form kann die Fachleute in Wissenschaft und Forschung aber auch weiterbringen.

Smarte Geräte im Überblick

Smartphones und → Tablets gehören heute zum Alltag vieler Menschen. Die Palette der angebotenen Geräte ist groß, und die Unterschiede sind auf den ersten Blick nicht immer ersichtlich. Wenn man sich heute mit mobilen Endgeräten befasst, spricht man aber längst nicht mehr nur von Smartphones und Tablets. Ob Brille oder Uhr – viele dieser Alltagsgegenstände werden allmählich ebenfalls smart. „Smart“ bedeutet in diesem Zusammenhang „intelligent“ oder „schlau“. Schlauer als die alten Geräte sind sie aufgrund ihrer ununterbrochenen Verbindung zum Internet, ihrer starken Rechenleistung und den immer häufiger verbauten Sensoren, zum Beispiel zum Messen des Pulsschlags.



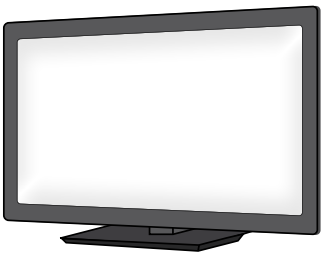
Smartphone & Tablet

Das klassische Smartphone hat ein Display mit einer Diagonalen von bis zu 4,5 Zoll. Die sogenannten Smartlets oder Phablets sind – wie die Namen andeuten – Mischformen aus Smartphones und Tablets und haben einen größeren Bildschirm als ein Smartphone, sind aber kleiner als Tablets. Die Bildschirmdiagonale beträgt zwischen 4,5 und 7 Zoll. Ist das Display zwischen 7 und 10,1 Zoll groß, spricht man von einem Tablet.

Tipp

Anleitungen, wie man beispielsweise ein Smartphone einrichtet, finden Sie unter *www.silver-tipps.de*. Aber auch andere Initiativen wie der Verein Wege aus der Einsamkeit e. V. aus Hamburg bieten Hilfestellungen im Umgang mit der Technik. Auf dem YouTube-Kanal des Vereins finden Sie unter anderem Videoanleitungen für die Installation verschiedener Apps: *https://s.rlp.de/ZmTJn*

Smart-TV



Wenn man sich heute einen neuen Fernseher anschafft, holt man sich wahrscheinlich ein sogenanntes Smart-TV ins Haus. „Smart-TV“, manchmal auch „Hybrid-TV“ oder „HbbTV“ genannt, ist die Bezeichnung für Fernsehgeräte, die internetfähig sind. Man kann hier zahlreiche Zusatzangebote nutzen, zum Beispiel die Mediatheken der Fernsehsender, und auch im Internet surfen. Außerdem kann man mit dem smarten Fernsehgerät auf Fotos zugreifen, die auf einem PC gespeichert sind. Auch Videotelefonie ist am Fernseher möglich.

Modul 3.2: Mediatheken und TV-Livestreams

Wearables

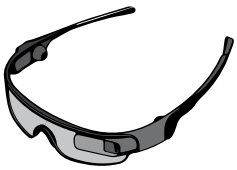
Unter dem Begriff „Wearables“ versteht man Geräte, die am Körper getragen werden können (vom englischen Verb „to wear“, zu Deutsch „tragen“). Dazu gehören Smartwatches, Fitness-Tracker und auch smarte Brillen.

Smartwatch

Smartwatches sind smarte Armbanduhren. Diese Uhren haben ein kleines Display von meist rund 1,5 Zoll. Sie verbinden sich per Bluetooth mit einem Smartphone, und über entsprechende Apps kann man sich an der Uhr dann zum Beispiel den Terminplaner, E-Mails oder auch Statusmeldungen aus sozialen Netzwerken anzeigen lassen. Mit einigen Modellen kann man auch direkt telefonieren, Fotos schießen oder den Puls messen.

Smartband/Fitness-Tracker

Als „Smartbands“ werden Fitnessarmbänder bezeichnet, die mit elektronischen Sensoren ausgestattet sind. Sie gehören zur Gruppe der Fitness-Tracker (vom englischen Verb „to track“, zu Deutsch „verfolgen“). Die Geräte sind in der Lage, Körperfunktionen und Aktivitäten zu messen, zum Beispiel die Herzfrequenz, Schritte oder Beschleunigung. Mithilfe dieser Tracker kann also auch die eigene Gesundheit „überwacht“ werden. Kabellos können die Daten an einen PC oder ein Smartphone übertragen werden, wo spezielle Programme sie auswerten. Auf diese Weise kann man eine Übersicht über die täglichen Aktivitäten und den Kalorienverbrauch erhalten. Die Körpersensoren finden vermehrt Einzug in Smartphones und Smartwatches. Das Tragen eines separaten Fitnessarmbands kann damit überflüssig werden.

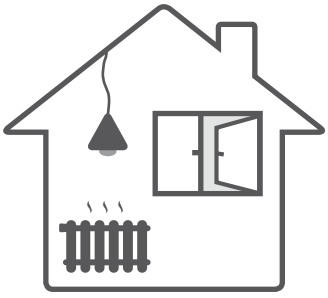


Smart-Brille

Mithilfe dieser Datenbrillen wird ein Bild ins Sichtfeld der Träger*innen projiziert. So kann man Daten lesen, Nachrichten empfangen oder sich den Weg weisen lassen. Über eine eingebaute Kamera kann die Brille auch die Umgebung wahrnehmen und Informationen zum gerade Gesehenen, etwa einer Sehenswürdigkeit, geben.

Smart-Kamera

Mittlerweile gibt es auch bereits smarte Kameras, die genau wie ein Smartphone und alle anderen smarten Geräte über ein Betriebssystem und eine Internetverbindung verfügen. So ist es möglich, Fotos zum Beispiel direkt zu verschicken oder in einem sozialen Netzwerk zu veröffentlichen.



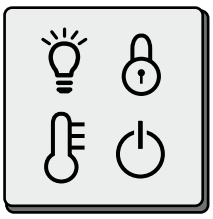
Smart Home

Das „Smart Home“, zu Deutsch „intelligentes Zuhause“, ist heute in vielen Bereichen zu finden. Dazu gehört die Vernetzung beispielsweise von Schließanlagen, Lampen, Jalousien, Heizungs- oder Alarmanlagen. Über entsprechende Apps können dann via Smartphone oder Tablet die Jalousien geöffnet oder geschlossen, die Lampen ein- oder ausgeschaltet und die Heizung reguliert werden. Auch sicherheitstechnisch

ist diese Idee nicht uninteressant. So gibt es Lösungen in Kombination mit Bewegungsmeldern und Webcams. Wenn das Smartphone sich meldet, hat jemand das Grundstück betreten und den Bewegungsmelder aktiviert. Eine Textnachricht informiert darüber, ob sich vermeintliche Einbrecher*innen schon im Haus oder noch auf dem Grundstück befinden. Per Webcam kann man nun via Smartphone verfolgen, was diese so anstellen.

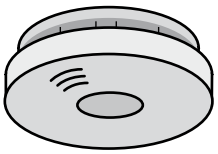
Für die Nutzung von Smart Home sind verschiedene Komponenten notwendig:

Smart-Home-Zentrale



Die Smart-Home-Zentrale bildet das Herzstück des vernetzten Hauses. Von ihr geht die zentrale Steuerung der heimischen Geräte aus. Zudem stellt sie über den Internetrouter die Verbindung nach außen, also zum Smartphone her. Es gibt auch Router, die die Funktion einer Smart-Home-Zentrale übernehmen.

Smart-Home-Sensoren

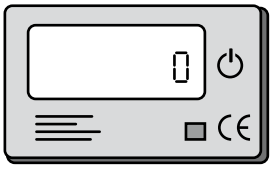


Unter den Smart-Home-Sensoren versteht man Geräte, die gemessene „Zustände“ im Haus an die Zentrale übermitteln. Typische Sensoren sind Bewegungsmelder, Türkontakte, Temperatursensoren, Rauchmelder und Wasserstandssensoren.

Smart-Home-Aktoren

Aktoren sind die Geräte, die gesteuert werden können. Beispiele sind hier Schalter, Heizungsventile, Rollladenmotoren, Türschlösser oder smarte LED-Lampen. Aktoren werden entweder direkt durch die Benutzer*innen über die App am Smartphone gesteuert oder nach einer vorgegebenen Regel durch die Smart-Home-Zentrale. Ein Beispiel wäre hier: Wenn der Bewegungsmelder (Sensor) eine Bewegung feststellt, soll sich die smarte LED-Lampe (Aktor) einschalten.

Smart Meter



Unter „Smart Meter“ sind „intelligente Verbrauchsmesser“ zu verstehen. Die Geräte ersetzen in Wohnungen oder Häusern die herkömmlichen Zähler für Strom, Gas, Wasser oder Fernwärme. Damit wird das Zuhause ebenfalls zu einem Smart Home. Neu an diesen Geräten ist

ihre Fähigkeit, die gemessenen Daten elektronisch an das jeweilige Versorgungsunternehmen zu übermitteln. Derzeit kommen die neuen Messgeräte vor allem bei der Erfassung des Stromverbrauchs zum Einsatz. Die Smart Meter machen nicht nur die jährliche Ablesung überflüssig, sie sollen den Anbietern auch erlauben, den Verbrauch genauer zu überwachen und die Stromerzeugung damit bedarfsgerechter und effizienter zu machen. Wer von seinem Energieversorger einen digitalen Stromzähler (auch „moderne Messeinrichtung“ genannt) eingebaut bekommen hat, besitzt noch keinen Smart Meter. Nur wenn der digitale Stromzähler über ein entsprechendes „Smart Home Gateway“ mit dem Internet verbunden ist, handelt es sich um einen Smart Meter.

5.2 Identifizierung im Internet – ohne Benutzerkontos geht es nicht

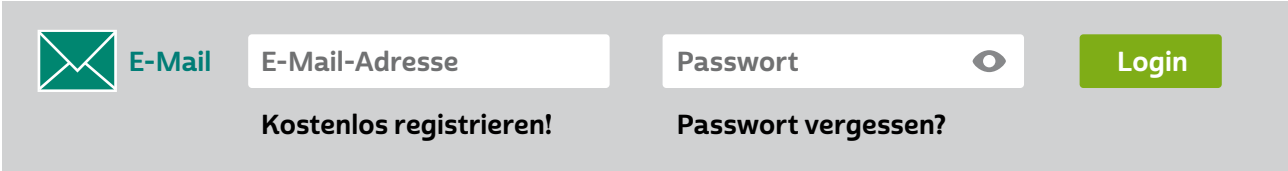
Um mobile Geräte und Onlinedienste nutzen zu können, braucht man in der Regel ein Benutzerkonto. Wer ein mobiles Gerät zum ersten Mal in Betrieb nimmt und einrichtet, muss sich mit einem eventuell bereits bestehenden Benutzerkonto anmelden oder ein Benutzerkonto erstellen, um die Dienste im vollem Umfang nutzen zu können.

Modul 7.1: E-Mailing

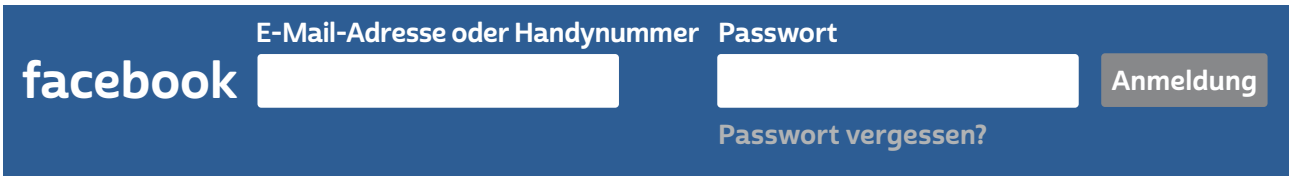
Durch die Anmeldung über das Benutzerkonto, englisch „Account“, identifiziert sich ein*e Nutzer*in gegenüber dem Anbieter. Doch nicht nur für die Verwendung des Smartphones oder Tablets ist ein Account notwendig. Auch für das eigene E-Mail-Postfach, das Onlinebanking oder für ein soziales Netzwerk müssen Nutzer*innen eine Identifizierung festlegen. Wer häufig beim selben Onlineshop Waren bestellt, kann auch dort einen eigenen Account einrichten.

