Wie man Risiken
im Netz vermeidet

MODUL
04

verbraucherzentrale
Berlin

SMART SURFER
Fit im digitalen Alltag

Lernhilfe für aktive Onliner:innen

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 Rheinland-Pfalz

Der Landesbeauftragte für den DATENSCHUTZ und die INFORMATIONSFREIHEIT Rheinland-Pfalz

MKFS MEDIEN KOMPETENZ FORUM SÜDWEST STIFTUNG

Katholische Hochschule Mainz
Clearingstelle Medienkompetenz

Das Projekt wird gefördert durch:

RheinlandPfalz
MINISTERIUM FÜR FAMILIE, FRAUEN, KULTUR UND INTEGRATION

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

BERLIN
Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung

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

Mehr Informationen zum Projekt „Smart Surfer“ und alle PDF-Dateien zum Download finden Sie unter: *www.verbraucherzentrale-berlin.de/smart-surfer-be*

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: smartsurfer@vz-bln.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 der Verbraucherzentrale Berlin gearbeitet und der Gender-Doppelpunkt (:) genutzt, um alle Leser:innen gleichermaßen anzusprechen.

MODUL 04

Wie man Risiken im Netz vermeidet

Das Internet birgt nicht nur viele Chancen, sondern auch so manches Risiko. So bietet der zunehmende Handel über das Internet leider auch Kriminellen mehr Möglichkeiten. Um sich sicher im Internet zu bewegen, ist es daher wichtig, mögliche Gefahren zu kennen. Wer über seine Rechte und Pflichten auch im Internet Bescheid weiß, kann die vielfältigen Möglichkeiten des Webs selbstbestimmt und verantwortungsvoll nutzen. Ganz nach dem Motto: Auf Basis guter Informationen gute Entscheidungen treffen.

Aber wie schützen Sie sich am besten vor Abzocke im Netz? Wie funktioniert sicheres Onlinebanking? Welche Rolle spielt das Urheberrecht im Internet? Und wie wichtig ist die Verwendung von sicheren Passwörtern? Das und mehr erfahren Sie im Modul 4. Im Interview stellt Ulrike von der Lühe, Vorstand der Verbraucherzentrale Rheinland-Pfalz, wichtige Grundregeln vor, die Sie zur Risikovermeidung beachten sollten.

4.1 Einkaufen im Netz

Onlineshopping ist bei vielen das Mittel der Wahl, wenn es darum geht, schnell etwas zu besorgen. Die Vorteile liegen klar auf der Hand: Das Internet hält ein unendliches Angebot bereit. Zudem sind Onlineshops rund um die Uhr erreichbar. Hinzu kommt, dass der Einkauf im Netz unabhängig von Wetter, Uhrzeit oder dem Wochentag erfolgen kann. Die Lieferzeiten sind oft so kurz, dass der Gang in ein Ladengeschäft kaum weniger Zeit kostet. Kurzum: Onlineshopping ist bequem.

Das neue Smartphone, die neuen Turnschuhe, das Zug- oder Flugticket oder auch die nächste Städtereise lassen sich komfortabel von zu Hause aus kaufen. Außerdem können die Preise vor dem Einkauf miteinander verglichen werden. Zumeist stehen alle Größen und Mengen zur Verfügung. Und das ist gewiss: An der Kasse ist keine Schlange. Auch die verschiedenen Zahlungsmöglichkeiten wie Bezahlen per Lastschrift, Kreditkarte, Onlinebezahlsystem oder Vorabüberweisung sind denkbar einfach. Also steht der Schnäppchenjagd nichts im Wege. Oder doch?

Eine mögliche Situation könnte die Folgende sein:

Ich möchte mir ein Tablet kaufen, um darauf ein E-Paper, also eine Zeitung online zu lesen. Außerdem möchte ich über Videotelefonie in Kontakt mit Familienangehörigen treten können. Mein Laptop ist mittlerweile in die Jahre gekommen, da ist ein Tablet eine gute Alternative. Daher schaue ich mich zunächst in Onlineshops um, lese Kundenrezensionen und vergleiche Herstellerangaben. Schnell muss ich feststellen, dass es eine Vielzahl an Angeboten gibt und die Qualität und Ausstattung der Geräte sich natürlich auch auf den Preis auswirken. Wegen der vielen verschiedenen Ausstattungsmerkmale entschließe ich mich, die Auswahl etwas einzugrenzen, und ziehe Testberichte zurate. Den kostenpflichtigen Test bezahle ich mithilfe eines Onlinebezahldienstes. Dabei bemerke ich: Der Test enthält viele Angaben und jedes Gerät weißt mindestens ein Ausstattungsmerkmal auf, das meinen Kaufkriterien entspricht. Ich muss also weiter recherchieren. Nachdem ich mich nun endlich für ein Gerät entschieden

habe, fange ich an, nach dem besten Preis zu suchen. Dafür nutze ich den Service einer Suchmaschine beziehungsweise verschiedener Vergleichsportale. Auch hier habe ich die Qual der Wahl. Da ich aber nicht um jeden Preis sparen will, berücksichtige ich beim Kauf auch die Seriosität des Händlers sowie der Bezahlweise.

Nachdem ich endlich bestellt und das Tablet nach kurzer Lieferzeit erhalten habe, muss ich feststellen: Der stationäre Händler um die Ecke verkauft ein vergleichbares Gerät ca. 100 Euro günstiger. Nun überlege ich, das bestellte Gerät im Rahmen eines Widerrufs zurückzusenden und das im Einzelhandel sofort verfügbare Gerät zu kaufen. Ein Kauf vor Ort hat zudem den Vorteil, dass ich das Gerät in die Hand nehmen kann. Außerdem kann man sich im Ladengeschäft einmal durch ein paar Anwendungen klicken, um die Handhabung des Geräts direkt zu testen.

Damit man nicht auf vermeintliche Schnäppchen hereinfällt, sollte man vor dem Onlinekauf einige Fragen beantworten. Das gilt vor allem, wenn man den Onlineshop noch nicht kennt.

- Ist das → Impressum vollständig?
- Sind die Preisangaben vollständig?
- Sind alle Lieferkosten, Einfuhrsteuern und Zölle ausgewiesen?
- Wie erfolgt eine eventuelle Rücksendung der Ware und wer hat die Kosten dafür zu tragen?
- Welche Garantien gibt der Händler?
- Kann man sich mit dem Händler kostenlos oder kostengünstig in Verbindung setzen?
- Welche Zahlungsmöglichkeiten gibt es?
- Gibt es einen sicheren Anmeldebereich (mit „https://“ am Anfang der Adresse) für die Eingabe vertraulicher Daten?
- Wie aussagekräftig sind Produktbeschreibungen und Kundenrezensionen?
- Gibt es Qualitätssiegel wie Trusted Shops, TÜV Süd etc.?

Seriosität eines Onlineshops erkennen: https://s.rlp.de/bZWVB

Zudem gibt es sogenannte Fake-Shops, auf denen vermeintliche Produkte angeboten werden und die seriösen Shops täuschend ähnlich sehen.

Österreichische Liste von Fake-Shops: https://s.rlp.de/6W0gQ

Tipp

Die Verbraucherzentralen beraten zu den unterschiedlichsten Themen. Die teilweise auch kostenpflichtigen Beratungen können telefonisch, schriftlich, persönlich und auch per Video-Chat erfolgen. Mehr Informationen: *www.verbraucherzentrale.de/beratung*

Vorsicht bei Bestellungen aus Ländern außerhalb der Europäischen Union: Je nach Warenwert und Sitz des Unternehmens müssen Waren nicht nur zollamtlich abgefertigt werden, sondern es fallen zum Teil auch Zollgebühren oder Steuern an. Die Händler sollten hierauf hinweisen. Eine Rückgabe ist meist wegen der hohen Transportkosten teuer. Reklamationen lassen sich oft nur aufwendig oder gar nicht durchsetzen. Bei Anbietern, die ihr Angebot nicht erkennbar auf Kund:innen in der Europäischen Union ausrichten, gilt ausländisches Recht. Dann haben Verbraucher:innen zum Beispiel kein gesetzliches Recht, den Vertrag zu widerrufen.

Geprüfte Onlineshops

Viele Onlineshops benutzen sogenannte Gütesiegel, die ihre Qualität auszeichnen sollen. Das Siegel findet man meist bereits auf der Startseite, oft in der Fußzeile einer Website. Dabei ist zu beachten: Es gibt kein einheitliches Siegel für Internetshops auf gesetzlicher Basis. Jeder Gütesiegelbetreiber legt den Schwerpunkt auf andere Prüfkriterien und -maßstäbe. Informationen darüber, welche Gütesiegel verlässlich sind, finden sich auf der Website der Initiative D21. Die Initiative ist ein parteien- und branchenübergreifendes Netzwerk von annähernd 200 Mitgliedsunternehmen und -institutionen sowie politischen Partnern aus Bund, Ländern und Kommunen. Ihr Ziel ist es, gemeinnützige wegweisende Projekte auf den Weg zu bringen.

Verlässliche Gütesiegel für Onlineshops: www.initiatived21.de/arbeitsgruppen/guetesiegelboard

Empfohlene Gütesiegel

Seriöse Siegel verfügen über einen verifizierten Link, das heißt, klickt man auf das Siegel, so gelangt man auf die Website des jeweiligen Gütesiegels.

Trusted Shops Das wohl bekannteste Gütesiegel ist das Siegel, welches von der Trusted Shops GmbH für Onlinehändler, Reisebüros und Onlinedienste vergeben wird. Hierfür müssen bestimmte Qualitätskriterien eingehalten werden. Es ist immer für ein Jahr gültig und kann dann nach einer Folgeprüfung jeweils für ein weiteres Jahr geführt werden. Zudem kann Trusted Shops seine Kunden nach eigenem Ermessen darauf überprüfen, ob das Siegel bestimmungsgemäß verwendet wird. Bei Verstoß kann das Siegel entzogen werden.	Nähere Infos: *www.trustedshops.de*
S@fer Shopping Das Siegel wird vom TÜV Süd für Onlineshops in den Bereichen Handel, Touristik und Versicherungen an Shops vergeben, die bestimmte Qualitätskriterien erfüllen. Die Gültigkeit ist unbegrenzt. Es wird jedoch jährlich überprüft, ob die vorgegebenen Kriterien eingehalten werden. Der Händler muss jederzeit damit rechnen, dass unangemeldete Online-Checks erfolgen. Verstößt eine Firma gegen die Kriterien, kann das Siegel entzogen werden.	Nähere Infos: *www.tuvsud.com/de*
EHI Geprüfter Online-Shop Das Siegel wird von der EHI Retail Institute GmbH für den Onlinehandel vergeben. Die Einhaltung der Kriterien wird jährlich überprüft. Bei Beschwerden erfolgt eine Kontrollprüfung. Die Prüfkriterien und -verfahren sind auf der EHI-Webiste beschrieben. Bei Verstoß gegen die Kriterien kann das Siegel entzogen werden.	Nähere Infos: *www.ehi-siegel.de*
internet privacy standards Das Siegel wird von der datenschutz cert GmbH für Onlinedienstleistungen, Gesundheitsanwendungen und Onlinehandel vergeben und ist zwei Jahre gültig. Gegebenenfalls erfolgen Nachzertifizierungen nach einem Jahr, insbesondere bei Veränderungen des Angebots. Bei Verstoß gegen die Kriterien kann das Siegel entzogen werden.	Nähere Infos: *www.datenschutz-cert.de*

Der technische Ablauf eines Einkaufs im Internet

In fast jedem Onlineshop werden die Artikel in einen Warenkorb gelegt. Dazu müssen Artikel meist nur angewählt und markiert werden. Wie im echten Supermarkt symbolisiert oftmals ein Einkaufswagen den Warenkorb. Sind alle Artikel zusammengestellt, kann man mit einem Klick auf den Einkaufswagen den Warenkorb noch einmal ansehen, gegebenenfalls die Mengen anpassen oder Artikel löschen. Im nächsten Schritt gelangt man über einen Link zum Bezahlvorgang.