Modul 4.1: Einkaufen im Netz

Beispiel für einen Free-Mail-Account:



Beispiel für ein soziales Netzwerk (Facebook):

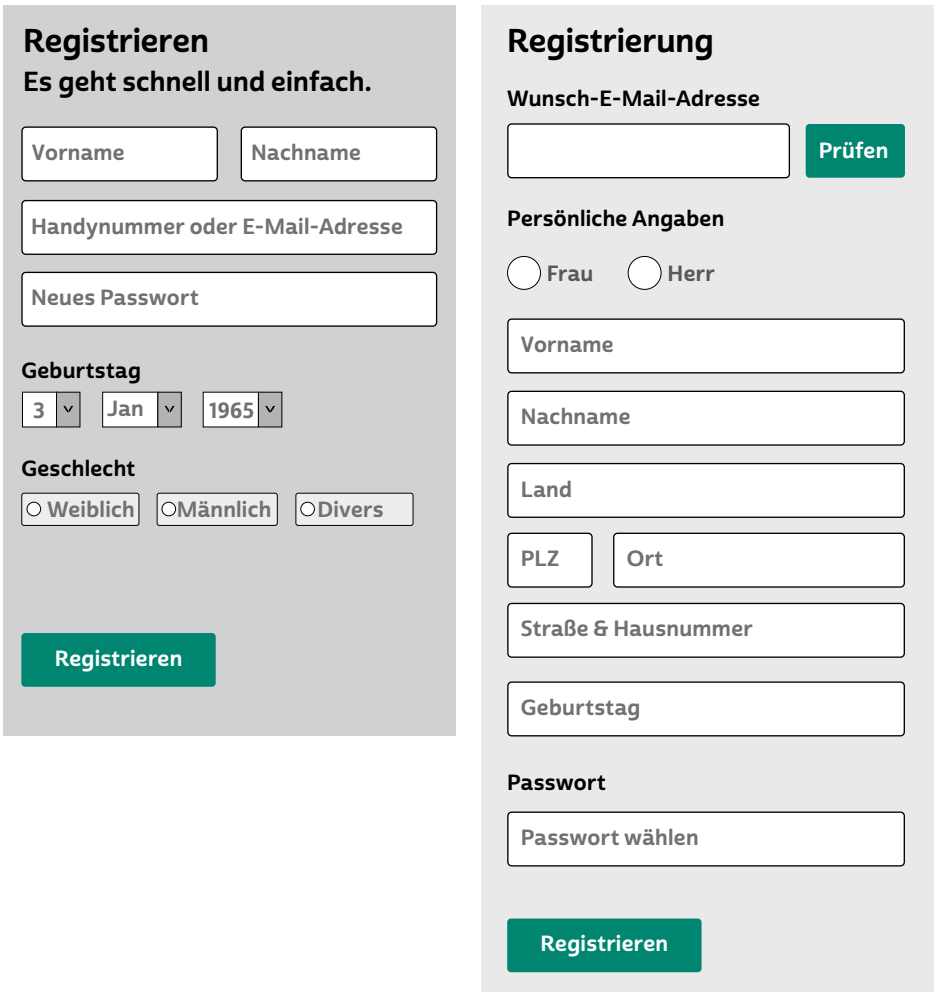


Ein Konto zu erstellen ist einfach. Bei der Einrichtung, auch Registrierung genannt, werden persönliche Daten abgefragt. Danach müssen ein Benutzername und ein Passwort gewählt werden. Der gewählte Name und das Passwort dienen später dazu, sich gegenüber dem jeweiligen Anbieter auszuweisen. Will man sich also bei einem Dienst anmelden, muss man zwingend den Benutzernamen und das zugehörige Passwort angeben.

Tipp

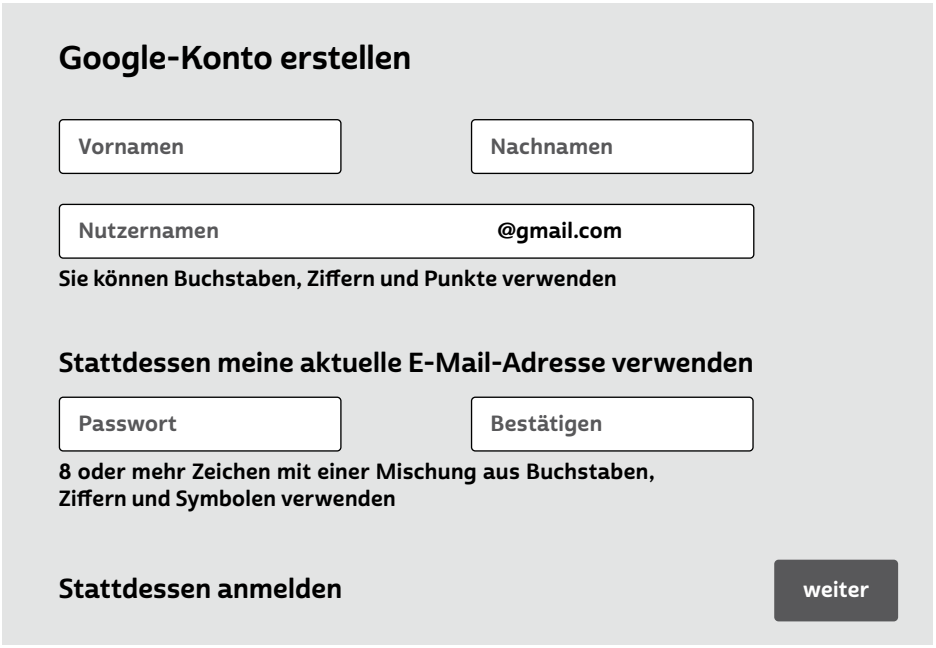
Seien Sie – so weit möglich – sparsam mit Ihren Daten. In der Regel sind Pflichtfelder mit einem Sternchen (*) gekennzeichnet.

Registrieren (Facebook/Free-Mail-Account)



Für das Einrichten eines Smartphones beispielsweise mit dem Betriebssystem Android wird in aller Regel beim ersten Einschalten abgefragt, ob bereits ein Konto bei Google besteht. Wenn noch kein Google-Konto vorhanden ist, muss ein solches erstellt werden. Durch die Einrichtung eines Google-Kontos können alle Google-Produkte über dieses Konto genutzt werden. Ohne Einrichten dieses Kontos kann das Smartphone oft nur sehr eingeschränkt genutzt werden.

Konto erstellen (google.de)



Auch bei anderen Anbietern von Smartphone-Betriebssystemen funktioniert dieses Prinzip ähnlich: Apple und Microsoft verlangen das Einrichten eines entsprechenden Nutzerkontos. Das Nutzerkonto kann oft mit einer Cloud verknüpft werden, also mit einem persönlichen Datenspeicher im Internet. Die dort gespeicherten Daten können über die Kombination aus Benutzernamen und Passwort von jedem beliebigen Gerät mit Zugang zum Internet abgefragt werden.

Aufgrund der Fülle an unterschiedlichen Benutzerkonten und der Empfehlung, für jeden Dienst ein eigenes Passwort zu verwenden, ist es fast unmöglich, sich alle Zugangsdaten auf Dauer zu merken. Hilfestellung bieten Passwortmanager. Um an die im Passwortmanager hinterlegten Passwörter zu gelangen, genügt es, sich nur noch ein Passwort, nämlich das Masterpasswort, zu merken.

Modul 4.7: Passwörter und Schutz von mobilen Endgeräten

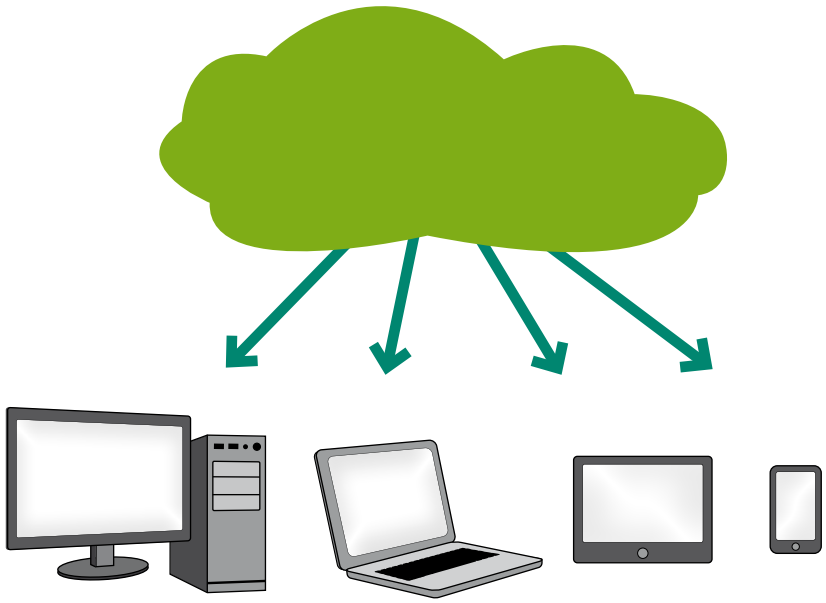
Wer ein Smartphone oder Tablet verkaufen oder verschenken möchte, sollte sich zuvor versichern, dass im Gerät keine Zugangsdaten zum Benutzerkonto mehr gespeichert sind. Das Benutzerkonto selbst bleibt auch ohne das Gerät noch so lange bestehen, bis eine vollständige Löschung des Accounts angestoßen wurde.

Wer alle Daten seines PCs oder Smartphones durch ein Zurücksetzen auf Werkseinstellung unwiderruflich löscht, löscht damit aber nicht das Konto. Dieses wird in der Cloud des Kontoanbieters gespeichert und ist weiterhin erreichbar. Bei der Neueinrichtung eines

Gerätes müssen nur die Zugangsdaten neu eingegeben werden. Danach hat man Zugriff auf alle zuvor in der Cloud gespeicherten E-Mails, Musikdateien, Apps oder Bilder.

Synchronisation

Ein weiterer Vorteil von Benutzerkonten besteht in der Möglichkeit, Daten auf mehreren Geräten einsehen und bearbeiten zu können. Die Daten werden synchronisiert. „Synchronisieren" bedeutet hier „abgleichen" oder „aufeinander abstimmen". Gemeint ist damit die Funktion, welche die eigenen Daten auf den unterschiedlichsten Geräten verfügbar macht. So können Kalender, Adressbücher oder E-Mails zum Beispiel von einem Smartphone durch einen automatischen Abgleich auch auf einem Tablet oder dem heimischen PC eingesehen und genutzt werden.



Mithilfe der Cloud können alle Dateien auf allen Geräten aktuell gehalten werden.

Werden die Daten am Tablet verändert, so wird die Änderung durch Synchronisation wiederum im Smartphone sichtbar. Die Daten werden in einer Cloud im Internet zwischengespeichert. Der Abgleich hilft außerdem beim Wechsel des Gerätes. Ein neues Smartphone muss nicht mühsam komplett neu eingerichtet werden. Stattdessen können die Daten aus einem bestehenden Benutzerkonto einfach auf das neue Gerät übertragen werden.

5.3 Cloud-Computing als Grundlage des mobilen Internets

Wenn es um das Speichern von Daten wie Fotos, Musik oder Dokumenten geht, nutzt man in der Regel einfach das Gerät, das man gerade in Gebrauch hat, seien es Smartphone, Tablet, Standcomputer, Laptop oder für größere Dateien auch externe Festplatten oder diverse USB-Sticks. Das Problem an der Sache: Sobald man die Daten auf mehreren Geräten verfügbar haben möchte, muss man sie umständlich von einem zum anderen kopieren. Auch von unterwegs kann man nur auf die Daten zugreifen, die auf dem jeweils mitgeführten Gerät vorhanden sind. Noch komplizierter wird es, wenn mehrere Personen im selben Haushalt oder einer Arbeitsgruppe mit unterschiedlichsten Geräten arbeiten und trotzdem miteinander Daten austauschen wollen. Hinzu kommt das Problem, dass bei Datendopplung, also wenn dieselbe Datei auf unterschiedlichen Geräten gespeichert ist, schnell der Überblick verloren geht, welches die aktuellste Version der jeweiligen Datei ist. Bei Dokumenten in Bearbeitung kann das fatal sein und erhebliche Mehrarbeit und Datenverlust verursachen.

So entstand der Bedarf nach einer zentralen Speichermöglichkeit, auf die von überall, sprich über das Internet, zugegriffen werden kann. Für einen solchen Speicherort im Internet hat sich heute der englische Begriff „Cloud“, zu Deutsch „Wolke“, etabliert. Da man die Speicherorte nicht sieht, erscheint es, als lägen sie in den Wolken. Wie auch immer man zu der Begrifflichkeit steht, kaum jemand wird heute noch abstreiten können, dass die Technik sehr hilfreich sein kann, um die oben beschriebenen Probleme und Bedürfnisse zu bedienen. Das Ganze funktioniert folgendermaßen:

Die Anbieter solcher Clouddienste stellen ihren Benutzer*innen Speicherplatz im Netz zur Verfügung. Die Benutzer*innen melden sich beim jeweiligen Anbieter an und können dann von ihrem PC, Laptop, Smartphone und Tablet auf den persönlichen Speicherplatz zugreifen. Doch was einen so innovativen Namen hat, ist gar nicht so neu. Früher nannte man das „Webspace“ oder „Onlinespeicher“. Jede Person, die schon einmal eine E-Mail in einem Internetbrowser gelesen oder geschrieben hat, hat schon einmal eine (Daten-)Wolke genutzt. Wie jeder Clouddienst greift auch das E-Mail-Konto auf Speicherplatz im Internet zurück.

Bei allen Clouddiensten ist eine Registrierung beziehungsweise ein Nutzerkonto bei den entsprechenden Anbietern erforderlich. Für die Auswahl des richtigen Speicherdienstes sollte man sich die Zeit nehmen und sich Vergleichstests einer seriösen Einrichtung (zum Beispiel Stiftung Warentest) anschauen. Hintergrund ist, dass es die unterschiedlichsten Anbieter und Angebote von Clouddiensten gibt, die sich in ihrem Angebot, ihrer Zuverlässigkeit und ihrer Seriosität teilweise erheblich voneinander unterscheiden.

Wer beim Datenschutz Wert auf eine erhöhte Absicherung legt, sollte zum Beispiel auf Anbieter zurückgreifen, die die Daten ausschließlich auf deutschen oder zumindest europäischen Servern ablegen. Damit unterliegen sie dem Schutz des strengen europäischen Datenschutzrechts sowie der entsprechenden Aufsichtsbehörden. In Deutschland bietet etwa die Telekom Deutschland GmbH mit der Magenta Cloud einen solchen Dienst an. Andere bekannte Anbieter, in der Regel mit Sitz in den USA, sind Amazon, Apple, Google, Microsoft oder Dropbox. Die Hersteller von Betriebssystemen wie Windows oder Android bauen Zugriffsmöglichkeiten für die von ihnen betriebenen Clouds schon jetzt in ihre Produkte ein, sodass keine Zusatzsoftware mehr notwendig ist. Wer etwa Microsoft 365 abonniert, erhält automatisch auch Speicherplatz in der Microsoft-Cloud. Wer seinen Cloudspeicher auch mit seinem Tablet oder Smartphone nutzen möchte, muss bei der Auswahl eines Dienstes darauf achten, ob es dafür passende Apps gibt.

§

Art. 51 Datenschutz-Grundverordnung

Tipp

NAS-Systeme für Profis

Erfahrene Nutzer*innen können sich auch ihren eigenen Cloudspeicherdienst konfigurieren. Bei diesen auf Englisch „**N**etwork **A**ttached **S**torages“ (kurz: NAS, zu Deutsch „netzgebundene Speicher“) genannten Systemen werden im Wesentlichen eine oder mehrere Festplatten mit dem Internet verbunden. Der Vorteil ist, dass Nutzer*innen die größtmögliche Kontrolle über die gespeicherten Daten haben. Von Nachtteil ist dagegen, dass ein NAS-System wartungsintensiv und nicht ganz leicht einzurichten ist.

Damit der Einsatz von Internetspeicherdiensten zuverlässig und sicher abläuft, sollten folgende Grundregeln beachtet werden:

- Sensible Daten sollten am besten verschlüsselt gespeichert werden. Gerade wenn der Dienst Daten auf US-Servern ablegt, besteht eine gewisse Unsicherheit, wer wann Zugriff auf die Daten hat. Daher sollte man auf Nummer sicher gehen.

Verschlüsseln von Daten

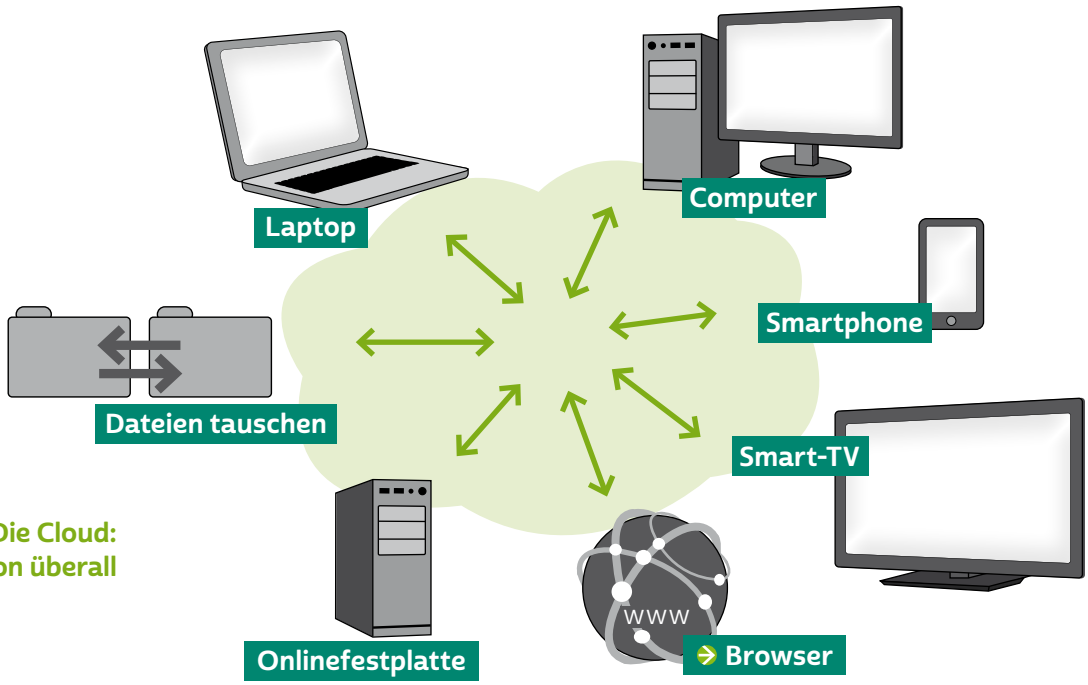
Nicht jede*r möchte, dass Dritte die Daten in der Cloud oder auf dem Weg dorthin auslesen können. Deswegen sollte man einen Clouddienst nutzen, der Daten auf dem Transportweg automatisch verschlüsselt. Für einen noch höheren Schutz sollte man die Daten selbst verschlüsseln.

Bei der Verschlüsselung werden digitale Daten, also zum Beispiel Texte oder Bilder, mittels mathematischer Verfahren für Dritte unleserlich gemacht. Entschlüsseln kann die Daten bei sicheren Verschlüsselungsverfahren nur diejenige Person, welche die richtigen digitalen Schlüssel besitzt. Für die Verschlüsselung benötigt man spezielle Programme, die kostenpflichtig und zum Teil auch kostenlos erhältlich sind. Auch hier sollte man vor der Auswahlentscheidung einen guten Produkttest lesen. Um die Daten jedoch auf allen gewünschten Endgeräten nutzen zu können, muss das entsprechende Verschlüsselungsprogramm auf allen Geräten installiert sein. Es gilt also, darauf zu achten, dass das Verschlüsselungsprogramm auch auf mobilen Endgeräten wie Smartphones oder Tablets funktioniert. Außerdem zu beachten:

- Man sollte vorab prüfen, wie groß die Dateien sind, die man in der Cloud ablegen möchte. Kostenfreie Dienste bieten in der Regel nur sehr begrenzten Speicherplatz.
- Zum vernünftigen Arbeiten mit einem Speicherdienst ist eine stabile Internetverbindung notwendig, da insbesondere das Hochladen großer Datenmengen ins Internet viel Zeit in Anspruch nehmen kann. In Gebieten mit schlechter Mobilfunkversorgung kann eine unzuverlässige Verbindung zu Clouddiensten die Freude an der Nutzung erheblich mindern.
- Je nach individuellen Bedürfnissen sollte geprüft werden, ob der Internetspeicherdienst Zusatzfunktionen bietet, wie das Freigeben von Dateien für andere Nutzer*innen, das Einrichten von Ordnern mit unterschiedlichen Zugriffsberechtigungen und Passwortsperren etc.

Tipp

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt etwa die Software True Crypt zur Verschlüsselung von Daten: *https://s.rlp.de/B88ch*



Die Cloud: Datenzugriff von überall

Worauf man bei der Auswahl eines Clouddienstes achten sollte

Cloudnutzer*innen sollten darauf achten, dass die Cloud so transparent und sicher wie möglich gestaltet ist. Das bedeutet, dass Verbraucher*innen darüber informiert werden:

- wo (Land, Region) sich welche ihrer Daten befinden,
- welche Subunternehmen noch eingeschaltet werden,
- wer Zugriff auf die Daten hat,
- welche Rechte und Pflichten der Cloudanbieter und welche Cloudnutzer*innen haben und
- ob der Anbieter die Daten für den Transport und die Lagerung verschlüsselt.

Was bringt die Zukunft?

Zukünftig werden nicht nur Daten, sondern ganze Rechenprozesse von Computern auf Server ins Internet ausgelagert werden. Dies nennt man heute schon Cloud-Computing. So ist es möglich, dass aufwendige Anwendungen wie professionelle Bildbearbeitung oder Computerspiele, die ansonsten einen Computer mit viel Hardware benötigen, auch auf einem kleinen Smartphone stattfinden können. Damit dies flächendeckend möglich ist, wird indes eine hervorragende Glasfaser-Internetinfrastruktur mit hohen Bandbreiten benötigt.

5.4 Persönliche Daten und Datenschutzrechte im Internet

Mobile Geräte wie Smartphones, Tablets oder Smartwatches wissen sehr viel über ihre Nutzer*innen: Aufenthaltsorte, Kontakte, Kommunikationsverhalten, Nutzungsgewohnheiten im Internet, Konsumgewohnheiten oder Gesundheitsdaten. Und häufig werden diese Daten weitergegeben. Vor allem die Werbewirtschaft hat Interesse an diesen Daten. Sie haben einen wirtschaftlichen Wert und werden daher vielfach verkauft. Auf der Grundlage der gesammelten Daten wird zum Beispiel Werbung auf die individuelle Situation der Nutzer*innen oder ihre tatsächlichen oder vermuteten Bedürfnisse zugeschnitten. Die Daten geben mobile Geräte dabei häufig preis, oft ohne, dass ihre Besitzer*innen dies wissen. Zudem versuchen Kriminelle oftmals, sensible Bankdaten oder Zahlungsdaten auszuspähen, um damit Zugriff auf fremde Konten zu erhalten oder im Namen der Betroffenen Käufe zu tätigen.

Gegen das Ausspähen der eigenen Daten kann man sich mit ein wenig Vorsorge allerdings schützen. Zudem bestehen Datenschutzrechte, mit denen man die Kontrolle über die eigenen Daten behalten kann.

§

Art. 12 ff. Datenschutz-Grundverordnung

Was mobile Geräte alles wissen

Die neuen digitalen Alleskönner Smartphone, Tablet oder Smartwatch können sehr genau verzeichnen, wie und wo Nutzer*innen das Gerät verwenden. Der eingebaute GPS-Chip ermöglicht dem Gerät, mittels Satelliten seinen Standort metergenau zu bestimmen. Auch

die Information über die empfangbaren Funknetzwerke erlaubt die Ortung des Gerätes und damit die Ortung der Person. Wird der Standort in regelmäßigen Abständen ermittelt, kann nachvollzogen werden, welche Orte Nutzer*innen gerne aufsuchen, wie häufig und wie lange sie sich dort aufhalten.

Das Gerät weiß zudem, wie häufig, wann und wie lange mit wem telefoniert wurde. Im Internet eingegebene Suchbegriffe und aufgerufene Seiten können gesammelt werden, ebenso wie die persönlichen Interessen und Vorlieben, die in sozialen Netzwerken wie Facebook, Instagram oder Pinterest eingetragen werden.

Smartwatches erfassen in Verbindung mit Fitness-Apps auf dem Handy minutiös Bewegungsaktivitäten und Vitalparameter wie Pulsschlag oder Herzrhythmus und berechnen daraus Kondition, Schlafverhalten oder mobile Aktivitäten ihrer Besitzer*innen – Daten, die man sicher mit Ärzt*innen teilt, mit anderen jedoch nur bedingt.