Internetbestellung:
https://s.rlp.de/7JKTa

In vielen Fällen ist eine Anmeldung erforderlich, wenn man bereits zuvor in diesem Shop eingekauft hat, oder man muss sich mit Name, Anschrift und E-Mail-Adresse registrieren. Seit einiger Zeit ist es auch möglich, sich mit den Nutzerdaten von Onlinediensten wie Google oder Facebook in einem Onlineshop anzumelden – in diesen Fällen fällt eine zusätzliche Registrierung weg und man muss sich kein weiteres Passwort merken. Hier ist jedoch darauf zu achten, dass die Verwendung dieser Onlinedienste die Gefahr birgt, dass Dritte Zugriff auf die Daten erhalten können. Daher ist es ratsam, die Nutzung gezielt, nicht zu oft und nur unter Anwendung sicherer Passwörter für die Anmeldung einzusetzen, um einem Datenklau vorzubeugen. Es gibt jedoch auch Fälle, in denen man nicht extra ein eigenes Benutzerkonto anlegen muss, um den Kauf abzuschließen. Oft reicht die Eingabe der Lieferanschrift und einer E-Mail-Adresse. Aber auch hier sollten natürlich am Ende die Daten überprüft und geschaut werden, ob beispielsweise die richtige Adresse angegeben ist.

Nach Auswahl der Zahlungsmethode, zum Beispiel auf Rechnung, per Kreditkarte, Lastschrift, Vorabüberweisung oder über Bezahldienste wie PayPal oder Klarna, müssen die entsprechenden Angaben dafür eingegeben werden. Über die Auswahl und Verwendung eines solchen Bezahldienstes ist es sogar möglich, die dort hinterlegten Daten, etwa die Versandadresse, in den Bestellvorgang einbinden zu lassen. Danach ist der Einkaufsvorgang beendet.

Möchte man Medikamente im Internet erwerben, sollte man kein Risiko eingehen und vornehmlich Markenware bei seriösen Onlinehändlern oder -apotheken erwerben.

Für Elektronikartikel ist wegen der ständigen Neuerungen neben dem Vergleich von Testergebnissen, Kundenrezensionen und Herstellerangaben auch immer wichtig, das Gerät einmal in echt anzufassen

und auszuprobieren. Verbraucher:innen können Ware aus dem Versandhandel zu Hause prüfen und erhalten den Kaufpreis bei Nichtgefallen zurück. Der Vorteil bei einem Kauf im Einzelhandel vor Ort ist ganz klar, dass Käufer:innen vor dem Kauf eine ausführliche Beratung erhalten können; nicht immer können Onlinetestberichte oder Erfahrungsberichte anderer Verbraucher:innen diese ersetzen.

Für das Buchen von Reisen, ob Pauschal-, All-inclusive-, Abenteuer- oder Städtereisen, bietet das Internet ebenfalls eine Fülle an Seiten. Vergleichsportale von Hotels, Veranstaltern und Reiseservices sind zahlreich vorhanden. Neben den Preisen gibt es hier auch Auskunft über die Qualität der Zimmer, des Essens und des Serviceangebots. Zu beachten ist vor allem das Kleingedruckte, bevor man bucht. Vorsicht: Zu den beworbenen Preisen kommen oft noch Gebühren für Kreditkartenzahlung, Flughafensicherheitsgebühren, Touristenpauschalen, Aufpreise für alternative Flugtermine und vieles Weitere hinzu. Daher sollte man vor dem Abschluss des Buchungsvorgangs genau prüfen, welcher Preis zu zahlen ist und aus welchen Bestandteilen sich dieser zusammensetzt. Auch die Währung des zu zahlenden Preises spielt eine Rolle. Bucht man im Ausland, kann es vorkommen, dass Preise in der jeweiligen Landeswährung angezeigt werden.

Bewertungen und Bewertungsportale

Kaum ein Onlineshop kommt heute ohne ein Bewertungssystem aus. Fast jedes Produkt kann mit Noten und Kommentaren versehen werden. Daneben bestehen selbstständige Bewertungsportale, die Meinungen sammeln.

Solche Bewertungen können vor dem Kauf wertvolle Orientierung geben und scheinen die Spreu vom Weizen zu trennen. Grundsätzlich ist jedoch Vorsicht geboten, denn Manipulationen sind möglich. Wenn jedermann eine Bewertung abgeben kann, können dies auch Konkurrenzunternehmen oder der Hersteller eines Produktes selbst tun. Das Lesen möglichst vieler Bewertungen auf unterschiedlichen Portalen kann das Risiko einer Irreführung zumindest verringern. Vorsicht ist geboten bei überschwänglich lobenden oder stark abschätzigen Bewertungen. Subjektive Meinungen von Privatpersonen stellen keinen Produkttest dar.

Fake-Bewertungen:
https://s.rlp.de/gpscg

Tipp

Wie objektiv sind Vergleichsportale wirklich, und welche Tücken gibt es hier zu beachten? Mehr Wissen zum Thema finden Sie unter: *https://s.rlp.de/BPSTC*

Preisvergleichsdienste

Im Internet finden sich viele Dienste, mit denen Preise für Waren und Dienstleistungen verglichen werden können (zum Beispiel idealo.de, guenstiger.de, geizhals.de, check24.de, billiger.de). Allerdings müssen zusätzliche Kosten beachtet werden: Manche Händler bieten sehr günstige Waren an, verlangen jedoch hohe Preise bei der Versandleistung. Teilweise locken gerade unseriöse Anbieter mit extrem günstigen Preisen. Von außen gar nicht ersichtlich ist, ob bei einer Anfrage tatsächlich alle verfügbaren Angebote aufgelistet werden oder ob es sich um Werbung handelt, die geschaltet wurde. Die Preisvergleichsportale geben keine Garantie auf Vollständigkeit. Ratsam ist deswegen die Preisabfrage bei mehreren unabhängigen Preisvergleichsdiensten. Außerdem zu empfehlen ist ein Blick auf die Preisentwicklung über einen längeren Zeitraum. So kann man anhand der Eingabe des Produktnamens in einen Suchdienst oftmals über eingebundene Ergebnisseiten einen Überblick über die Preise und anbietenden Firmen finden. Aber auch hier gilt, dass man nicht das erstbeste Angebot auswählen, sondern auf die Preisgestaltung und weitere Optionen achten sollte.

Online-Auktionen

Zu guter Letzt kann die Schnäppchenjagd auch in ein Online-Auktionshaus wie Ebay oder Hood.de führen. Hier werden sowohl Neuwaren als auch gebrauchte Gegenstände veräußert. Das Risiko besteht hier vor allem in der subjektiven Beschreibung der Waren und den auf Basis eines Verkäuferbewertungssystems gesammelten Erfahrungswerten anderer Einkäufer:innen. Hier kann trotz positiver Aussagen keine absolute Sicherheit gewährleistet werden, da die Bewertungen immer subjektiv sind. Andererseits müssen Negativbewertungen nicht zwangsläufig dem Versagen des Verkäufers geschuldet sein.

Ein weiteres Risiko: Auktionen verleiten oft zum Mitbieten über das eigene Limit hinaus. So kommen schnell für ein gebrauchtes Produkt plus Versandkosten Summen nahe dem Neupreis zustande. Wer umsichtig bleibt, der kann trotz der genannten Risiken im Online-Auktionshaus erfolgreich einkaufen.

Schließlich sollte man noch auf Folgendes achten: Handelt es sich um gewerbliche Anbieter oder wird die Ware im Rahmen eines Privatverkaufs veräußert? Gerade im letzteren Fall greifen dann nämlich das gesetzliche Widerrufsrecht oder Gewährleistungsansprüche nicht.

Die gesetzliche Widerrufspflicht gilt nicht bei Privatverkäufen.

Zahlungsmöglichkeiten im Internet

Anders als in einem Ladengeschäft kann bei Einkäufen im Internet nicht bar bezahlt werden. Grundsätzlich haben die Kund:innen kein Recht, eine bestimmte Zahlungsart zu verlangen, die meisten Shops bieten jedoch Alternativen an. Über die Wahl der Zahlungsart lassen sich aber bereits viele Risiken vermeiden. Die am häufigsten angebotenen Zahlungsmöglichkeiten sind:

- Rechnung,
- Lastschrift nach Erteilung einer ➔ Einzugsermächtigung,
- Vorkasse mit Kreditkarte, mittels Überweisung oder über einen ➔ Zahlungsauslösedienst wie zum Beispiel Sofortüberweisung, jetzt Klarna Sofort,
- Vorkasse über einen Internetbezahldienst wie zum Beispiel PayPal, Klarna Rechnung, Apple Pay, Google Pay, pay direkt usw.
- oder Nachnahme.

Am sichersten ist die Bezahlung per Rechnung oder die Erteilung einer Einzugsermächtigung. Ist die Ware fehlerhaft oder bekommt man erst gar keine geliefert, muss man so seinem Geld nicht hinterherlaufen. Im Falle der Rechnung wird nur dann gezahlt, wenn die Ware in Ordnung ist. Bei der Einzugsermächtigung kann dem Bankeinzug innerhalb von acht Wochen ab der Kontobelastung bei der (eigenen) Bank widersprochen werden; das kontoführende Kreditinstitut holt den Betrag dann zurück.

Anders ist dies bei Vorkasse durch Überweisung oder Zahlung mit Kreditkarte. In diesen Fällen ist das Geld bereits vor Erhalt der Ware weg. Wenn den Kund:innen die Ware nicht gefällt, müssen sie die

bereits erfolgte Zahlung zurückfordern. Werden gestohlene Kreditkartendaten missbraucht, wird der Schaden nach Meldung bei der kartenausgebenden Bank ausgeglichen.

Eine Besonderheit stellt die Überweisung mit dem Dienst Sofortüberweisung dar. Dieser Dienst erleichtert die Nutzung des eigenen Onlinebanking-Zugangs. Aus der Seite eines Onlineshops heraus werden Kunden zur Eingabe einer PIN/TAN-Kombination außerhalb des Systems der gewählten Bank aufgefordert, um eine Überweisung im Onlinebanking anzustoßen. Die Nutzer:innen sollten vor dem Verwenden dieses sogenannten Zahlungsauslösedienstes (PSD2) vorab klären, ob die eigene Bank im Falle eines Missbrauchs haftet, wenn PIN und TAN außerhalb des jeweiligen Banksystems verwendet werden. In diesem Fall weigert sich das Institut nämlich möglicherweise, den Schaden zu übernehmen. So hätten die Kund:innen den Schaden selbst zu tragen. Auch sollte beachtet werden, dass es sich hier nicht um eine Zahlungsweise als solche, sondern um einen sogenannten Drittdienst handelt. Der Vorteil dieses Angebots liegt darin, dass der Händler zwar nicht sofort die Zahlung erhält, zumindest aber die Bestätigung durch den Drittdienstanbieter, dass die Zahlung vorgenommen wurde.