Smartphones – kleine Geräte für riesige Datenmengen

Mobile Geräte beziehungsweise die darauf installierten Apps können mit Kenntnis dieser persönlichen Daten tiefe Einblicke in die Privatsphäre der Nutzer*innen nehmen. Gegebenenfalls haben durch eine App auch Dritte einen Zugang zu den eigenen Daten, mit denen man selbst über die App in Kontakt ist. Wer die Neugierde und Sammel-

leidenschaft seiner digitalen Alltagsbegleiter verringern möchte, kann dies zum Beispiel durch Anpassung der Datenschutzeinstellungen tun.

Einstellungsoptionen findet man sowohl in den gängigen Betriebssystemen der Geräte als auch in den jeweiligen Apps. Es lohnt sich, diese genauer unter die Lupe zu nehmen. Häufig ist hier das Datensammeln, die Ablage der Daten in der Cloud oder das Teilen von Daten standardmäßig aktiviert, lässt sich jedoch mühelos abschalten. Hier kann man als Nutzer*in entscheiden, welches Programm auf welche Daten Zugriff bekommt und inwieweit diese zu Marketingzwecken verwendet werden dürfen.

Tipp

Wenn Sie sichergehen wollen, dass sich Geräte nicht unkontrolliert orten beziehungsweise orten lassen, sollten Sie darauf achten, dass die Funktionen GPS (Satellitenortung), WLAN und der Datenaustausch über die Funktechnik Bluetooth nur dann eingeschaltet sind, wenn Sie sie wirklich benötigen. Ein schöner Nebeneffekt: Der Akku wird weniger stark beansprucht. Hier vier praktische Tipps, wie der Akku in Zukunft länger durchhält: *https://s.rlp.de/NoSmo*

Rechte von Verbraucher*innen

Die Anbieter von Betriebssystemen und Apps dürfen mit den Daten auf mobilen Geräten nicht nach freiem Belieben verfahren. Die Erhebung, Speicherung und Nutzung von personenbezogenen Daten sind in vielen Fällen nur zulässig, wenn die Nutzer*innen zuvor eingewilligt haben. Wer die Kontrolle behalten will, sollte sich daher die jeweiligen Datenschutzbestimmungen anschauen. Denn durch die Bestätigung der Bestimmungen bei der Installation von Apps per Fingertipp wird diese Einwilligung erteilt.

Häufig, aber nicht immer, lassen sich bestimmte Datenübertragungen über die Einstellungen unterbinden. Die Datenschutzbestimmungen können sich jedoch genauso wie die Einstellungsmöglichkeiten jederzeit ändern.

Tipp

Das deutsche und das europäische Datenschutzrecht geben Verbraucher*innen ein Recht auf Auskunft über die zur eigenen Person gespeicherten Informationen, auf deren Berichtigung, wenn sie falsch sind, oder auf deren Löschung.

Setzen Sie sich bei Fragen dazu am besten direkt mit den Anbietern von Apps oder Geräten in Verbindung. In den meisten Fällen erreicht man den Anbieter über die Einstellungen der App oder den App-Store. Viele App-Anbieter haben zudem eine Website, über die Kontaktdaten zu finden sind. Seit Geltung der Datenschutz-Grundverordnung können diese Rechte auch gegenüber außereuropäischen Anbietern, zum Beispiel aus den USA, geltend gemacht werden, insbesondere, wenn diese sich mit ihrem Angebot an Nutzer*innen aus Deutschland oder Europa richten. Dies ist beispielsweise der Fall, wenn eine App in der jeweiligen Landessprache angeboten oder beworben wird.

Bei Problemen können die Aufsichtsbehörden für den Datenschutz weiterhelfen, das heißt die Datenschutzbeauftragten des Bundes und der Länder.

Silver Tipps!

Schutz der Privatsphäre:
https://s.rlp.de/v1Rsp

Datenschutzkontrolle:
https://s.rlp.de/tYiTt

Bezahlen mit den eigenen Daten

Viele Apps für mobile Geräte werden kostenfrei angeboten. Tatsächlich werden bei der Installation solcher Programme keine Kosten berechnet. Nutzer*innen zahlen stattdessen mit ihren Daten. Kostenlose Apps finanzieren sich üblicherweise durch Werbeeinblendungen, die sich am Verhalten der Nutzer*innen und ihren Gewohnheiten ausrichten. Aus den gesammelten Daten lässt sich das Konsumverhalten ablesen, wodurch Werbung gezielter platziert und deswegen auch teurer verkauft werden kann. In diesem Zusammenhang kann es passieren, dass sich der Hersteller eines kostenlosen Spielprogramms die Einwilligung geben lässt, dass er auf die Standortdaten und auf das im Gerät hinterlegte Adressbuch Zugriff nehmen darf. Dies geschieht auch dann, wenn dies zum Funktionieren der App gar nicht notwendig wäre.

Kaum eine App lässt sich installieren, ohne dass zuvor eine Reihe von Zugriffsrechten eingeräumt werden soll. Und die Nutzung und

Weitergabe der auf diese Weise gewonnenen Daten ist oftmals in Nutzungsbedingungen versteckt, die man mit der Installation der App akzeptiert. Vielfach kann eine App gar nicht erst installiert werden, ohne dass eine breite Einwilligung gegeben wird. Auch die Datenschutzeinstellungen erlauben häufig keine nachträglichen Änderungen zum Umfang der Datennutzung.

Tipp

Fragen Sie sich beim Installieren einer App, warum das Programm Zugriff auf bestimmte Daten des Smartphones will. Überlegen Sie, was die eigentliche Funktion der App ist und ob die erfragten Daten dazu plausibel benötigt werden. Eine Taschenlampen-App muss beispielsweise keinen Zugriff auf das Telefonbuch beanspruchen, um funktionsfähig zu sein, ein Spiel benötigt in der Regel nicht Ihren Aufenthaltsort und eine Blutdruck-App nicht Ihre Telefonliste. In solchen Fällen empfiehlt sich die Suche nach einer anderen App oder der Verzicht auf die Installation.

Kriminelle greifen nach Daten

Mobile Geräte werden in einem immer größeren Ausmaß zum Ziel krimineller Aktivitäten. Mit technischen Tricks versuchen Kriminelle, sensible Daten auszuspähen oder Zugriff auf Smartphones und Tablets zu erhalten. All das dient dem Ziel, Kreditkarten oder Bankkonten der Betroffenen zu eigenen Gunsten zu belasten oder auf Bezahlfunktionen zugreifen zu können, um Käufe zu tätigen. Wer Kreditkartenzahlungen oder Bankgeschäfte unmittelbar an seinem mobilen Gerät durchführt, sollte die Kontoauszüge aufmerksam auf Unregelmäßigkeiten untersuchen und diese der zuständigen Bank sofort mitteilen.

Häufig sollen Nutzer*innen dazu verleitet werden, zum Beispiel auf einen per E-Mail, SMS, WhatsApp-Nachricht oder Tweet verteilten Link zu klicken oder ein als Anlage mitgeschicktes Foto, Video oder Dokument zu öffnen. Das Anklicken eines Anhangs ist nur dann zu empfehlen, wenn die Absenderin oder der Absender bekannt ist. Im Zweifelsfall ist es besser, hierbei vorsichtiger zu sein und sich Rat zu holen. Zur Sicherheit sollte man E-Mail-Adressen genau prüfen und bei Unsicherheit lieber auf anderem Wege Kontakt aufnehmen, wie beispielsweise persönlich anrufen.

Modul 7.1: E-Mailing

Vor solchen kriminellen Zugriffen schützt – wie auch am heimischen PC – neben Aufmerksamkeit eine geeignete Sicherheitssoftware. Solche Programme sind von unterschiedlichen Anbietern in den App-Stores zu erhalten. Diese erkennen Schadsoftware, mit der Geräte manipuliert werden sollen, recht zuverlässig oder warnen vor dem Besuch verdächtiger Internetseiten. Neben der Einrichtung einer Sicherheitssoftware sollten Sie Programme grundsätzlich nur aus dem offiziellen Anbietershop des Geräteherstellers beziehen. Bei Quellen außerhalb der überwachten Bereiche ist die Gefahr, Schadsoftware zu erhalten, besonders groß.

Wichtige Datenschutztipps für die Nutzung von Apps

- Verwenden Sie nur Apps aus sicheren Quellen, also den Anbietershops der Geräteher-steller.
- Machen Sie sich mit den Datenschutzbestimmungen einer App vertraut. Beachten Sie, dass diese sich auch ändern können.
- Nutzen Sie die Datenschutzeinstellungen der Geräte oder Apps, um ungewollte Datenübertragungen einzuschränken; Bluetooth, GPS und WLAN sollten nur aktiviert sein, wenn sie benötigt werden.
- Prüfen Sie in den Datenschutzeinstellungen, welchen Apps Sie Zugriff auf Ihre Kontaktdaten, Telefonliste, Standortdaten, Kamera, Mikrofon oder Kalender eingeräumt haben. Wenn Sie sich nicht sicher sind, deaktivieren Sie den Zugriff. Wenn die App diesen zum Funktionieren wirklich benötigt, werden Sie eine entsprechende Meldung erhalten.
- Achten Sie darauf, welche Daten Sie auf Ihrem Smartphone gespeichert und abrufbar haben.
- Schützen Sie Ihre Daten durch Verschlüsselung, Passwort und nutzen Sie gegebenenfalls die Löschfunktion beim Verlust Ihres Geräts.
- Sichern Sie Ihre Daten und löschen Sie sie auf dem Gerät, bevor Sie das Smartphone zur Reparatur geben oder verkaufen. In der Regel ist dies mit dem Zurücksetzen auf die Werkseinstellungen oder den Auslieferungszustand verbunden.
- Virenschutz ist beim Smartphone unbedingt zu empfehlen – auch wenn sein Schutz nicht dem beim heimischen PC entspricht.
- Führen Sie Sicherheitsupdates durch und aktualisieren Sie regelmäßig das Betriebssystem.
- Sie können sich an den Anbieter von Apps oder Diensten wenden und Auskunft über die zu Ihrer Person gespeicherten Daten fordern.

Die Datenschutz-Grundverordnung (DSGVO)

Seit dem 25. Mai 2018 gilt die europäische Datenschutz-Grundverordnung (DSGVO) als europaweit einheitlicher Rechtsrahmen für den Datenschutz. Ein sehr wesentliches Prinzip ist, dass personenbezogene Daten nur auf gesetzlicher Grundlage oder mit Einwilligung verarbeitet werden dürfen.

Für die Wirtschaft wurde damit ein verlässlicher Rechtsrahmen geschaffen, um in der gesamten Europäischen Union tätig werden zu können. Die Datenschutzregeln der EU gelten dann auch für Unternehmen aus anderen Staaten, die in Europa ihre Dienste anbieten oder Waren verkaufen.

Über einige sogenannte Öffnungsklauseln haben die nationalen Gesetzgeber trotz der zumeist unmittelbar geltenden Datenschutz-Grundverordnung gewisse Spielräume für das jeweilige nationale Datenschutzrecht. Daher gibt es auch in Deutschland weiterhin das Bundesdatenschutzgesetz sowie mit Blick auf den Datenschutz in Behörden und Verwaltungen das jeweilige Landesdatenschutzgesetz. Diese enthalten jedoch nur ergänzende Vorschriften. Im Kern gibt die Datenschutz-Grundverordnung vor, an welche Regelungen man sich bei der Verarbeitung personenbezogener Daten halten muss.

Die wesentlichen Vorgaben bei der Verarbeitung personenbezogener Daten sind in den Grundsätzen in Artikel 5 DSGVO zusammengefasst. Dies sind

- die Rechtmäßigkeit der Verarbeitung nach Treu und Glauben,
- eine angemessene Transparenz,
- die Bindung an festgelegte Verarbeitungszwecke,
- eine Datenminimierung, d. h. die Beschränkung auf die Daten, die für den vorgesehenen Zweck erforderlich sind, und deren
- Richtigkeit, einschließlich des Schutzes vor unbefugter Veränderung,
- die Begrenzung der Speicherdauer und
- die Vertraulichkeit der Daten.

Datenverarbeitungsverfahren müssen so gestaltet werden, dass sie die Rechte der Betroffenen schützen. Außerdem müssen sie, etwa was den Umfang der Daten angeht oder ihre Weitergabe, über datenschutzfreundliche Voreinstellungen verfügen.

25. Mai 2018: Einführung der DSGVO

Verordnung: https://s.rlp.de/F0SXT

Art. 6 Datenschutz-Grundverordnung

Art. 5 Datenschutz-Grundverordnung

Ihre Rechte:
https://s.rlp.de/mBpuu

Informationspflichten und Auskunftsrechte:
https://s.rlp.de/auskunftsrecht

Recht auf Datenübertragbarkeit:
https://s.rlp.de/DcsrG

Modul 6:
Datenschutz im Internet

Die DSGVO stärkt die Betroffenenrechte, beispielsweise durch bestimmte Anforderungen an die Transparenz von Datenverarbeitungen und umfangreiche Informations- und Benachrichtigungspflichten.

Eine wichtige Rolle spielt dabei das Recht auf Auskunft. Nur wer weiß, welche Daten über die eigene Person gespeichert sind, zu welchen Zwecken und auf welcher Grundlage diese verarbeitet werden und ob und an wen die Daten gegebenenfalls weitergegeben werden, kann souverän über die Verarbeitung entscheiden oder beurteilen, ob man dies hinnehmen muss.

Der Anspruch auf Datenübertragbarkeit, also das Recht, die eigenen Daten bei einem Wechsel des Anbieters mitzunehmen, oder das „Recht auf Vergessenwerden“ stärken den Einfluss Einzelner auf die Verarbeitung ihrer Daten.

Gerade im Internet spielt für die Verarbeitung personenbezogener Daten die Einwilligung der Betroffenen eine große Rolle. Die Datenschutz-Grundverordnung enthält daher eine Reihe von Bestimmungen, die sicherstellen sollen, dass vor einer Einwilligung eine angemessene Unterrichtung darüber erfolgt, wie und wozu die Daten verarbeitet werden. Wichtig ist auch zu wissen, dass eine freiwillig erteilte Einwilligung jederzeit wieder zurückgenommen werden kann beziehungsweise dass bestimmten Verarbeitungen widersprochen werden kann.

Das Internet kennt keine Landesgrenzen. Die Datenschutz-Grundverordnung regelt daher, dass Anbieter, die sich mit ihrem digitalen Angebot an Nutzer*innen in der Europäischen Union richten, sich den dort geltenden Datenschutzvorschriften unterwerfen müssen. Hierzu zählen zum Beispiel Datenschutzerklärungen, die die vorgesehene Datenverarbeitung und die den Nutzer*innen dabei zustehenden Rechte beschreiben. Die Rechte, die die Grundverordnung gewährt, können damit zum Beispiel gegenüber Anbietern aus den USA oder anderen Ländern außerhalb der EU geltend gemacht werden.

Die DSGVO nimmt sich darüber hinaus auch digitalen Themen an, die für Verbraucher*innen erhebliche Auswirkungen haben, wie beispielsweise das sogenannte → Scoring (ein Verfahren zur Einschätzung der Kreditwürdigkeit) und das → Profiling (nutzenorientierte Erstellung eines Persönlichkeitsprofils).

5.5 Risiken und Nebenwirkungen von Apps

2020 nutzen 4 von 5 Deutschen ein Smartphone.

Modul 1.4: Die Entwicklung von Mobilfunknetzen und mobilen Endgeräten

Vier von fünf Menschen in Deutschland nutzen ein Smartphone (Stand 2020). Der digitale Alleskönner ist weit mehr als ein mobiles Telefon. Er ist ein handlicher Computer, mit dem man auch telefonieren kann. Die Anwendungen können alle Themenbereiche betreffen und mit den unterschiedlichsten Funktionen ausgestattet sein. Sie liefern beispielsweise Bus- und Bahnverbindungen, fungieren als Kommunikationsdienst, zeigen aktuelle Nachrichten an, bieten kleine Onlinespiele, Taschenrechner und vieles mehr. Die Software kann in den verschiedenen App-Stores, wie zum Beispiel Google Play Store (Android) oder Apple App Store (iOS), heruntergeladen werden.

Apps sind auch außerhalb der offiziellen App-Stores der Betriebssystemanbieter erhältlich. Das Herunterladen von Apps aus externen Quellen ist aber nicht empfehlenswert, da die Gefahr hier viel höher ist, das Gerät mit schädlicher Software zu infizieren.

Auf der Website eines angeblichen Produkttestanbieters wurde zum Beispiel eine gefälschte Produkttest-App zum Download angeboten, die nach einer bekannten Drogeriemarktkette benannt war. Diese seriös klingende App wurde unter anderem über soziale Medien beworben. Hatte man sich die App heruntergeladen, musste man auf der Mobilfunkrechnung unerklärliche Abbuchungen feststellen. Offensichtlich war die in der App installierte Schadsoftware in der Lage, Bezahlcodes per SMS anzufordern, die ankommenden SMS auszulesen und die Codes einzulösen.

Viele Apps sind kostenlos. Eine kostenlose App bedeutet aber nicht, dass der angebotene Dienst ohne Gegenleistung erfolgt. Diese Gratis-Apps finanzieren sich durch die Verwendung und Verarbeitung der Nutzerdaten. Daher verlangen einige von ihnen bei der ersten Anmeldung beispielsweise Daten zur Identität der Nutzer*innen oder Zugriff auf Kontakte, Standort, Fotos/Medien/Dateien oder den Speicher, die Kamera oder das Mikrofon des Gerätes, die WLAN-Verbindungsinformationen und vieles mehr.

Nutzer*innen sollten sich mit den (geforderten) Zugriffsberechtigungen einer App beschäftigen und diese im Einzelfall hinterfragen. Warum sollte man Berechtigungen erteilen, die für das Funktionieren einer App nicht benötigt werden? Für Smartphones mit dem weit verbreiteten Betriebssystem Android lässt sich dies vor dem Download

oder spätestens bei der Installation klären. Nutzer*innen werden in einem extra eingeblendeten Fenster gefragt, ob sie den Zugriff erlauben oder verweigern. Bei Geräten mit dem Betriebssystem iOS (iPhone/iPad) erfolgt jeweils eine Nachfrage, wenn auf das Adressbuch oder den Standort zugegriffen werden soll.

Darüber hinaus kann in den Einstellungen festgelegt werden, welche Apps überhaupt auf Standortdaten, das Adressbuch, den Kalender, Fotos, das Mikrofon oder die Kamera zugreifen dürfen. Von dieser Möglichkeit sollte man, wo immer möglich, Gebrauch machen und Apps nur Zugriff auf Informationen gewähren, die für die Nutzung eines bestimmten Dienstes erforderlich sind beziehungsweise deren Nutzen nachvollzogen werden kann.

Steuern kann man grundsätzlich auch, ob, wann und wer erfährt, wo man sich gerade befindet. Schließlich müssen die GPS- oder die WLAN-Funktion des Smartphones nicht dauerhaft aktiv sein. Wenn sie abgeschaltet sind, kann keine Applikation ungefragt auf Standortdaten zugreifen. Auch über die sogenannten mobilen Daten eines Smartphones können Standorte abgerufen und Daten vom Smartphone ins Internet (oder andersherum) übertragen werden. Deshalb ist es manchmal eine Überlegung wert, die mobilen Daten nur dann zu aktivieren, wenn der Zugang zum Internet tatsächlich benötigt wird.

Ein Beispiel für eine App, die man auf jeden Fall auf dem Smartphone haben sollte, ist eine Antiviren-App. Denn ein Smartphone ist mehr Computer als Telefon und daher genauso anfällig für Viren oder Trojaner wie der heimische PC. Von allen großen Anbietern, die man aus dem PC-Bereich kennt, gibt es bereits Virenschutzprogramme speziell für Smartphones. Auch diese können über den entsprechenden Store heruntergeladen werden. Sie sollen Schadsoftware im Smartphone-Speicher finden und jeden Versuch unterbinden, diese zu installieren.

Modul 7.1: E-Mailing

Tipp

Wer ein Virenschutzprogramm für seinen PC oder Laptop hat, bekommt hier häufig einen Virenschutz für das Smartphone dazu. Hierfür fallen keine extra Kosten an.

Auch das Betriebssystem eines Smartphones sollte regelmäßig aktualisiert werden. Die Anbieter stellen Updates für die Software zur Verfügung, die zeitnah auf dem Gerät installiert werden sollten. Sie bieten den besten Schutz gegen Schadsoftware, denn die meisten Schadprogramme nutzen Sicherheitslücken. Diese können durch ständige Aktualisierungen geschlossen werden.

Auf neuen Smartphone-Modellen befinden sich oft vorinstallierte Apps. Diese sollen Smartphone-Nutzer*innen dazu bringen, gleich nach dem Kauf Produkte wie Hörbücher, Musik und Filme möglichst bei bestimmten Anbietern zu kaufen. Nicht jede*r ist über diese „Bloatware“ erfreut. Leider lässt sie sich in den meisten Fällen nicht vom Gerät löschen. Die unerwünschten Apps können aber zumindest deaktiviert werden.

5.6 Mobile Payment

Der Begriff „Mobile Payment“ bedeutet auf Deutsch „mobiles Bezahlen“. Dahinter stehen zahlreiche technische Verfahren, mit deren Hilfe Verbraucher*innen mit mobilen Geräten wie dem Smartphone oder einer Smartwatch oder mit der Giro- oder Kreditkarte kontaktlos bezahlen können. In der Vorstellung der Anbieter solcher Systeme sollen diese Techniken das Bargeld, vor allem bei Kleinbeträgen, irgendwann vollständig ersetzen. Ein Vorteil von Mobile-Payment-Technologien ist die geringe Zeit, die ein Bezahlvorgang benötigt. Seit Kurzem ist das Interesse an kontaktlosem Bezahlen aus ganz anderen, zuvor wenig beachteten Gründen enorm angestiegen: Mit der Corona-Krise wurde das kontaktlose Zahlen über die Giro- oder Kreditkarte 2020 aus Hygienegründen zur Pionieranwendung des mobilen Bezahlens. Jenseits der kartenbasierten Systeme ist der Markt für mobile Bezahllösungen aber noch immer unübersichtlich, da sich bislang keine verbreiteten Standards herausgebildet haben.

Wie funktioniert das mobile Bezahlen?

Die neuen Bezahlverfahren funktionieren kaum anders als das Zahlen mit der Girokarte am Kassenterminal. Der wesentliche Unterschied besteht in der Neuerung, dass beim mobilen kontaktlosen Bezahlen

keinerlei Kontakt mehr zwischen der Karte oder dem Smartphone als Datenträger und dem Kassenterminal bestehen muss. Die Datenübertragung zwischen Smartphone beziehungsweise funkfähiger Kredit- oder Girokarte und dem Kassenterminal wird bei den meisten Verfahren durch den Funkstandard NFC ermöglicht. Diese Abkürzung steht für „**N**ear **F**ield **C**ommunication“, bedeutet also wörtlich übersetzt auf Deutsch „Nahfeldkommunikation“. Karten und Geräte müssen zur Übertragung nur für einen kurzen Moment zusammengehalten werden. In den Karten und Geräten verbergen sich Computerchips, die über eine Miniaturantenne verfügen. Ob eine Karte oder ein Lesegerät NFC-fähig ist, ist anhand dieser Kennzeichen zu erkennen:

Kennzeichnung der Lesegeräte

Kennzeichnung auf Karten

2020 bieten ca. 75 Prozent der Giro- und Kreditkarten die Möglichkeit zum kontaktlosen Bezahlen.

Mobiles Bezahlen mit funkfähigen Karten

Etwa 75 Prozent der in Umlauf befindlichen Giro- und Kreditkarten sind mittlerweile mit einem entsprechenden Chip ausgestattet (Stand 2020). Und immer mehr Kartenzahlungsterminals an den Kassen bieten die Kontaktlos-Funktion an. Die Karte muss nur noch mit einem Abstand von weniger als vier Zentimetern an das Kartenzahlungsterminal gehalten werden und der Bezahlvorgang wird durchgeführt. Bei Beträgen unter 25 Euro erfolgt die Zahlung sogar meist ohne Eingabe

der PIN, der **p**ersönlichen **I**dentifikations**n**ummer, die man beim Zahlen durch das Einstecken der Karte ins Zahlungsterminal normalerweise eingeben muss. Wegen der hohen Nachfrage nach kontaktlosen Bezahlmöglichkeiten wurde dieses Limit sogar von 25 auf 50 Euro erhöht.