Tipp

Zahlungsauslösedienste nehmen Überweisungen zulasten eines Bankkontos vor. Dabei werden durch die Inhaberin oder den Inhaber des Kontos einem Drittdienst die Rechte zur Nutzung des Onlinebankings bei ihrer beziehungsweise seiner Bank eingeräumt. Mittels des PSD2-Verfahrens wird der Zugriff des Drittdiensts auf die Kontodaten beschränkt. Zudem gilt: Ohne Zustimmung der Kontoinhaber:innen darf keine Zahlung ausgeführt werden.

Nachnahmesendungen reduzieren zwar das Risiko, können aber auch nicht vollständig vor Betrügereien schützen. Ob die bestellte Ware tatsächlich im Paket ist, kann man vor der Annahme nicht mit Sicherheit feststellen. Daher sollte man nach Möglichkeit per Rechnung nach Erhalt der Ware oder per Lastschrift bezahlen, vor allem, wenn man erstmalig bei einem Händler bestellt und noch keinerlei Erfahrungen hinsichtlich seiner Zuverlässigkeit vorliegen.

Internetbezahldienste wie PayPal, Klarna oder ClickandBuy stellen eine weitere und verbreitete Art des Geldtransfers dar. Für die Nutzung ist eine vorherige Anmeldung bei dem jeweiligen Dienst nötig. Hier lassen sich Zahlungsmittel wie Kreditkarte oder Girokonto hinterlegen, ohne dass man die Daten dann beim Einkauf auf einer Website angeben muss. Bei der Abwicklung des Onlinekaufs wird man vom Onlineshop auf die Seite des Bezahldienstes weitergeleitet und kann die Zahlung darüber abwickeln lassen. Der Bezahldienst belastet dann die im Benutzerkonto hinterlegten Zahlungsmittel. Gibt es ein Problem bei der Bestellung, kann man über den sogenannten Käuferschutz eine Klärung anstoßen. Aber Vorsicht: Bei Problemen im Rahmen der Ausübung des Widerrufs oder von Gewährleistungsrechten hilft der Käuferschutz meist nicht. Im Falle einer Rücksendung können diese Dienste auch die Zahlung aussetzen oder die Rückzahlung darüber abwickeln lassen.

Der Vorteil von Internetbezahldiensten liegt in der Tatsache, dass beim Bezahlen keine Konto- oder Kreditkartendaten unmittelbar an den Verkäufer weitergegeben werden müssen. Ein Missbrauch dieser Bezahlmethode ist dennoch nicht auszuschließen. Kriminellen gelingt es immer wieder, Zugangsdaten abzugreifen und illegal zu nutzen. Aber wer sich gut über die Bezahlverfahren informiert hat, sichere Passwörter verwendet und regelmäßig seine Bezahlvorgänge kontrolliert, kann den Komfort der Internetbezahlverfahren gut nutzen. Ein Risiko besteht jedoch immer, ähnlich wie auch bei der Geldbörse, die einem auf der Straße aus der Tasche geklaut werden könnte.

Grundsätzlich ist beim Zahlen im Netz zu beachten, dass der Einsatz der unterschiedlichen Bezahlverfahren mit Zusatzentgelten verbunden sein kann. Unternehmen müssen Kund:innen jedoch immer zumindest eine verbreitete Bezahlmethode anbieten, die ohne Zusatzkosten genutzt werden kann. Im Übrigen dürfen als Zusatzentgelt nur jene Kosten berechnet werden, die einem Unternehmen für eine Zahlung tatsächlich von dem Anbieter des Bezahlsystems in Rechnung gestellt werden.

Mögliche Zusatzentgelte für Zahlungsmittel

Beispielshop 24

Warenpreis	129,95 €
Geschenkverpackung	2,95 €
Versandkosten	4,95 €
Zahlungsmittelentgelt	
Summe	

Überweisung:	kostenfrei
PayPal:	+ 1,50 €
Kreditkarte:	+ 1,50 €
Sofortüberweisung:	+ 1,50 €

Wie für die Informationsbeschaffung gelten auch für Einkäufe im Netz zusammenfassend folgende Prinzipien:

- **Misstrauensprinzip:** Ein Händler muss sich das Vertrauen der Kundschaft erst verdienen.
- **Vielquellenprinzip:** Je häufiger eine gute oder schlechte Bewertung auftritt, desto wahrscheinlicher ist ihr Wahrheitsgehalt.
- **Ergänzungsprinzip:** Eine Internetseite ist gut geeignet für die Erstinformation. Diese sollte aber bestätigt werden durch Printprodukte, zum Beispiel durch Testberichte, oder durch Beratung im Einzelhandel.
- **Kontrollprinzip:** Bestimmte Informationen sollte man immer kontrollieren: Stimmt die Webadresse in der Adresszeile? Sind alle Fragen zum Online-Einkauf in Bezug auf den Händler positiv beantwortet? Gibt es sonstige Hinweise auf seine Seriosität (zum Beispiel Gütesiegel)?

4.2 Abzockmaschen

Vor allem in den vergangenen Jahren hat man häufig davon gehört: Im Internet locken Seiten mit angeblichen Nachrichten von Nachbar:innen, andere ködern mit Routenplanung, Computerprogrammen, Intelligenztests oder Rezeptvorschlägen. Mit solchen vermeintlich kostenlosen Webangeboten zogen zweifelhafte Firmen neugierigen Nutzer:innen das Geld aus der Tasche. Inzwischen wurde auf Basis der Gesetzgebung versucht, viele dieser illegalen Aktivitäten einzudämmen. Dennoch finden Kriminelle wie in allen Bereichen auch im Internet immer Mittel und Wege, ihr Treiben fortzusetzen. Für Internetnutzer:innen bedeutet das: Kennt man die Maschen unseriöser Anbieter, kann man sie eher durchschauen.

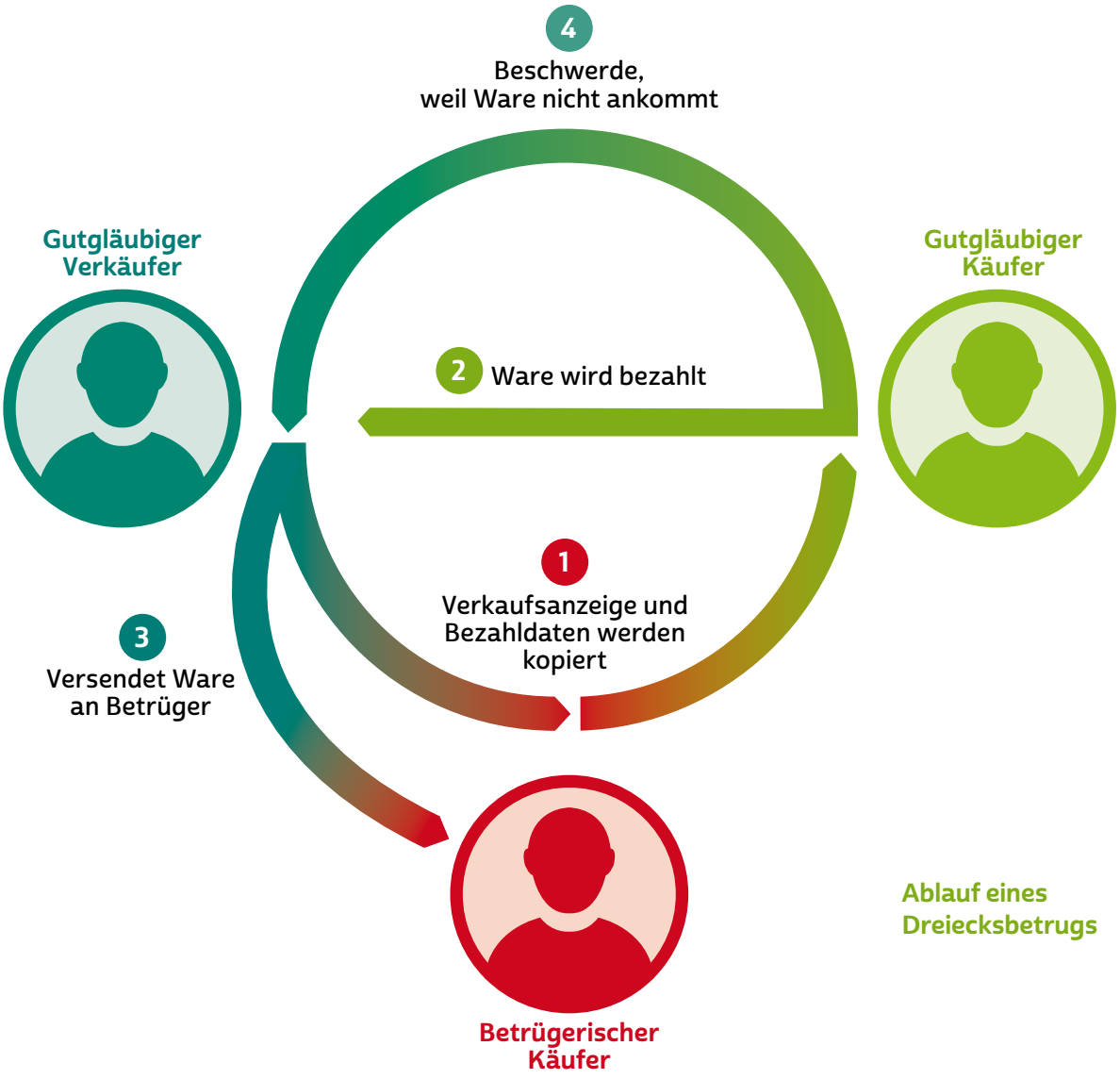
- **Großhandelsportale**
  Seit einiger Zeit fallen Verbraucher:innen auf Internetangebote herein, die sich nur an Gewerbetreibende (Business-to-Business, kurz B2B oder B-to-B) richten. Die Seiten sind häufig so gestaltet, dass sie auch private Internetnutzer:innen ansprechen. Oft werden Betroffene über eine Werbeanzeige auf die Seiten dieser Anbieter gelockt. Dabei kann man anhand der Anzeige nicht erkennen, dass sie auf die Seite einer Großhandelsplattform führt. Bei einer Anmeldung auf diesen Portalen entstehen Kosten für eine Jahresmitgliedschaft von zum Teil mehreren Hundert Euro. Die Anbieter bestehen häufig auf Zahlung, weil die Verbraucher:innen angeblich bei ihrer Anmeldung eine Täuschung in Bezug auf ihren Status begangen haben und somit kein Widerrufsrecht bestehe.

- **Köder-Gewinnspiele**
  Ein weiterer Köder sind Sach- und Geldgewinne, die auf der Internetseite angekündigt werden. Um den versprochenen Gewinn zu erhalten, gibt man seine echten persönlichen Daten an, wie beispielsweise Name, Anschrift und E-Mail, zusätzlich oft noch Alter und Geschlecht. Meist dienen diese Gewinne zum einen dazu, von entstehenden Kosten abzulenken, zum anderen kommen die Betreiber:innen so an personenbezogene Daten, um sie zu Werbezwecken zu verwenden oder an Dritte weitergeben zu können.

- **Dreiecksbetrug**
  Gerade auf Verkaufsplattformen wie Ebay Kleinanzeigen muss man sich vor Abzockmaschen in Form eines Dreiecksbetruges schützen, insbesondere, weil der Polizei und den Staatsanwaltschaften oftmals in ihren Ermittlungen die Hände gebunden sind. Hier ein Beispiel für einen typischen Ablauf: Ein argloser Verkäufer bietet einen Artikel zum Verkauf an und einigt sich mit einer Käuferin, die insgeheim betrügerische Absichten hegt. Der Verkäufer leitet seine PayPal-Daten weiter, auf seinem Konto geht der Betrag ein. Schließlich wird die Ware übergeben oder versendet. Kurz darauf wird der ahnungslose Verkäufer mit dem Vorwurf des Betruges konfrontiert.

    Denn die Käuferin hat dessen PayPal-Daten und das ursprüngliche Verkaufsangebot missbraucht, um eine inhaltsgleiche Anzeige zu schalten. Dem zweiten, ebenfalls ahnungslosen Käufer gibt sie die PayPal-Daten des ursprünglichen Verkäufers durch, sodass dieser die Verbindlichkeit der betrügerischen Käuferin beim ersten Verkäufer begleicht, ohne es zu wissen. Die Ware wird er nie erhalten, da sich diese inzwischen bei der betrügerischen Käuferin befindet.

    Der ursprüngliche Verkäufer ist in diesem Fall doppelt betroffen, da er sowohl die Ware bereits versandt hat als auch den gezahlten Betrag an den zweiten Käufer zurückzahlen muss, da er diesen ohne Rechtsgrund erhalten hat. Die Identität der betrügerischen Käuferin wird sich in den meisten Fällen nicht mehr aufklären lassen. Auch der Portalbetreiber Ebay Kleinanzeigen sieht für sich keine Möglichkeit, gegen diese Betrugsmasche vorzugehen.



Ablauf eines Dreiecksbetrugs

Tipp

Bei einer persönlichen Übergabe der Ware kann man diesen Tricks von Internetkriminellen entgehen. Dabei kann der Preis für die Ware außerdem ohne Zwischenschritt bar bezahlt werden. Wer unsicher ist beim Vereinbaren eines Termins, der fragt am besten im Familien- und Bekanntenkreis, ob jemand zur Unterstützung zusätzlich anwesend sein kann.

- **Umgehung des Käuferschutzes**
  Auch PayPal selbst kann gerissenen Betrüger:innen eine geeignete Plattform bieten. Diese nutzen aus, dass man zwischen zwei verschiedenen Bezahlmethoden, „Geld senden für Waren und

Dienstleistungen“ oder „Geld an Freunde und Familie senden“, wählen kann. Wählt man die zweite Alternative, fallen zwar keine PayPal-Gebühren von 1,9 % an, jedoch wird auch weder ein Schutz der Käufer:innen noch der Verkäufer:innen durch die Plattform gewährt. Kommt es in diesem Fall zu einem Ausfall oder anderen Unregelmäßigkeiten, wird dies nicht durch PayPal erstattet.

Tipp

Schlägt Ihnen ein:e gänzlich unbekannte:r Vertragspartner:in die Bezahlung „an Freunde oder Familie“ vor, ist Vorsicht geboten. Halten Sie auf jeden Fall Ausschau nach weiteren Warnsignalen.

- **Fehlendes oder unvollständiges Impressum**
  Gewerblichen Websites ohne Impressum sollte man generell nicht vertrauen. Aber auch wenn ein Impressum angegeben ist, schützt das nicht vor Abzockmaschen. Hinter den Adressen unseriöser Anbieter stecken häufig lediglich Briefkastenfirmen, hinter Telefonnummern Bandansagen. Oft schließen diese Seiten nach kurzer Zeit und werden unter leicht geändertem Namen und mit neuem Impressum fortgesetzt. Hier ist es ratsam, sich über den Anbieter mittels einer Suche im Internet zu informieren und seine tatsächliche Existenz zu überprüfen. Misstrauisch werden sollte man vor allem, wenn Adressen im Ausland angegeben werden. Beliebte Standorte unseriöser Seitenbetreiber sind Großbritannien samt (ehemaliger) Kolonien wie zum Beispiel die British Virgin Islands, aber auch die Arabischen Emirate oder die Schweiz.

- **Ungenügender Kostenhinweis**
  Früher versuchten dubiose Anbieter durch versteckte Preisangaben, Kund:innen in die Irre zu führen, um an ihr Geld zu gelangen. Das ist heute nicht mehr erlaubt.

Generell müssen Unternehmer:innen den Bestellvorgang so gestalten, dass die Verbraucher:innen die Zahlungspflicht dabei ausdrücklich bestätigen müssen. Dies ist die sogenannte „Button-Lösung“, zu Deutsch „Schaltflächen-Lösung“. Erfolgt die Bestellung über eine

Schaltfläche, ist die gesetzliche Regelung nur erfüllt, wenn diese Schaltfläche gut lesbar mit nichts anderem als den Worten „zahlungspflichtig bestellen“ oder mit einer entsprechenden eindeutigen Formulierung, wie nachfolgend abgebildet, beschriftet ist:

Dabei muss für Verbraucher:innen deutlich werden, dass der Klick mit Kosten verbunden ist. Nur wenn eine solche Schaltfläche bei der Bestellung angezeigt und durch die Kundin oder den Kunden explizit bestätigt wurde, ist die Erklärung der Kundin oder des Kunden als rechtswirksam anzusehen. Andernfalls kann kein Vertrag zustande kommen.

Darüber hinaus müssen alle nötigen Pflichtinformationen, auf deren Grundlage die Verbraucher:innen ihre Kaufentscheidung treffen, auf eine klar verständliche und optisch hervorgehobene Weise dargestellt werden. Dies umfasst Produktmerkmale, Mindestlaufzeit, Gesamtpreis, Versand- und Zusatzkosten. Diese müssen in unmittelbarem, direktem zeitlichen Zusammenhang vor dem eigentlichen Bestell-Button angezeigt werden.

Unklare Beschriftungen wie „Anmeldung“ oder „Weiter“ genügen den Anforderungen nicht. Auch Formulierungen wie „bestellen“ oder „Bestellung abgeben“ sind nicht geeignet.

Tipp

Verwenden Onlineshops einen falschen Kauf-Button, kann keine Zahlung verlangt werden.

Auch langatmige oder umständliche Formulierungen dürfen nicht von der Tatsache ablenken, dass es für Verbraucher:innen darum geht, eine rechtliche Verbindlichkeit einzugehen. Fällt man auf fragwürdige und nicht gesetzeskonforme Angebote herein, kommt rechtlich gesehen kein wirksamer Vertrag zustande. Der Grund: Werden die Kosten für die Informationen oder Dienste verschleiert, hatte die Nutzerin oder der Nutzer beim Absenden der Bestellung nicht die Absicht, einen kostenpflichtigen Vertrag einzugehen.

Tipp

Rechnungen von Internetabzockern sollten Sie nicht ungeprüft zahlen. Wenden Sie sich im Zweifel beispielsweise an die Verbraucherzentrale. Die Verbraucherzentrale berät auch zum Thema Einkaufen im Netz: *http://s.rlp.de/NkHf2*

§

Vergleiche § 2 Preisangabenverordnung (PAngV)

Preisangaben sind gesetzlich geregelt. Der Preis muss nach dem Grundsatz der Preisklarheit und der Preiswahrheit leicht erkennbar und deutlich lesbar oder gut wahrnehmbar sein. Außerdem müssen sich der Preis und alle seine Bestandteile in unmittelbarer räumlicher Nähe zum Angebot oder zur Werbung befinden oder sich auf anderem Wege direkt dem Angebot zuordnen lassen.

Wer auf ein irreführendes Angebot hereingefallen ist, kann in vielen Fällen von seinem 14-tägigen Widerrufsrecht Gebrauch machen und schriftlich vom Vertrag zurücktreten. Ist man sicher, dass es sich um Internetabzocke handelt, sollte man den Zahlungsaufforderungen per E-Mail und Brief sowie darin enthaltenen Drohungen des entsprechenden Unternehmens nicht nachkommen und nicht sofort bezahlen. Die Verbraucherzentrale rät, unberechtigte Forderungen sicherheitshalber schriftlich abzuwehren und die Forderung zu bestreiten, und stellt dafür Musterbriefe zur Verfügung. Auch wer bei einer Forderung mit Mahnungen und Schreiben von Inkassobüros oder Rechtsanwält:innen überhäuft wird, sollte sich auf keinen Fall einschüchtern lassen. Wird jedoch ein Mahnbescheid von einem Amtsgericht zugestellt, muss man unbedingt reagieren und innerhalb von zwei Wochen der Geldforderung auf dem beiliegenden Widerspruchsformular offiziell widersprechen. Denn auch wenn bereits ein Mahnbescheid zugestellt worden ist, gibt dies noch keine Anhaltpunkte auf die Erfolgsaussichten. Die Rechtspflegerin oder der Rechtspfleger bei Gericht, die oder der den Mahnantrag bearbeitet, überprüft diesen nicht auf seinen Inhalt, sondern nur auf das Vorliegen formaler Erfordernisse.

Tipp

Die Verbraucherzentralen bieten Unterstützung im Umgang mit Abzocke im Netz. Musterbriefe finden Sie unter: *https://s.rlp.de/pH2vf*

Außerdem bieten die Verbraucherzentralen Web-Seminare zu verschiedenen Themen wie Anbieterwechsel oder dem Umgang mit dem Smartphone an. Zu den Seminaren der Verbraucherzentrale Rheinland-Pfalz gelangen Sie unter: *www.verbraucherzentrale-rlp.de/webseminare-rlp*

Weitere Erkennungsmerkmale einer Website mit betrügerischem Inhalt können eine auffällige Internetadresse, ein auffallend günstiger Preis, ein falsches Gütesiegel, sehr positive Kundenbewertungen oder frei erfundene, grammatikalisch falsche oder kopierte AGB sein.

Auffällig ist eine Internetadresse, wenn sie statt auf ein simples „.de“ auf „de.com“ endet oder in der Internetadresse ein ganz anderes Schlagwort steht, als der Inhalt der Seite behandelt. Auch ein ungewöhnlich niedriger Preis sollte nicht einen zusätzlichen Kaufanreiz setzen, sondern eher stutzig machen. Gefälschte Gütesiegel lassen sich recht schnell mit einem Klick auf das Symbol aufdecken. Öffnet sich daraufhin keine Seite zu einem echten Gütesiegel wie etwa Trusted Shops, dürfte es sich um eine Fälschung handeln. Häufen sich sehr positive Bewertungen von Kund:innen, die in ihren Inhalten jedoch unbestimmt und oberflächlich bleiben, beziehungweise stehen diese positiven Bewertungen in einem krassen Gegensatz zu übereinstimmenden negativen Bewertungen, muss deren Glaubwürdigkeit zumindest angezweifelt werden. Es besteht die Gefahr, dass die positiven Bewertungen gekauft worden sind.