Mobiles Bezahlen mit Smartphone und Smartwatch

Ganz ohne Karte kommt aus, wer ein Smartphone oder eine Smartwatch zum Zahlen benutzt. Dies ist nur in Verbindung mit einer speziellen App eines Finanzdienstleisters mit Bezahlfunktion möglich, die zuvor heruntergeladen und installiert werden muss. Die Auswahl der Verfahren ist groß. Es gibt:

- Banking-Apps mit Bezahlfunktion (etwa Paydirekt oder Giropay)
- Kunden-Apps des Einzelhandels (z.B. von Edeka oder Netto)
- Apps von übergreifenden Kundenbindungs-/Bonusprogrammen (z.B. von PayPal)
- Bezahl-Apps von Betriebssystemherstellern (Google Pay und Apple Pay)
- sonstige Zahlungsdienste (etwa Vimpay oder Bluecode)

Marktüberblick: https://s.rlp.de/8l74I

Für die Übertragung der Zahlungsdaten werden meist die in den Geräten standardmäßig verbauten NFC-Chips genutzt. Manche Verfahren arbeiten aber auch mit Grafiken oder Codes, die auf dem Smartphone angezeigt und an der Kasse ausgelesen werden. Zur Nutzung der Bezahlverfahren sind eine Anmeldung beim jeweiligen Anbieter und die Installation der entsprechenden App erforderlich. Die Registrierung und Nutzung können mit Kosten verbunden sein. Teilweise müssen Verbraucher*innen zur Bonitätsprüfung in eine Schufa-Abfrage einwilligen. In jedem Fall muss ein Bezahlweg in dem System hinterlegt werden, sei es ein Girokonto zur Durchführung eines Lastschriftverfahrens, sei es eine Kreditkarte oder ein Internetbezahlsystem wie PayPal.

Auch Zahlungen an Freund*innen oder Bekannte von einem Smartphone zu einem anderen sind möglich. Diese Anwendungen sind vor allem für den privaten Bereich gedacht, benötigen aber ebenfalls spezielle Apps. Vorsicht: Für geschäftliche Transaktionen mit Unbekannten sind solche Zahlungssysteme nicht geeignet, da einmal gezahltes Geld nicht zurückgeholt werden kann.

Geld an Freunde senden: https://s.rlp.de/4EWhL

Eine besondere Funktion bieten „E-Wallets“, zu Deutsch „elektronische Geldbeutel“. Hierbei handelt es sich um Apps, in denen Karten ganz unterschiedlichen Typs hinterlegt und beim Bezahlen genutzt werden können. Neben Kreditkarten können dort zum Beispiel Flug- und Veranstaltungstickets, Mitgliedskarten und Karten aus Kundenbindungsprogrammen wie Payback oder DeutschlandCard eingepflegt und gemeinsam verwendet werden.

Abrechnung

Die Abrechnung im Mobile Payment ist häufig nicht so einfach nachzuvollziehen. Je mehr Unternehmen an einem mobilen Bezahlvorgang beteiligt sind, desto unübersichtlicher wird der Geldfluss. Im Mobile Payment fließt das Geld nicht direkt zwischen Kund*innen und Händlern, sondern über meist mehrere Finanzdienstleister. Am Ende eines Zahlungsvorgangs wird in aller Regel das Girokonto der Kund*innen im Zuge eines Lastschriftverfahrens belastet. Bei manchen Bezahlsystemen erscheinen die Beträge zunächst auf der Telefon- oder Kreditkartenabrechnung. Außerdem fallen manchmal Zusatzgebühren an.

Wie steht es mit der Sicherheit?

Die Gefahr für das Auslösen ungewollter Transaktionen oder für Zugriffe durch Kriminelle ist wegen der zahlreichen Schutzmaßnahmen von Seiten der Anbieter grundsätzlich als gering einzustufen. Vollkommen ausgeschlossen ist dies aber nicht: So gelang es Journalist*innen für einen Fernsehbeitrag von 2019, von Karteninhaber*innen unbemerkt kontaktlose Zahlungsvorgänge auszulösen. Hiervor können spezielle Kartenhüllen schützen. Außerdem haften Bankkund*innen bei einer solchen missbräuchlichen Nutzung nur bis zu einem Betrag von 50 Euro. Zum Vergleich: Wird einem das Portemonnaie gestohlen, ist das Bargeld auch weg – ohne irgendeine Begrenzung.

Trotzdem gilt: Wer Smartphone oder Karten zum mobilen Bezahlen nutzt, muss besonders gut auf diese aufpassen. Nutzer*innen von Mobile Payment sollten ihre Kontoauszüge stets sorgfältig auf mögliche unberechtigte Abbuchungen prüfen. Auf dem mobilen Gerät, über das mobile Bezahlvorgänge abgewickelt werden, sollte eine Schutzsoftware gegen Viren und Trojaner eingesetzt werden.

Fernsehbeitrag:
https://s.rlp.de/TMcz5

Tipp

Kommen zum Zahlen genutzte Smartphones, Kredit- oder Girokarten abhanden, sollten Sie Karten und Konten unverzüglich über den zentralen Sperr-Notruf 116 116 sperren lassen und Ihre Bank informieren.

Worauf man achten sollte

Wer sich einem mobilen Bezahlsystem anschließen möchte, hat die Wahl unter einer Reihe von Anbietern. Solange noch zahlreiche konkurrierende Systeme am Markt bestehen, entscheidet man sich am besten für einen Anbieter, dessen System dort genutzt werden kann, wo man regelmäßig einkauft. Unterschiede gibt es daneben bei den angebotenen Bezahlwegen. Zu beachten ist auch, dass nicht alle Systeme überall im Ausland nutzbar sind.

Die Informationen aus den Bezahlvorgängen geben Details zum Konsumverhalten preis. Bei Abschluss eines Nutzungsvertrages sollte anhand der Datenschutzbestimmungen sichergestellt werden, dass diese Daten nicht zu Marketingzwecken, sondern nur zur Abwicklung der Bezahlvorgänge verwendet werden. Leider ist es jedoch oft so, dass Unternehmen die Daten an Partnerunternehmen weiterleiten.

Silver Tipps!

Interview mit der deutschen Bundesbank: https://s.rlp.de/vX7Op

Unterschied zwischen Mobile Banking und Mobile Payment: https://s.rlp.de/BxjSh

5.7 Back-ups

Was passiert mit den Daten, wenn der Laptop durch ein Missgeschick vom Schreibtisch fällt und sich nicht mehr anschalten lässt oder das Smartphone unglücklicherweise in einer Bar geklaut wird? Es gibt wohl wenig, was so frustrierend ist, wie mitansehen zu müssen, wie das Ergebnis langer, mühevoller Arbeit in Sekundenbruchteilen unwiederbringlich in Rauch aufgeht. Genau darin besteht die Gefahr, die einem drohen kann, wenn man es versäumt, die eigenen Daten ausreichend gegen Ausfall abzusichern, sprich ein Back-up der Daten zu erstellen.

Der Verlust dieser Daten kann leider schneller geschehen, als man sich das vorstellen möchte. Häufigster Grund für Datenverlust sind wohl der Verlust oder die Beschädigung der Festplatte, auf der die

Daten liegen. Dies kann bei Festplatten, gerade wenn sie schon etwas älter sind, leider sehr plötzlich geschehen, ohne dass es zuvor warnende Anzeichen gegeben hätte. Gleichermaßen kann ein Laptop, Smartphone etc. gestohlen werden, in den Pool fallen oder sonstige endgültige Begegnungen erfahren. Häufig ist heute leider auch der Verlust durch Internetkriminalität zu beklagen, wenn Geräte durch Schadsoftware in Mitleidenschaft gezogen werden. Zuletzt sind es nicht selten auch die Anwender*innen selbst, die aus Versehen oder Unkonzentriertheit ungewollt Daten löschen, die sich nicht wiederherstellen lassen.

All dies kann verhindert werden durch das Einrichten regelmäßiger Datensicherungen. Hierbei sollten folgende Punkte beachtet werden:

Modul 5.3: Cloud-Computing als Grundlage des mobilen Internets

- Datensicherungen sollten immer auf einem anderen physischen Gerät erfolgen, damit die Datensicherung bei Verlust oder Beschädigung des ursprünglichen Geräts nicht auch betroffen ist. Sprich, es reicht nicht, wenn man auf dem Laptop einfach nur einen neuen Ordner anlegt und in diesen die wichtigsten Dateien hineinkopiert. Um die Dateien wirklich zu sichern, muss der fragliche Ordner am besten auf einer externen Festplatte oder in einem Cloudspeicher abgelegt sein.

Tipp

Ist ein Computer mit Schadsoftware infiziert, breitet sie sich meist über alle Festplatten aus. Daher sollte die Datensicherung auf einer Festplatte oder einem Dienst erfolgen, der nicht dauerhaft mit dem zu sichernden Gerät verbunden ist.

- Die einfachste Form der Datensicherung besteht aus dem oben beschriebenen händischen Kopieren von Daten. Dies birgt indes die Gefahr, dass man vergisst, die Daten regelmäßig zu speichern.

- Sicherer ist es, Datensicherungen mithilfe spezieller Software zu automatisieren, sodass man sich dazu keine Gedanken mehr machen muss.

- Je mehr Datensicherungen an unterschiedlichen Orten, desto höher ist der Schutz.
- Je nach Bedarf gibt es hierfür kostenlose und kostenpflichtige Softwarelösungen, wobei für die einfache Datensicherung problemlos kostenlose Lösungen ausreichen.

Datensicherungen einrichten: https://s.rlp.de/gDKR6

Daten sicher löschen

Daten sind heute auf vielen Geräten gespeichert. Daher ist es umso wichtiger, die Daten richtig zu löschen, wenn diese Geräte nicht mehr benötigt werden. Leider ranken sich hier noch viele Mythen um die richtige Art der Löschung. In der digitalen Welt bedeutet das Wort „gelöscht“ lediglich, dass der Speicherplatz zum Überschreiben freigegeben ist. So sind die Daten für die Nutzer*innen zwar nicht mehr zu sehen, sind aber trotzdem noch vorhanden. Mit kleinen, einfachen Programmen können die Daten durchaus wiederhergestellt werden. Um dies zu verhindern, sollte Folgendes beachtet werden:

Datenträger (USB-Sticks, Festplatten, Speicherkarten): Vor der Weitergabe oder dem Verkauf sollten die Datenträger mindestens gründlich formatiert werden (Achtung: Die „Schnellformatierung“ reicht hier nicht aus!). Zudem gibt es Programme, die die Datenträger mit unsinnigen Daten vollschreiben, also sicher und nicht wiederherstellbar löschen. Wird der Datenträger sowieso entsorgt, so kann dieser auch vorher mechanisch zerrstört werden. Mechanische Zerstörung kann dabei bedeuten, dass man die Festplatte aufschraubt und die Einzelteile beispielsweise zersägt. Dies gilt insbesondere auch für defekte Geräte vor der Entsorgung.

Geräte (Smartphones, Tablets, Internetrouter): Vor der Weitergabe oder dem Verkauf dieser Geräte sollten ebenfalls alle Daten gelöscht werden. Der Internetrouter hat mindestens die Zugangsdaten für den Internetanschluss, den Festnetzanschluss sowie das WLAN gespeichert. Auch auf Smartphones oder Tablets sind viele persönliche Daten gespeichert. Achten Sie darauf, dass solche Geräte auf die Werkseinstellungen zurückgesetzt werden. Auch hier gilt: Wird das Gerät entsorgt, so kann dieses auch mechanisch zerstört werden.

„Das Smartphone kann ein großartiges Instrument der Teilhabe sein, wenn wir allen die Chance geben können, souverän, frei und weitgehend gefahrlos mit diesem Werkzeug umzugehen.“

INTERVIEW MIT

Dr. Marc Jan Eumann

Direktor der Medienanstalt Rheinland-Pfalz

Vor welche Herausforderungen stellt uns das mobile Internet? Welche Chancen bietet es uns?

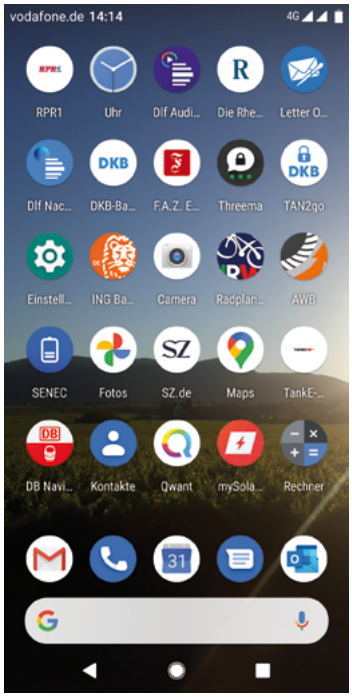
Dr. Marc Jan Eumann: Das mobile Internet holt uns die Welt auf den Bildschirm unseres Handys oder Tablets. Darin liegen immense Chancen wie auch große Herausforderungen. Verstärkt in den Zeiten der Corona-Pandemie machen wir doch alltäglich die Erfahrung, dass wir mit fast allem und allen in Verbindung treten können: Mit unseren Freund*innen und Familienangehörigen, die weit entfernt leben oder in Zeiten der Kontaktbeschränkungen „real“ nicht erreichbar sind. Aber auch mit dem gesamten Wissen der Welt, ohne dass wir eine Volkshochschule, ein Museum oder eine Bibliothek betreten. Die vielfältigen Möglichkeiten beinhalten aber auch Risiken: Wer sagt uns, welche Informationen vertrauenswürdig sind, welche Kontakte auf Social-Media-Kanälen echt und verlässlich sind, welche Angebote seriös und wirklich günstig sind? Eine Herausforderung liegt darin, immer aufs Neue sein eigenes Urteilsvermögen zu trainieren, möglichst ohne dabei in allzu große Fallen zu tappen.