Wenn man dennoch auf eine Abzockmasche hereingefallen ist, sollte zunächst so schnell wie möglich der Kontakt zur eigenen Bank gesucht werden, um die Zahlung nach Möglichkeit noch zu stoppen. Darüber hinaus sollten alle schriftlichen oder elektronischen Unterlagen, die im Rahmen des Falles entstanden sind, aus Beweisgründen gesichert werden. Hierzu zählen auch die Chatverläufe mit den Betrüger:innen und alles, was zur Identifizierung der Täter:innen führen kann.

4.3 Rechte der Verbraucher:innen

Im Internet müssen Verbraucher:innen vor dem versehentlichen Abschließen von kostenpflichtigen Verträgen besonders geschützt werden. Insbesondere im Rahmen der Button-Lösung muss eine Bestellung stets ausdrücklich bestätigt werden. Dies ist insbesondere dann wichtig, wenn es sich um eine kostenpflichtige Bestellung handelt.

Wurde eine Bestellung getätigt, kommt es für die Verbraucher:innen schließlich auch darauf an, dass ihnen der Kauf durch die Gegenseite bestätigt wird. Dies geschieht beispielsweise durch den Erhalt einer E-Mail, die auf die Bestellung folgt, oder aber durch die Tatsache, dass man eine Leistung sofort nutzen kann, zum Beispiel ein Streamingangebot oder eine App.

Der Fernabsatzvertrag

Widerrufsrecht §§ 355 ff. BGB

Kauft man Waren über das Internet ein oder beauftragt darüber Dienstleistungen wie zum Beispiel einen Telefonanschluss, schließt man einen sogenannten Fernabsatzvertrag ab. Die Regeln zum Fernabsatzgeschäft finden sich im Bürgerlichen Gesetzbuch in den Normen der §§ 312 b ff. BGB.

Informationspflichten § 312i ff. BGB; Art. 246, 246a

Mit Fernabsatzverträgen sind einige verbraucherschützende Regelungen verbunden, die bei einem Einkauf im Handel vor Ort so nicht gelten. Hierüber herrscht bei den Verbraucher:innen oftmals Verwirrung. So gilt im Unterschied zum stationären Händler bei Fernabsatzverträgen in der Regel das sogenannte Widerrufsrecht. Zudem müssen durch die Anbieter zusätzlich besondere Informationspflichten eingehalten werden. So muss das Angebot zum Beispiel über die wesentlichen Eigenschaften der Ware oder Dienstleistung und den Gesamtpreis informieren.

Gerade für Verträge, die im Rahmen des Fernabsatzes geschlossen werden, gelten hier dann enger gefasste Regeln:

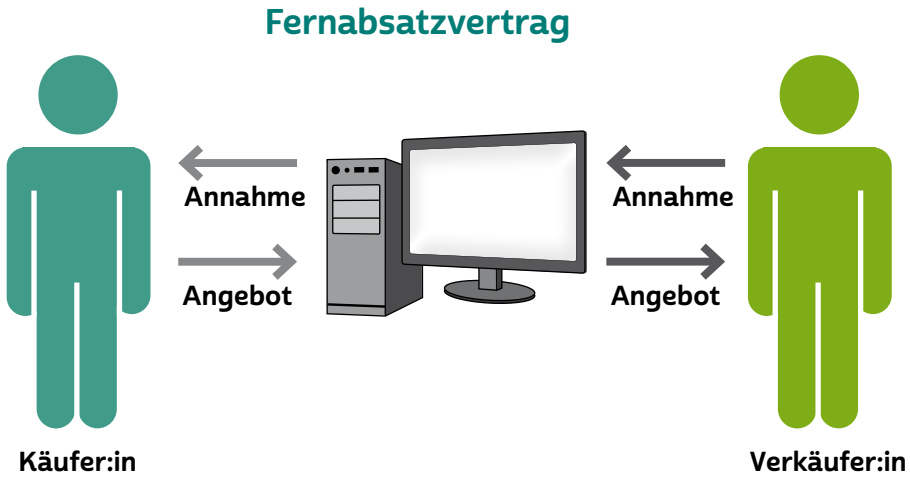
- Wurde der Vertrag außerhalb eines Ladengeschäfts geschlossen, müssen alle Informationen klar und verständlich zur Verfügung gestellt worden sein. Dies kann auf Papier oder nach Zustimmung zum Beispiel auch per E-Mail erfolgen.

- Wurde die Bestellung online vorgenommen, müssen die Informationen auch auf der Website des Anbieters einseh- und verfügbar sein.

- Nach erfolgter Bestellung müssen die Kund:innen hierüber eine Information erhalten.

Voraussetzung für einen Fernabsatzvertrag ist das Handeln eines Unternehmens auf der einen und eines Kunden oder einer Kundin auf der anderen Seite. Ausgeschlossen von den Regelungen des Fernabsatzes sind Verträge zwischen Privatpersonen. Gerade auf Auktionsplattformen wie eBay oder Portalen für (private) Kleinanzeigen tummeln sich vor allem private Verkäufer:innen. Bei solchen Geschäften sind Verbraucher:innen weniger geschützt, insbesondere kann die Gewährleistung ausgeschlossen sein und es gilt auch kein Widerrufsrecht.

Ein Fernabsatzvertrag kommt nur dann zustande, wenn sowohl die Vertragsverhandlungen als auch der Vertragsschluss ausschließlich über Fernkommunikationsmittel, also mittels Internet oder per Briefpost, Telefax, SMS oder Telefon erfolgen. Außerdem gelten die Regeln nur, wenn der Anbieter seine Waren oder Dienstleistungen regelmäßig auf diese Weise anbietet. So kommt kein Fernabsatzvertrag zustande, wenn man eine Ware stationär erwirbt, beispielsweise ein Brot beim Bäcker oder Hygieneartikel im Drogeriemarkt.



Wie ein Fernabsatzvertrag zustande kommt

Das Widerrufsrecht

Wie bereits erwähnt, unterscheiden sich der stationäre Handel und der Onlinekauf in einigen Punkten. Anders als im Laden vor Ort kann man die Ware oder Dienstleistung, die man im Internet bestellt, nicht vor dem Kauf prüfen. Deswegen erhalten Verbraucher:innen bei Fernabsatzverträgen per Gesetz ein 14-tägiges Widerrufsrecht. Mithilfe des Widerrufsrechts kann man sich innerhalb dieser Frist von einem Vertrag lösen, ohne dass hierfür ein Grund angegeben werden muss. Es ist dabei jedoch zu beachten, dass der Händler von den Verbraucher:innen trotz Ausübung ihres Widerrufsrechtes einen Wertersatz verlangen kann, etwa dann, wenn die Prüfung des Artikels über das Notwendige hinausging. Dabei handelt es sich um eine Einzelfallprüfung. Die meisten Vertragsabschlüsse über das Internet fallen unter diese Regelung, es gibt jedoch auch Ausnahmen. So werden von den Regelungen des Widerrufsrechts bestimmte Gruppen von Waren oder Leistungen ausgenommen, wie beispielsweise folgende Bereiche:

§

Ausnahmen in § 312g Abs. 2 BGB

- Reiseleistungen, zum Beispiel Pauschalreisen oder Unterkünfte
- Beförderung von Personen, zum Beispiel Flugtickets, Bahnfahrscheine, Mietwagen
- Freizeitveranstaltungen, zum Beispiel Konzerttickets
- medizinische Behandlungen wie zahnärztliche Versorgung oder Rehabilitationsleistungen
- Lieferdienste für Lebensmittel, Getränke oder Haushaltsgegenstände des täglichen Bedarfs (Stichwort „Pizzataxi“)
- Waren, die schnell verderben können oder deren Mindesthaltbarkeitsdatum schnell überschritten wird
- Waren, die für Kund:innen nach eigenen Wünschen individuell angefertigt werden

- versiegelte Waren, die aus Gründen des Gesundheitsschutzes oder der Hygiene nicht zur Rückgabe geeignet sind, wenn das Siegel gebrochen wurde

- versiegelte Ton- oder Videoaufnahmen oder Computersoftware

- Lieferung einzelner Zeitungen, Zeitschriften oder Illustrierter außerhalb von Abonnements

Beispiel: Eine Frau bestellt im Onlineshop einen Lippenstift. Dieser kommt versiegelt an. Als sie ihn testet, stellt sie fest, dass die Farbe nicht zu ihr passt, und möchte den Lippenstift zurückschicken. Als sie gegenüber dem Händler ihre Rücksendung anmelden möchte, widerspricht der Händler. Aus hygienischen Gründen versiegelte Waren – hierzu gehören auch Kosmetika – sind vom Widerrufsrecht ausgenommen.

§
Widerrufsrecht
§ 312g Abs. 2 Nr. 3 BGB

Die Frist, in der ein Widerruf erklärt werden muss, beträgt 14 Tage. Sie beginnt bei Warenlieferung mit Erhalt der Ware, bei Dienstleistungen ab der Belehrung über das Widerrufsrecht. Über das Widerrufsrecht müssen Verbraucher:innen bei jedem Vertragsschluss in verständlicher Form informiert werden. Erfolgt keine ausdrückliche Information über das zustehende Widerrufsrecht, verlängert sich die Widerrufsfrist auf ein Jahr und 14 Tage.

Beispiel: Ein Mann erhält am 1. Juli 2020 eine Zahlungserinnerung für einen Vertrag, den er angeblich am 21. Juni 2019 online abgeschlossen hat. Er kann sich aber an einen solchen Vertragsschluss nicht erinnern. Er hat auch keine Bestellbestätigung erhalten, weder per Post noch per E-Mail. Also entschließt er sich, der Forderung zu widersprechen und das Geld nicht zu zahlen. Für online abgeschlossene Verträge gilt: Sofern die Belehrung über das den Käufer:innen im Rahmen des Fernabsatzvertrages zustehende Widerrufsrecht ausgeblieben ist, besteht eine Widerrufsfrist von einem Jahr und 14 Tagen. Deswegen kann er den angeblichen Vertrag nun schriftlich widerrufen.

§
Widerrufsfrist
§ 356 Abs. 3 S. 2 BGB

Für die Einhaltung der Frist genügt es, dass die Widerrufserklärung innerhalb der Frist abgeschickt wurde. Verbraucher:innen müssen die Widerrufsbelehrung in Textform erhalten. In der Regel geschieht das durch Zusendung der Belehrung als E-Mail.

Tipp

Verträge, die Sie über das Internet abgeschlossen haben, können Sie in aller Regel innerhalb einer Frist von 14 Tagen widerrufen.

Eine Besonderheit besteht beim Streaming und beim Herunterladen von Software, zum Beispiel Apps für das Smartphone. In diesen Fällen besteht zwar grundsätzlich ein Widerrufsrecht, die Anbieter haben jedoch die Möglichkeit, es auszuschließen. Bevor die Leistung erbracht wird, muss man am Gerät bestätigen, dass man auf das Widerrufsrecht verzichtet. Erst dann kann die Leistung in Anspruch genommen werden. Bei anderen digitalen Dienstleistungen können Anbieter ebenso verfahren.

Wer einen Vertrag widerrufen will, muss dies dem Anbieter ausdrücklich mitteilen. Das bloße Zurücksenden einer Ware oder die Verweigerung der Paketannahme sind dazu nicht ausreichend. Diesbezüglich hat sich eine langjährige Rechtslage mit einer Gesetzesreform im Sommer 2014 geändert. Die Erklärung kann formlos erfolgen oder mithilfe des Widerrufsformulars. Dieses ist einer Warensendung beigelegt oder kann von der Internetseite des Onlineshops heruntergeladen werden. Der Widerruf kann über E-Mail, Telefax, Brief oder sogar telefonisch erklärt werden. Letzteres ist aus Beweisgründen aber nicht zu empfehlen.

Wurde der Widerruf erklärt, ist die Ware an den Händler zurückzusenden. Die Kosten für die Rücksendung können den Verbraucher:innen vom Händler vollständig auferlegt werden. Zahlreiche Unternehmen verzichten jedoch darauf und gestatten die kostenlose Rücksendung. Wer sichergehen möchte, sollte sich vorab beim Händler informieren. Nach erfolgreichem Widerruf sind der Kaufpreis und gegebenenfalls gezahlte Versandkosten zu erstatten.

Anbieter haben auch außerhalb des Widerrufs Pflichten, Verbraucher:innen vor dem Vertrag ausführlich zu informieren. Sie müssen die Ware beispielsweise in ihren wesentlichen Eigenschaften beschreiben, zusätzlich muss der Gesamtpreis der Ware einschließlich aller damit verbundenen Preisbestandteile angegeben und über Zahlungs-, Lieferungs- und Leistungsbedingungen informiert werden.

Widerrufsrecht
§§ 312g ff., 355 ff. BGB

Vertragsabschluss	Widerrufsrecht

Vertragsschluss im Rahmen einer besonderen Vertriebsform per
• Fernabsatz
  • E-Mail
  • Fax
  • Telefon
  • SMS
• außerhalb von Geschäftsräumen
  • Haustür
  • Kaffeefahrt
  • Kauf außerhalb Ladengeschäft
	Ausnahmen vom Widerrufsrecht: Es gilt die Auflistung des § 312g. Abs. 2 BGB.
	Dazu zählen beispielsweise:
	• online abgeschlossene Pauschalreiseverträge
	• Verträge, bei denen die Leistung sofort erbracht und bezahlt wird und nicht mehr als 40 Euro kostet
	• maßangefertigte Waren
	• Kosmetika
	• u.a.

Frist: Erklärung innerhalb von 14 Tagen • ab Warenlieferung oder • ab Erbringung der Dienstleistung • ohne Angabe von Gründen • Kosten für die Retoure können Verbraucher:innen auferlegt werden • Verbraucher:innen müssen über ihr Widerrufsrecht informiert werden • keine ordnungsgemäße Belehrung: Widerrufsfrist von 1 Jahr und 14 Tage **Folge des erfolgreichen Widerrufs: Rückerstattung des Kaufpreises & ggf. gezahlter Versandkosten**	**Kein Widerrufsrecht:** • Kauf im Ladengeschäft • Kauf auf einer Warenmesse **Informationen finden Verbraucher auch unter: *https://s.rlp.de/PxFp3***

4.4 Sicheres Onlinebanking

7 von 10 Deutsche nutzen Onlinebanking.

Nach Informationen des Branchenverbandes Bitkom nutzen sieben von zehn Bankkund:innen in Deutschland Onlinebanking (Stand 2020). Damit die Nutzung nicht nur bequem, sondern auch sicher ist, sollten man einige Dinge beachten. Beim Onlinebanking greift man über eine Internetverbindung direkt auf den Bankrechner zu und kann seine Bankgeschäfte erledigen. Das funktioniert entweder direkt über die Internetseite der Bank („browserbasiertes Onlinebanking“) oder über spezielle, meist kostenpflichtige Onlinebanking-Programme (zum Beispiel WISO Mein Geld, StarMoney oder moneyplex).

Girokonto im Test: https://s.rlp.de/y9GHG

Von → „Mobile Banking“ spricht man, wenn eine App auf einem mobilen Endgerät fürs Onlinebanking verwendet wird. Manche sogenannten Smartphone-Banken spezialisieren sich schon darauf, die Erledigung von Bankgeschäften einzig über ihre Smartphone-App anbieten.

Gut zu wissen: Zunehmend bieten auch Unternehmen aus dem Bereich der Finanztechnologie, sogenannte FinTechs, Leistungen rund um Zahlungsverkehr oder Kontoverwaltung an. Beispiele sind Bezahlanwendungen für mobiles Bezahlen oder zum Zahlen im Internet, Portale, auf denen man seine Bankkonten und Verträge (Energie, Internet, Mobiltelefon, Versicherungen) verwalten kann, Haushaltsbuch-Apps und vieles mehr. Bei diesen Unternehmen handelt es sich aber nicht um Banken, sie benötigen nur eine Zulassung aus ihrem jeweiligen europäischen Herkunftsland.

Modul 5.6: Mobile Payment

Technische und organisatorische Maßnahmen sollen das Onlinebanking für Verbraucher:innen sicher machen. Kund:innen müssen sich zunächst von ihrer Bank für das Onlinebanking freischalten lassen und erhalten individuelle Anmeldedaten, meist bestehend aus einem Benutzernamen/einer Benutzernummer und einem Passwort. Diese werden oft per Post geschickt. Außerdem ist für viele einzelne Aktivitäten wie Überweisungen die Eingabe einer weiteren, einzigartigen Nummer erforderlich, der **T**rans**a**ktions**n**ummer (TAN). Die TAN ist ein wichtiger zweiter Sicherheitsfaktor, der für jede Aktivität oder Transaktion eigens erstellt wird. Hierzu bieten die Banken unterschiedliche Verfahren an.

Sicherheitstipps fürs Onlinebanking: https://s.rlp.de/XewnS

TAN-Verfahren

- **Einfache oder indizierte TAN-Listen** genügen den rechtlichen Anforderungen an die Autorisierung von Transaktionen für den Zahlungsverkehr nicht mehr. Sie hatten sich als missbrauchsanfällig erwiesen.

TAN-Verfahren im Test: https://s.rlp.de/qwKK9

- **mTAN (mobile TAN) oder smsTAN**
  Bankkund:innen bekommen eine TAN per SMS direkt auf das eigene Handy oder Smartphone geschickt und geben diese dann am Computer ein. Sicherheit bringt hier die Trennung der Übertragungswege. Diese Sicherheit ist jedoch nicht mehr gegeben, wenn ausschließlich das Smartphone für den kompletten Bankvorgang genutzt wird, also sowohl die SMS empfangen als auch die TAN in die Onlinebanking-Oberfläche der Bank eingegeben wird. Außerdem könnten sowohl das Smartphone als auch der PC mit Schadsoftware infiziert sein.

- **TAN-Generatoren (Chip-TAN, Smart-TAN)**
  Für dieses Verfahren wird ein spezieller TAN-Generator benötigt, wobei die einzelnen Banken unterschiedliche Varianten nutzen. Der Generator kann bei der Bank oder im freien Handel erworben werden. Es entstehen Kosten ab zehn Euro. Technisch ist der TAN-Generator zugleich ein Kartenlesegerät. Kund:innen geben ihre Auftragsdaten am Computer ein, stecken dann ihre Bankkarte in das Lesegerät und halten das Gerät vor den Computerbildschirm. Hier werden die Auftragsdaten über eine angezeigte Grafik ausgelesen und eine TAN auf dem Gerät generiert. Diese muss nur noch auf dem Computer eingegeben werden. TAN-Generatoren sind sehr sicher, da zwei getrennte Geräte genutzt werden und die Bankkarte als weiterer Sicherheitsfaktor erforderlich ist.

TAN-Verfahren: Welche es gibt und wie sicher sie sind: https://s.rlp.de/FLUMc

- **TAN via Smartphone-App (Push-TAN, Photo-TAN, App-TAN, BestSign)**
  Die Generierung der TANs erfolgt über eine kostenlose Smartphone-App. Auch hier gibt es unterschiedliche Varianten. Gemein ist ihnen, dass eine spezielle App der Bank auf dem Smartphone installiert und freigeschaltet werden muss. Diese generiert dann aus den Auftragsdaten die entsprechende TAN. Hierzu muss die

passwortgeschützte App geöffnet werden. Dann wird ein Code oder eine Grafik ausgelesen und die TAN erzeugt. Bei einer Variante müssen Kund:innen nach Eingabe des Passworts den Auftrag nur noch bestätigen – die TAN-Übertragung erfolgt automatisch im Hintergrund. BestSign fordert direkt zur Auftragsfreigabe durch die Eingabe eines Passworts oder durch biometrische Sicherheitsmerkmale wie Finderabdruckccan oder Gesichtserkennung auf.

Die App-Verfahren sind auch hier nur sicher, wenn für Banking und TAN-Generierung unterschiedliche Geräte genutzt werden. Manche App-Verfahren sind sogar so konzipiert, dass dasselbe Gerät auch für das Onlinebanking genutzt werden kann. Wer das Smartphone allein oder als Komponente für das Onlinebanking nutzt, sollte ganz besonders auf die IT-Sicherheit des Gerätes achten. Schadsoftware auf dem Smartphone könnte die Sicherheit der Verfahren kompromittieren.

Tipp

Geht das Smartphone verloren oder wird es gestohlen, sollten Sie nicht nur die SIM-Karte beim Mobilfunkanbieter sperren lassen, sondern vor allem auch Ihre Konten und Onlinebanking-Zugänge. Am schnellsten geht dies über den zentralen Sperr-Notruf 116 116. Informieren Sie anschließend unverzüglich Ihre Bank.

- **TAN via HBCI/FinTS**
  HBCI/FinTS (Home Banking Computer Interface/Financial Transaction Services) ist ein Standard für das softwarebasierte Banking mittels eigener Onlinebanking-Programme. Wird dieses mit Chipkarte und Kartenlesegerät zur TAN-Generierung genutzt, bietet es eine sehr hohe Sicherheit. Auch die Nutzung anderer TAN-Verfahren ist je nach Bank möglich.

Tipp

Bei allen Verfahren werden oberhalb der erstellten TAN noch einmal die wesentlichen Auftragsdaten angezeigt – kotrollieren Sie diese zur Sicherheit sorgfältig.