Warum ist das mobile Internet bzw. die Nutzung eines Smartphones so wichtig, um an der Gesellschaft teilhaben zu können?

Dr. Marc Jan Eumann: Jede*r kann sich selbst befragen, wie lange sie oder er auf das eigene Smartphone verzichten kann – meistens ist „Handyfasten“ sehr schnell kritisch: Viele Alltagsbedarfe werden mehr und mehr über das Smartphone gedeckt – Einkäufe, Bankerledigungen, Bus- und Zugtickets, Eintrittskarten –, aber auch für Fitnesstraining, Reise- und Wanderplanung, Gesundheitsinfos und Genusstipps sind Smartphone-Apps gut, von den Nachrichten aus der großen Welt und den kurzen Dialogen mit Angehörigen und Freund*innen ganz zu schweigen. Im gleichen Maß verschwinden in der analogen Welt Orte, die für Teilhabe stehen: Post- und Bankfilialen, Buchläden und vieles mehr. Das Smartphone kann ein großartiges Instrument der Teilhabe sein, wenn wir allen die Chance geben können, souverän, frei und weitgehend gefahrlos mit diesem Werkzeug umzugehen.

Zeigen Sie uns einen Screenshot Ihres Smartphone-Home-Bildschirmes?

Dr. Marc Jan Eumann: Klar!



Glossar

Account: Ein Account ist ein Benutzerkonto für einen Onlinedienst, zum Beispiel für einen E-Mail-Service oder eine Videoplattform. Meistens gewährt dieses Benutzerkonto Zugang zu gespeicherten persönlichen Informationen oder zu sonst nicht frei zugänglichen Bereichen einer Internetseite oder eines Internetdienstes.

analog und digital: Bei der analogen und der digitalen Signalübertragung geht es zunächst um die Frage, wie ein Signal von einem Sender zu einem Empfänger kommt. Ein Beispiel hierfür ist die Übertragung von Musik etwa einer Schallplatte oder einer CD zu einem Verstärker. Bei einer klassischen Schallplatte wird die Musik analog in Form eines elektrischen Signals übertragen. Der Begriff „analog" kommt aus dem Griechischen und bedeutet „ähnlich". Analoge Signale ähneln dem, was sie wiedergeben. Eine Schallplatte gibt Tonschwingungen wieder und erzeugt daraus eine elektrische Schwingung. Diese Schwingung nimmt dabei viele unterschiedliche Spannungswerte an. Bei der digitalen Übertragung, beispielsweise bei der Aufnahme einer CD, werden Tonschwingungen in eine eigene digitale Sprache übersetzt.

Im Vergleich zum analogen Signal gibt es beim digitalen nur zwei Spannungen oder zwei Werte. Man nennt dies auch „binäre Codierung" (1 oder 0). Die Kunst beim Digitalen besteht darin, analoge Signale aus der Umwelt (Stimmen, Töne etc.) in digitale zu übersetzen. Der Vorteil ist die universelle Einsatzmöglichkeit: Sind sie einmal digital, können Daten nahezu überall in der digitalen Welt eingesetzt werden, beispielsweise weil die Tonaufnahme in Form von Daten vorliegt. Eine CD kann im Computer gelesen und die Musikstücke auf den PC kopiert werden. Von dort kann die Musik mithilfe von Programmen in eine MP3-Datei umgewandelt und auf den MP3-Player übertragen werden und so weiter. Eine Schallplatte hingegen kann nur von einem Schallplattenspieler gelesen werden und ist daher nicht universell nutzbar.

Ein weiterer Vorteil des Digitalen ist die Möglichkeit, unterschiedliche Inhalte miteinander zu kombinieren, wie Audio, Video und Text. Dies geht nur, weil beim Digitalen eine Art Universalsprache zum Einsatz kommt. Dieser verdanken wir auch, dass zum Beispiel der Computer alle möglichen Inhalte wiedergeben und kombinieren kann.

App: Die Abkürzung „App“ steht für das englische Wort „**App**lication“, was so viel wie „Anwendung“ bedeutet. Diese Anwendungen sind nichts anderes als Programme, die je nach Funktionalität mal größer und mal kleiner im Datenumfang sind. Der Begriff „Apps“ ist in seiner Verwendung sehr eng an Smartphones und Tablet-Computer gebunden. Apps bezieht man über spezielle Stores (virtuelle Einkaufsläden), am sichersten über den Anbieter des geräteeigenen Betriebssystems.

Benutzerkonto: siehe *Account*

Betriebssystem: Das Betriebssystem ist die Schaltzentrale eines PCs, Smartphones oder Tablets. Es verwaltetet alle verbauten Komponenten wie Festplatten, Grafikkarten oder Arbeitsspeicher und stellt den Nutzer*innen eine grafische Oberfläche zur Verfügung, mit der sowohl Programme aufgerufen als auch Dateien verwaltet werden können. Bekannte Betriebssysteme für PCs sind Windows, macOS oder Linux, für mobile Geräte Android und iOS. Damit keine Schädlinge auf einen Computer gelangen und Sicherheitslücken seitens Krimineller genutzt werden können, ist es wichtig, das Betriebssystem immer auf dem aktuellen Stand zu halten und regelmäßig Aktualisierungen, sogenannte Updates, vorzunehmen.

Bloatware: Mit dem Begriff „Bloatware“ (zu Deutsch „Blähware“) bezeichnet man eine Software, welche aufgrund einer Vielzahl an Funktionen überladen ist, ohne den Nutzer*innen einen wirklichen Mehrwert zu bieten. Die Unübersichtlichkeit macht es schwer, die Software zu warten, weshalb sie besonders fehleranfällig ist und somit auch ein Einfallstor für Schadsoftware sein kann.

Bluetooth: Unter diesem Begriff versteht man einen Standard zur Datenübertragung per Funktechnik. Per Bluetooth lassen sich beispielsweise Daten wie Bilder von einem Smartphone oder Handy zu einem anderen übertragen.

Browser: Egal ob am Laptop oder Smartphone: Browser sind der Dreh- und Angelpunkt des Internetgebrauchs. Das Wort „Browser“ kommt aus dem Englischen, das Verb „to browse“ bedeutet „durchstöbern“.

Browser machen das Anschauen von Internetseiten im World Wide Web erst möglich. Sie können den sogenannten Quelltext, der auf Websites hinterlegt ist, lesen und ihn grafisch darstellen. Bekannte Browser sind Microsoft Edge, der bereits auf den meisten Computern mit Windows als Betriebssystem installiert ist, Mozilla Firefox und Google Chrome, die oft separat installiert werden müssen. Auf Smartphones mit Android als Betriebssystem ist Google Chrome häufig standardmäßig als Browser eingerichtet. Der Standardbrowser für Apple-Geräte ist Safari.

Cloud: Eine Cloud (zu Deutsch „Wolke“) ist ein Speicher im Internet. Hat man früher Daten meistens lokal auf der eigenen Gerätefestplatte gespeichert, kann man heute Daten auch auf Rechnern eines Cloudanbieters speichern und über das Internet abrufen. Da man nicht genau weiß, wo die eigenen Daten tatsächlich liegen, passt der Begriff „Cloud“ sehr gut.

digital: siehe *analog und digital*

Download: Bei einem Download werden Daten aus dem Internet auf den heimischen Computer oder mobile Endgeräte wie Smartphones und Tablets heruntergeladen, also übertragen.

Gateway: Mit „Gateway“ (zu Deutsch „Torweg“) wird ein Bestandteil bezeichnet, welcher eine Verbindung zwischen zwei Systemen herstellt und so den Datenstrom vom Start- zum Endpunkt übermittelt. Dabei kann es sich sowohl um einen Teil der Hardware als auch einen Teil der Software handeln.

GPS: Die Abkürzung „GPS“ steht für „**G**lobal **P**ositioning **S**ystem“ und bezeichnet ein Navigationssystem, das mithilfe von Satelliten den Standort von Nutzer*innen auf einige Meter genau bestimmen kann. GPS findet man in vielen Autonavigationssystemen, aber auch in Smartphones oder Tablets.

Handy: Der Begriff „Handy“ hat sich in Deutschland als Synonym für die Begriffe „Mobiltelefon“ beziehungsweise „Smartphone“ durchgesetzt. Handy ist nur eine scheinbare Entlehnung, denn im Englischen bedeu-

tet das Wort so viel wie „handlich, geschickt“. Im englischen Sprachraum werden für Mobiltelefone eher die Begriffe „mobile (phone)“ oder „cell(ullar) phone“ genutzt.

Internet: Das Internet ist ein weltweit zwischenverbundenes Computernetzwerk (auf Englisch „**Inter**connected **Net**work“). Das bedeutet, dass viele einzelne Netzwerke, zum Beispiel von Firmen, öffentlichen Einrichtungen oder auch privaten Nutzer*innen, in einem Netzwerkverbund stehen.

Kartenzahlungsterminal: Ein Kartenzahlungsterminal ist ein Gerät, welches Bank- oder Kreditkarten auslesen kann und somit das bargeldlose Bezahlen in einem Geschäft ermöglicht. Die Nutzung ist meist durch die zusätzliche Eingabe einer PIN oder einer Unterschrift gesichert. Bei einem Betrag unter 25 Euro (oder unter 50 Euro) kann diese zusätzliche Sicherung aber auch entfallen.

LAN: Die Abkürzung „LAN“ steht für den englischen Begriff „Local Area Network“ (zu Deutsch „lokales Netzwerk“). Router und PC sind über ein Kabel miteinander verbunden. Ist dies nicht der Fall, ist das Netzwerk also kabellos (englisch „wireless“), nennt man es „Wireless Local Area Network“, abgekürzt „WLAN“.

Lastschrift: Als Lastschrift bezeichnet man ein bargeldloses Zahlungsverfahren, bei dem der Verkäufer den Rechnungsbetrag vom Konto des Käufers abbuchen lässt. Der Zahlungsvorgang wird dabei vom Verkäufer ausgelöst und unterscheidet sich hierdurch von der Überweisung, die vom Käufer ausgeht. Voraussetzung für dieses Verfahren ist das Einverständnis des Käufers.

Link: Der Begriff „Link“ leitet sich ab vom englischen Verb „to link“, was „verbinden“ bedeutet. Unter einem Link versteht man einen digitalen (Quer-)Verweis auf eine andere Stelle innerhalb einer Website, auf eine externe Internetseite, auf eine Datei oder eine Anwendung innerhalb des Internets. Links sind deshalb auch zentrale Strukturelemente des Internets.

Mediathek: Mediatheken sind eine Art Onlinebibliothek im Internet, nur dass dort keine Bücher im Regal stehen, sondern Filme, Serien und Reportagen online angeschaut werden können. Viele öffentlich-rechtliche, aber auch private Anbieter haben Mediatheken. Genutzt werden können diese über gängige Geräte wie Laptops, Smartphones oder Tablets. Oft stehen separate Apps für mobile Endgeräte zur Verfügung. Im Unterschied zu Videoportalen werden Mediatheken von der Redaktion eines Senders betreut, gepflegt und auf dem neuesten Stand gehalten. Nutzer*innen von Mediatheken können je nach Anbieter auch Beiträge auf ihre Geräte herunterladen und diese später anschauen. Meistens ist es ihnen aber nicht gestattet, eigene Videos hochzuladen.

NFC (Near Field Communication): Die „Near Field Communication" (zu Deutsch „Nahfeldkommunikation") bezeichnet eine Form der drahtlosen Datenübertragung zwischen zwei Geräten. Diese Funktion wird vor allem bei der Übertragung kleiner Geldbeträge genutzt. So können beispielsweise Geldbeträge von bis zu 25 (oder 50) Euro nur durch Auflegen der Bankkarte auf das Kartenzahlungsterminal übertragen werden, ohne dass die Eingabe der PIN erforderlich ist.

Passwort: Passwörter sind Losungswörter, mit denen der Zugang zu einem bestimmten Bereich im Internet gewährt wird. E-Mail-Konten, Onlinebanking und viele andere Benutzerkonten werden in der Regel mit einem Passwort versehen, damit nicht jede*r darauf zugreifen kann. Passwörter sollten mindestens acht Stellen haben und aus Buchstaben, Sonderzeichen sowie Ziffern bestehen.