Goldene Regeln für sicheres Onlinebanking

- **Lesen Sie die Bedingungen Ihrer Bank fürs Onlinebanking.**
  So erhalten Sie einen guten Überblick, welche Sorgfaltspflichten Sie einhalten müssen und wann Sie die Bank wegen einer Nutzungssperre kontaktieren sollten.
- **Halten Sie Zugangsdaten stets geheim.**
  Benutzername, Passwort, PIN und TAN sollten niemandem verraten werden. Außerdem sollte man nie der Aufforderung in E-Mails folgen, solche Daten preiszugeben. Eine Bank wird niemals die Angabe von PINs oder TANs zu Kontrollzwecken per E-Mail oder Telefon verlangen – dabei handelt es sich mit großer Wahrscheinlichkeit um Betrugsversuche.
- **Lassen Sie sich nicht von vermeintlichen Links täuschen.**
  Die Internetadresse zur Bank sollte man immer selbst eingeben und dann unter den Favoriten im Browser speichern. Bei E-Mails und Websites deuten Rechtschreibfehler, eine falsche Internetadresse oder ein fehlendes Schlüsselsymbol in der Statusleiste auf Fälschungen hin. Zum Schutz vor Phishing sollte man darauf immer zusätzlich achten.
- **Nutzen Sie Onlinebanking nur in sicherer Umgebung.**
  Öffentliche Computer und Netzwerke sind nicht der richtige Ort für Bankgeschäfte. Aber auch auf dem heimischen Rechner sollte man Zugangsdaten zum Onlinebanking nicht ungesichert speichern, sondern immer wieder neu eingeben.
- **Behalten Sie Ihre Konten im Blick.**
  Prüfen Sie regelmäßig Ihre Kontobewegungen. Bei Verfügungen, die man nicht selbst veranlasst hat, sollte man sich sofort an die Bank wenden und eventuell Anzeige bei der Polizei erstatten.

4.5 Sicheres WLAN

Auch der Zugang zum Internet kann Gefahren bergen. Mit ein paar Einstellungen lässt sich jedoch das Heimnetzwerk so gut schützen, dass ein unbefugter Zugriff sehr schwierig wird.

„WLAN“ steht für „**W**ireless **L**ocal **A**rea **N**etwork“. So nennt man den drahtlosen Zugang ins Internet. Damit kann man heute bequem vom Balkon oder Garten aus im Internet surfen – ganz ohne lästige Kabelverbindung. Grundsätzlich sind die Anschlussinhaber:innen für den Internetanschluss verantwortlich, das heißt auch für einen möglichen Missbrauch des Internetanschlusses durch unbefugte Dritte. Erhält beispielsweise eine fremde Person Zugang zum Netzwerk und begeht in einer Onlinetauschbörse eine Urheberrechtsverletzung, so

haftet möglicherweise die Anschlussinhaberin oder der Anschlussinhaber dafür. Aus diesem Grund sollte man den drahtlosen Internetzugang immer sorgfältig gegen unbefugte Nutzung absichern.

Für das drahtlose Surfen benötigt man zunächst einen WLAN-Router. Er ermöglicht, eine Internetverbindung drahtlos auf mehreren Rechnern zu verteilen. Handelsübliche Router können über eine sogenannte grafische Benutzeroberfläche mit dem Browser, beispielsweise dem Internet Explorer oder Mozilla Firefox, eingerichtet werden. Dazu gibt man die sogenannte IP-Adresse des Routers in die Adresszeile des Browsers ein. Manche Router können auch über ein Schlüsselwort wie „fritz.box“ oder „speedport.ip“ erreicht werden. Ein Hinweis auf die Zugangsdaten des Routers findet sich in der Bedienungsanleitung, bei manchen Geräten auch auf der Rückseite. Die meisten Router haben zudem ein Passwort für die Benutzeroberfläche, zum Beispiel „0000“, „admin“ oder „password“. Dieses ist oft voreingestellt. Beim Einrichten des Geräts sollte man das Passwort in jedem Fall ändern.

Bei manchen Routern ist für die Einrichtung oder die Änderung der Einstellungen eine Internetverbindung über ein Netzwerkkabel (LAN) notwendig. Im nächsten Schritt sollte man das WLAN verschlüsseln. Manche Router sind werkseitig auf „unverschlüsselt“ eingestellt. Bei anderen ist eine WEP-Verschlüsselung oder eine WPA/WPA2-Verschlüsselung vorhanden. Da die WEP-Verschlüsselung sehr leicht geknackt werden kann, sollte immer die WPA- oder WPA2-Verschlüsselung eingestellt werden. Das ist der heute gängige Verschlüsselungsstandard. Inzwischen gibt es mit WPA3 auch schon einen Nachfolgestandard, der allerdings momentan noch von sehr wenigen Geräten unterstützt wird.

Jedes WLAN hat einen Namen, eine sogenannte „SSID“ („Service Set Identifier“). Der Name wird standardmäßig vom Hersteller vergeben, meist wird einfach die Gerätebezeichnung verwendet. Diesen Namen kann man individuell verändern. Der neue WLAN-Name sollte keine Rückschlüsse auf die Besitzerin oder den Besitzer zulassen, um gezielte Angriffe zu verhindern. Eine Bezeichnung wie „MeyerWLAN“ wäre also ungeeignet.

Manche Router bieten die Möglichkeit, das WLAN zu bestimmten Uhrzeiten, beispielsweise nachts, abzuschalten. Manchmal gibt es auch einen Schalter, mit dem das WLAN manuell ein- und ausgeschaltet werden kann. Wenn man den Router nicht benutzt, sollte man ihn abschalten. Das spart auch Energie.

Die sogenannte Firmware ist die Betriebssoftware eines Routers. Im Laufe der Zeit bringen Hersteller neuere Versionen (Updates) der Firmware heraus, die den Router um Funktionen erweitern oder Sicherheitslücken schließen. Daher sollte man in regelmäßigen Abständen die Aktualität der Firmware auf dem eigenen Router überprüfen und bei Bedarf eine neuere Version installieren. Eine aktuelle Firmware steht meist auf der Website des Herstellers zum Download bereit. Bei einigen Routern kann die Firmware aber auch direkt über die Benutzeroberfläche heruntergeladen und installiert werden. Bei modernen Routern kann über die Benutzeroberfläche auch ausgewählt werden, dass sich Firmware-Updates automatisch installieren. Diese Auswahl ist für Nutzer:innen am bequemsten.

4.6 Verletzung von Urheberrechten im Internet

Seit Jahren kommt es leider immer wieder vor, dass Verbraucher:innen mit teuren Abmahnungen von Anwaltskanzleien konfrontiert werden, die je nach Fall mit mehreren Hundert oder gar Tausend Euro zu Buche schlagen können. Ihnen wird vorgeworfen, eine Urheberrechtsverletzung begangen zu haben. Dabei wird ihnen zur Last gelegt, dass sie rechtswidrig Dateien wie Musikstücke, Filme, Computerspiele oder Fotos in Tauschbörsen im Internet zum Download angeboten oder selbst heruntergeladen haben – ohne Erlaubnis der Rechteinhaber:innen. Rechteinhaber:innen sind in diesen Fällen beispielsweise die Urheber:innen eines Musiktitels (Komponist:innen, Texter:innen) oder die Fotograf:innen eines Bildes. Die Rechte können sie entweder ganz oder teilweise an Musikverlage oder Bildagenturen zur Verwaltung abtreten, die ihrerseits dann die Kanzleien mit der Durchsetzung der Urheberrechte in Form von Abmahnungen beauftragen. Mit einer Abmahnung gehen Rechteinhaber:innen gegen Urheberrechtsverletzer:innen vor und verlangen neben Schadensersatz die Unterlassung zukünftiger Verletzungen.

Die Beratungsfälle in den Verbraucherzentralen zeigen, dass die Urheberrechtsverletzungen insbesondere auf folgende Weise begangen werden:

Wie kommt es zu Urheberrechtsverletzungen?

Häufige Beispiele	Sachverhalt	So geht's richtig
	Inhalte werden rechtswidrig über sogenannte Bittorrent-Filesharing-Börsen heruntergeladen. Rechteinhaber:innen können dies dokumentieren und abmahnen.	Inhalte, die normalerweise nur gegen Geld zu bekommen sind – wie aktuelle Kinofilme –, sind mit hoher Wahrscheinlichkeit illegal, wenn sie kostenlos angeboten werden. Solche Quellen sollten gemieden werden.
	Urheberrechtlich geschützte Fotos werden einfach aus dem Netz kopiert, etwa aus der Google-Bildersuche, und an anderer Stelle von der abgemahnten Person hochgeladen und damit veröffentlicht.	Fotos im Netz sollten niemals einfach kopiert und an anderer Stelle verwendet werden. Im Zweifel muss von dem oder der Urheber:in eine Lizenz eingeholt werden. Bilder, deren Lizenz die freie Nutzung erlaubt, gibt es in speziellen ➔ Datenbanken wie zum Beispiel pixabay.
	Urheberrechtsverletzungen können auch durch Dritte begangen werden, wenn diese das WLAN des oder der Abgemahnten nutzen. Hier kommt die sogenannte Störerhaftung zum Tragen und der oder die Abgemahnte kann sich meist nur dann vom Vorwurf befreien, wenn er oder sie die Person benennen kann, welche die Urheberrechtsverletzung zum fraglichen Zeitpunkt begangen haben könnte.	Der Zugriff auf das eigene WLAN sollte stets geschützt sein – etwa durch ein Passwort oder noch besser durch einen gesonderten Bereich für Gäste. Das Passwort sollte nur sehr zurückhaltend herausgegeben werden. Familienmitglieder und insbesondere Kinder sollten ausführlich über urheberrechtliche Risiken aufgeklärt werden, bevor sie das Internet frei nutzen dürfen.

Tipp

Wer eine Abmahnung bekommt, sollte nicht einfach bezahlen, sondern sich fachkundig in einer spezialisierten Anwaltskanzlei oder beispielsweise bei der Verbraucherzentrale beraten lassen. Häufig kann der Abmahnung erfolgreich widersprochen werden oder die Geldforderungen können zumindest reduziert werden.

Eine Urheberrechtsverletzung begeht auch, wer auf einer Internetseite ohne Erlaubnis der Rechteinhaberin oder des Rechteinhabers Fotos, Auszüge von Stadtplänen und Ähnliches zeigt. Auch wer selbst gemachte Fotos veröffentlicht, muss gesetzliche Regelungen beachten, damit er oder sie die Rechte der dargestellten Personen nicht verletzt. So ist es in der Regel unzulässig, Fotos von anderen ohne deren ausdrückliche Zustimmung über das Internet, mit welcher Anwendung auch immer, zu verbreiten.

Modul 6.6: Das Recht am eigenen Bild

Die Rechteinhaber:innen der Werke sind meistens große Unternehmen der Musik- und Filmindustrie. Sie gehen strikt gegen Urheberrechtsverletzungen vor, indem sie Firmen beauftragen, Rechtsverletzer:innen zu ermitteln. Im Rahmen ihrer Ermittlungen gelangen die beauftragten Firmen an die IP-Adresse des Computers, deren Inhaber:innen sich aktiv in den Tauschbörsen betätigt haben sollen oder tatsächlich betätigt haben.

Um die Adresse der Besitzer:innen des Internetanschlusses zu erhalten, stellen sie einen Auskunftsantrag bei Gericht. Das Gericht prüft dann, ob der Provider dieser Person die Daten an die Rechteinhaber:innen herausgeben muss. Erhalten die Firmen die Daten, beauftragen sie ihre Anwälte, die Rechtsverletzer:innen abzumahnen. Dazu werden Abmahnschreiben – oft über mehrere Hundert Euro – verschickt und eine Frist zur Zahlung gesetzt. Durch die Abmahnung soll die Rechtsverletzung aufgezeigt und für die Zukunft unterbunden werden. Außerdem wird der abgemahnten Person Gelegenheit gegeben, die Rechtsverletzung außergerichtlich zu regeln. Die Abmahnung fordert die betroffene Person also formal auf, ein rechtswidriges Verhalten in Zukunft zu unterlassen.