PayPal: PayPal ist ein Online-Bezahlverfahren. Beim Online-Einkauf werden direkt vom Bezahldienst Überweisungen vom Käufer- zum Verkäuferkonto vorgenommen. PayPal kann nur verwendet werden, wenn vorher ein Benutzerkonto angelegt und verifiziert wurde.

personenbezogene Daten: Alle Daten, die sich direkt mit einer Person in Verbindung bringen lassen, nennt man personenbezogene Daten. Solche Daten können zum Beispiel der volle Name in Kombination mit der Adresse, der Telefonnummer und den Bankdaten sein. Personenbezogene Daten sind sehr sensible Daten, da sie tiefe Einblicke in die Privatsphäre eines Menschen erlauben.

PIN: Als „**P**ersönliche **I**dentifikations**n**ummer“ wird eine meist vierstellige Ziffernfolge bezeichnet, mit der man sich bei einem Gerät authentisieren kann. PINs werden vor allem zum (Ent-)Sperren von Smartphones sowie in Verbindung mit Bankkarten verwendet.

Profiling: Mit Profiling ist die automatisierte Verarbeitung personenbezogener Daten im Internet gemeint. Dies ermöglicht es, bestimmte Muster im Nutzungsverhalten zu identifizieren, sodass beispielsweise Werbeanzeigen individuell auf die Nutzer*innen zugeschnitten werden können.

Router: Ein Router (zu Deutsch „Verteiler“) übernimmt im Netzwerk die Funktion, eine Internetverbindung auf mehrere Rechner zu verteilen. So ermöglicht er für alle sich im Netzwerk befindlichen Computer einen Zugang zum Internet.

Scoring: Mit „Scoring“ (zu Deutsch „Wertung“) wird eine Methode bezeichnet, mit der die Kreditwürdigkeit von Personen eingeschätzt werden soll. Durch die Analyse relevanter Informationen für die Kreditvergabe soll ein zuverlässigeres Ergebnis erzielt werden. Diese Vorgehensweise kann kritisch betrachtet werden, da die Verwendung und Gewichtung der verwendeten Informationen nicht bekannt sind.

Server: Wie die Bezeichnung „Server“ (zu Deutsch „Diener“ oder „Zusteller“) schon andeutet, liegt die Funktion eines Servers in der Bereitstellung von Daten oder Anwendungen für die Teilnehmer*innen eines Netzwerks wie dem Internet. Dabei kann es sich bei einem Server entweder um einen Computer selbst oder auch nur um ein Programm handeln.

Smartphone: Der auch im deutschen Sprachraum genutzte Begriff „Smartphone“ bedeutet „intelligentes oder geschicktes Telefon“. Die Funktionalität von Smartphones geht dabei weit über die eines reinen Telefons hinaus. Smartphones sind Minicomputer, die die Nutzung von vielen Programmen wie Kalender, E-Mail oder anderen Internetdiensten ermöglichen. Besondere Merkmale der Smartphones sind hochauflösende Displays (Anzeigen), zahlreiche Sensoren wie GPS und die Bedienung über Touchscreen.

Social Community: Social Communitys oder soziale Netzwerke sind die großen Attraktionen im Web 2.0. Sie bieten Menschen einen virtuellen Raum, um sich zu präsentieren und mit anderen zu vernetzen. Mithilfe von Profilen können sich Menschen einer entsprechenden Internetgemeinde vorstellen. Je nach sozialem Netzwerk und den jeweiligen Privatsphäre-Einstellungen können mehr oder weniger Mitglieder der Social Community das persönliche Profil einsehen.

Software: Als Software bezeichnet man Programme wie das Betriebssystem eines Computers, Tablets oder Smartphones. Die Software bildet die Ergänzung zur sogenannten Hardware, also den technischen Bauteilen des Computers, und ist für die Steuerung von Prozessen innerhalb der Komponenten eines Computers zuständig.

soziales Netzwerk: siehe *Social Community*

Tablet: Ein Tablet ist ein internetfähiges Gerät, dessen Größe zwischen Smartphone und Laptop liegt. Der englische Begriff „Tablet" meint im Deutschen einen „Schreibblock" oder eine „kleine Tafel". Für den tragbaren Computer haben sich im deutschen Sprachgebrauch aber auch die Begriffe „Tablet-Computer" und „Tablet-PC" durchgesetzt. Im Vergleich zu Smartphones haben Tablets oft keinen SIM-Karten-Slot und sind damit auf eine WLAN-Verbindung angewiesen, um ins Internet zu gehen. Wer ein Tablet auch mobil nutzen möchte, der sollte darauf achten, ein Gerät mit einem SIM-Karten-Slot für den Zugang zum Mobilfunknetz zu kaufen.

Trojaner: Trojaner sind Schadprogramme, die sich als harmlose, oft auch bekannte Programme tarnen, aber tatsächlich gezielt Daten ausspionieren. Der Begriff „Trojaner" entstammt der Geschichte des Krieges um Troja, in dem das Trojanische Pferd eingesetzt wurde, um Soldaten der Belagerer unbemerkt in die gegnerische Stadt zu schmuggeln.

Update: Bei einem Update wird ein Programm auf den aktuellen Stand gebracht. Hierfür muss in den meisten Fällen das Programm selbst mittels einer Internetverbindung auf einen Rechner der Herstellerfirma zugreifen können, um dort die Version des Programms auf dem

heimischen Computer mit der auf dem Computer des Herstellers abzugleichen und gegebenenfalls zu aktualisieren. Updates sollten regelmäßig vorgenommen werden.

Videotelefonie: Videotelefonie beschreibt den Austausch von Video- und Audiosignalen in Echtzeit. Im Gegensatz zur Nutzung eines Telefons kann man hier nicht nur direkt mit der anderen Person sprechen, sondern diese auch über Video sehen. Voraussetzung für die Nutzung von Videotelefonie ist auf beiden Seiten ein internetfähiges Gerät, welches mit einem Mikrofon und einer Kamera ausgestattet ist, sowie einer Software, die diese Funktion anbietet. Zu den bekanntesten Anbietern solcher Software zählen Skype, Zoom und Microsoft Teams, aber auch Whatsapp und Telegram bieten mittlerweile diese Funktion an.

Webcam: Eine Webcam ist eine Kamera, die, wenn sie an einem PC angeschlossen ist, Bilder direkt ins Internet übertragen kann. Die Bildqualität bei Webcams ist meist nicht sonderlich gut. Dafür ist die Technik mittlerweile sehr günstig und leicht zu bedienen.

WLAN: siehe *LAN*

Autor*innen

Helmut Eiermann ist der stellvertretende Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz und leitet dort den Bereich Querschnittsaufgaben. Er kümmert sich um Fragen zum technischen Datenschutz und der Datensicherheit. Vor seiner Tätigkeit für den Datenschutzbeauftragten war er in der Bundesverwaltung tätig.

Dr. Julia Gerhards arbeitet bei der Verbraucherzentrale Rheinland-Pfalz als Referentin für Verbraucherrecht und Datenschutz. Neben Aufklärung und Information der Verbraucher*innen zu diesen Themen gehört vor allem die politische Interessenvertretung zu ihren Aufgaben. Die Nutzbarkeit digitaler Möglichkeiten bei gleichzeitigem Schutz der Privatsphäre ist dabei eines ihrer Anliegen.

Michael Gundall ist Ingenieur für Medientechnik und arbeitet bei der Verbraucherzentrale Rheinland-Pfalz in der Abteilung Digitales und Verbraucherrecht. Zu seinen Aufgaben gehören die Aufklärung und Information zu technischen Fragen rund um Telekommunikation. Ein weiterer Themenschwerpunkt seiner Tätigkeit sind Fernsehempfangswege.

Maximilian Heitkämper leitet den Fachbereich Digitales und Verbraucherrecht bei der Verbraucherzentrale Rheinland-Pfalz. Bereits im juristischen Studium waren Digitalisierung und wettbewerbsrechtliche Themen sein inhaltlicher Fokus. Zunächst als Rechtsreferent im Projekt Marktwächter Digitale Welt angestellt, übernahm er 2019 schließlich den neu geschaffenen Fachbereich.

Jennifer Kaiser ist Juristin und Rechtsanwältin. Seit Oktober 2010 ist sie bei der Verbraucherzentrale Rheinland-Pfalz tätig. Dort arbeitete sie zunächst als Beraterin in der Beratungsstelle Ludwigshafen mit den Schwerpunkten Telekommunikations- und Verbraucherrecht. Seit Juni 2018 ist sie Fachberaterin im Referat Digitales und Verbraucherrecht.

Impressum

Titel:
Smart Surfer – Fit im digitalen Alltag
Lernhilfe für aktive Onliner*innen

Projektkoordination:
Verbraucherzentrale Rheinland-Pfalz e.V.
Laura Günther
Seppel-Glückert-Passage 10, 55116 Mainz
www.verbraucherzentrale-rlp.de

Lektorat:
WORDS IN FLOW
Julia Gilcher
Schillerplatz 18, 55116 Mainz
www.wordsinflow.de

Gestaltung:
alles mit Medien
Anke Enders
Freiherr-vom-Stein-Straße 10, 55576 Sprendlingen
www.allesmitmedien.de

Bildnachweis:
Cover: Alexander Muth (Bildermuth);
Portrait Dr. Marc Jan Eumann: Stefan Blume;
Portrait Helmut Eiermann: picturepeople Mainz;
Portrait Dr. Julia Gerhards, Michael Gundall,
Maximilian Heitkämper, Jennifer Kaier: Laura Günther

Autor*innen:
Dr. Julia Gerhards, Michael Gundall, Maximilian Heitkämper, Jennifer Kaiser und Miriam Raic von der Verbraucherzentrale Rheinland-Pfalz e.V.; Hannah Ballmann und Fabian Geib von der Stiftung MedienKompetenz Forum Südwest; Anja Naumer und Dr. Florian Tremmel von der Medienanstalt Rheinland-Pfalz; Helmut Eiermann, Timo Göth und Sonja Wirtz als Mitarbeiter*innen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz; Andreas Büsch von der Clearingstelle Medienkompetenz der Deutschen Bischofskonferenz an der KH Mainz.
Ehemalige Autor*innen: Christian Gollner und Barbara Steinhöfel von der Verbraucherzentrale Rheinland-Pfalz e.V.; Christian Wedel und Jeanine Wein, freiberufliche Medienpädagog*innen; Annette Thunemann vom Medienkompetenz Netzwerk Mainz-Rheinhessen.

Dank:
Wir danken unseren Förderern, die ein solches länderübergreifendes Projekt möglich gemacht haben. Unser Dank gilt auch allen weiteren Multiplikatoren, die uns helfen, dieses Wissen an die interessieren Onliner*innen weiterzutragen.
Ein besonderer Dank gilt zudem allen Autor*innen und Interview-Partner*innen, den Coverfoto-Modellen und allen weiteren Unterstützer*innen des Projekts.

Herausgeber:
Bayerisches Staatsministerium für
Umwelt und Verbraucherschutz
Rosenkavalierplatz 2, 81925 München
stmuv.bayern.de

Bezugsadressen:
Bayerisches Staatsministerium für
Umwelt und Verbraucherschutz
Rosenkavalierplatz 2, 81925 München
verbraucherbildung.bayern.de

In Kooperation mit
Bayerische Landeszentrale für neue Medien (BLM)
Heinrich-Lübke-Straße 27, 81737 München
blm.de

Verbraucherzentrale Bayern e.V.
Mozartstr. 9, 80336 München
verbraucherzentrale-bayern.de

VerbraucherService Bayern im KDFB e.V.
Dachauer Str. 5, 80335 München
verbraucherservice-bayern.de

Diese Lernhilfe wurde erstellt von:

verbraucherzentrale Rheinland-Pfalz

medienanstalt rlp LMK

Der Landesbeauftragte für den DATENSCHUTZ und die INFORMATIONSFREIHEIT Rheinland-Pfalz

MKFS MEDIEN KOMPETENZ FORUM SÜDWEST STIFTUNG

Katholische Hochschule Mainz Clearingstelle Medienkompetenz

Das Projekt wurde gefördert durch:

RheinlandPfalz MINISTERIUM FÜR FAMILIE, FRAUEN, JUGEND, INTEGRATION UND VERBRAUCHERSCHUTZ

Bayerisches Staatsministerium für Umwelt und Verbraucherschutz

Baden-Württemberg MINISTERIUM FÜR LÄNDLICHEN RAUM UND VERBRAUCHERSCHUTZ

Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen

LAND BRANDENBURG Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz

LFK: Die Medienanstalt für Baden-Württemberg