In der Regel liegt eine Unterlassungs- und Verpflichtungserklärung bei, die der oder die Abgemahnte unterschreiben soll. In der Abmahnung wird den Betroffenen auch mehr oder weniger ausführlich

mitgeteilt, in welcher Höhe sie zur Zahlung von Schadensersatz und Rechtsverfolgungskosten verpflichtet sind. Allerdings sind sowohl die geforderten Rechtsanwaltsgebühren als auch die Schadensersatzforderungen oft zu hoch angesetzt. Ob der oder die Abmahnende überhaupt berechtigt ist, diese Ansprüche geltend zu machen, und ob die betroffene Person verpflichtet ist, diese Forderungen zu bezahlen, muss im Einzelfall juristisch überprüft werden.

Grundsätzlich richtet sich die Höhe der Zahlungsforderungen nach der Schwere des Verstoßes. Wer nicht auf das Abmahnschreiben reagiert, muss in aller Regel mit einer gerichtlichen Auseinandersetzung rechnen. Meistens stellt die Gegenseite einen Antrag auf Erlass einer einstweiligen Verfügung. Die dem Anwaltsschreiben beigefügten vorformulierten Unterlassungs- und Verpflichtungserklärungen sind häufig so weit gefasst, dass sie einem Schuldeingeständnis gleichkommen. 30 Jahre lang ist man daran gebunden. Wer also in den Folgejahren bewusst oder unbewusst dagegen verstößt, ist direkt dazu verpflichtet, die sehr hohe Vertragsstrafe zu zahlen.

Tipp

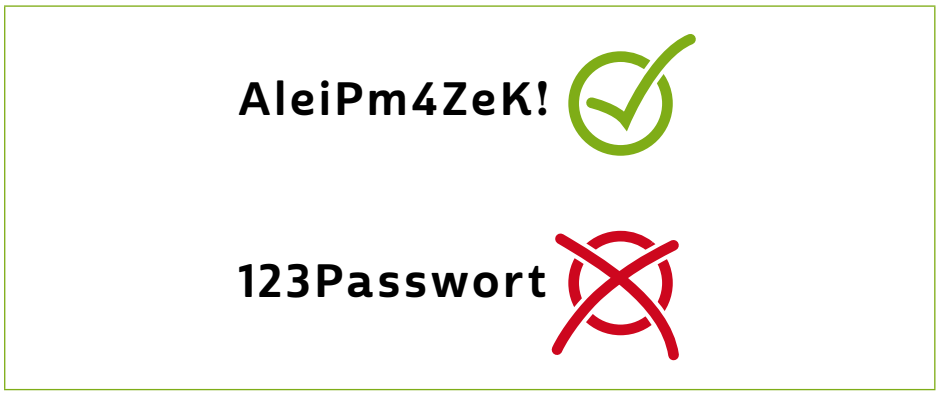
Wer ein anwaltliches Abmahnschreiben erhalten hat, sollte es nicht einfach ignorieren, sondern umgehend tätig werden. Häufig versuchen Kanzleien, mit sehr knapp gesetzten zeitlichen Fristen Druck auszuüben. Hier gilt es, Ruhe zu bewahren und, wenn nötig, die Kanzlei um Fristverlängerung zu bitten, die in der Regel auch gewährt wird. Keinesfalls sollte durch Zeitdruck vorschnell eine Erklärung abgegeben werden, bevor nicht ein:e Spezialist:in den Sachverhalt geprüft hat.

Bei jedem erneuten Verstoß wird die gleiche Summe wieder fällig. Es ist daher ratsam, die Unterlassungs- und Verpflichtungserklärungen nicht sofort zu unterschreiben, sondern nach fachkundiger Beratung abzuändern. Solche sogenannten modifizierten Unterlassungs- und Verpflichtungserklärungen „ohne Anerkennung einer Rechtspflicht“, die speziell auf den Einzelfall bezogen sind, kann aber nur eine Rechtsanwältin oder ein Rechtsanwalt mit Spezialisierung auf Urheberrecht erstellen. Auch die Verbraucherzentrale bietet im Bereich Urheberrecht außergerichtliche Rechtsberatung an.

4.7 Passwörter und Schutz von mobilen Endgeräten

Auch die vermeintlich besten Passwörter für Internet-Accounts sind niemals zu 100 Prozent sicher. Denn sogenannten Hackern (kriminellen IT-Spezialist:innen) ist in der Vergangenheit schon des Öfteren der Diebstahl von Daten großer Firmen, Kliniken und sogar Regierungen gelungen. Daher ist eine vernünftige Datensicherung unerlässlich. Sie dient als doppelter Boden im Falle des Falles und schützt vor Datenverlust. Dabei gibt es einige Punkte zu beachten, allen voran die Wahl eines sicheren Passworts.

Regeln für sichere Passwörter



Am einfachsten haben es Kriminelle beim Kapern von Konten, → Accounts und Geräten, die mit einem schlechten Passwort geschützt sind. Eine traurige Tatsache, die sich leider seit Jahren kaum ändert, ist, dass viele Menschen unsichere Passwörter verwenden (wie zum Beispiel: „123Passwort“).

Speziell schwache Passwörter sind für die meist erfahrenen Täter:innen geradezu eine Einladung. Profis knacken Passwörter unter anderem mithilfe von Entschlüsselungsprogrammen, die mit rasender Geschwindigkeit verschiedene Passwörter „durchprobieren“ und in denen die gängigsten und damit schwächsten Passwörter natürlich als Erstes abgefragt werden, dicht gefolgt von den am häufigsten verwendeten Wörtern. Bei den schwachen Passwörtern steht ganz oben die bereits genannte aufsteigende Zahlenfolge 1234..., dicht gefolgt von dem Wort „Passwort“. Nicht weniger gefährlich ist aber auch die Verwendung von Informationen, die Täter:innen leicht über

das Opfer in Erfahrung bringen können. So eignet sich der eigene Name oder der von Angehörigen nicht für Passwörter, ebenso wenig wie Geburtstage, Straßennamen und andere leicht zu recherchierende Informationen.

Um sich wirksam zu schützen, sollten folgende Grundregeln für Passwörter beherzigt werden:

- Passwörter sollten nicht aus existierenden Wörtern bestehen, da diese leicht erkannt werden.

- Passwörter sollten ausreichend lang und komplex sein, also am besten aus mindestens 12 Zeichen bestehen und Groß-, Kleinbuchstaben, Zahlen und Sonderzeichen beinhalten.

- Passwörter sollten niemals mehrfach verwendet werden, da sonst mehrere Zugänge auf einmal übernommen werden können, wenn Täter:innen das Passwort herausbekommen.

Grundsätzlich kann natürlich jedes Passwort geknackt werden, wenn die Täter:innen es nur ausreichend lange versuchen. Jedoch kann dies bei einem komplexen, ausreichend langen Passwort schon mal Jahre dauern. Hinzu kommt, dass immer mehr Dienste ihre Zugänge automatisch sperren, wenn eine gewisse Anzahl von falsch eingegebenen Passwörtern erfolgt ist. Fazit: Ein gutes Passwort ist ein zuverlässiger Schutz. Doch wie soll man sich diese ganzen Passwörter nur merken?

Diese Frage ist natürlich absolut nachvollziehbar. Ein langes abstraktes Passwort oder gar mehrere im Kopf zu behalten, ist nur schwer möglich. Dies ist wohl auch der Grund, warum so viele Menschen schwache, aber dafür leicht merkbare Passwörter verwenden.

Tipp

Merken Sie sich komplexe Passwörter mithilfe von Eselsbrücken.

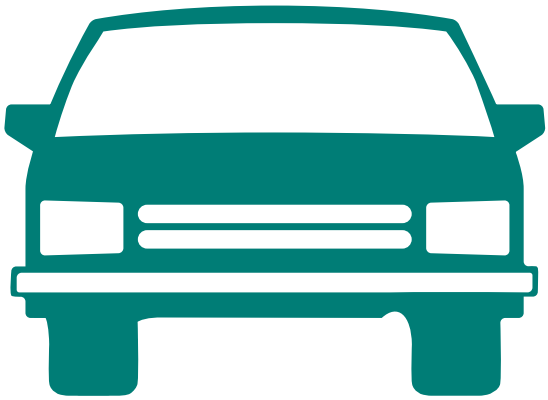
Doch mit ein wenig Organisation und Vorbereitung kann man auch mit kompliziertesten Passwörtern umgehen. Eine erprobte Methode sind Eselsbrücken. Hierbei werden die einzelnen Zeichen des Passwortes mit einem Merksatz verknüpft, wobei der Anfangsbuchstabe von jedem Wort für ein Passwortzeichen steht oder für eine Zahl oder ein Sonderzeichen. Eine gute Anleitung, die im Folgenden vorgestellt wird, bietet das Bundesamt für die Sicherheit in der Informationstechnik (kurz: BSI).

Was hat Ihr Passwort mit diesem Auto zu tun?

Denken Sie sich einen Satz aus, der mindestens eine Zahl und wenn möglich auch Sonderzeichen enthält:

„Seit ich das Auto nicht mehr kaufe, sondern mit Carsharing miete, spare ich jeden Monat fünfzig Euro."

Merken Sie sich jeweils den ersten Buchstaben der Wörter und fügen sie Zahlen und Sonderzeichen ein, um ein sicheres Passwort zu erhalten.



SidAnmk,smCm,sijM5€

Tipp

Nutzen Sie Passwortmanager!
Weitere Infos dazu hier im Modul sowie auf
https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/sichere-passwoerter-so-gehts-11672

Zwei-Faktor-Authentifizierungen

Besonders sensible Zugänge, wie etwa Onlinebanking-Accounts, sollten zusätzlich durch sogenannte Zwei-Faktor-Authentifizierungen abgesichert werden.

Tipp

Zwei-Faktor-Authentifizierungen bieten zusätzlichen Schutz.

Mehr zur Zwei-Faktor-Authentifizierung: https://s.rlp.de/RgQf2

Dieses Verfahren wird von immer mehr Dienstleistern angeboten. Dabei reicht es nicht aus, dass das Passwort eingegeben wird. Es muss zusätzlich noch der besagte zweite Faktor angegeben werden. Hierbei kann es sich um einen zusätzlichen Code handeln, der auf einem separaten Gerät generiert wird, etwa in einer speziellen Smartphone-App oder auf einem speziellen Code-Generator-Gerät. Alternativ können auch biometrische Daten wie Fingerabdrücke oder Gesichtsscans zur Sicherung verwendet werden. Für was man sich auch entscheidet, durch die Verwendung des zweiten Sicherheitsfaktors ist sichergestellt, dass Täter:innen selbst dann keinen Zugriff auf den Account erhalten, wenn sie das zugehörige Passwort erbeutet haben.

Ausblick in eine Zukunft OHNE Passwörter

Unter dem etwas sperrigen technischen Stichwort → „FIDO2“ könnte sich in nicht allzu ferner Zukunft die Ersatztechnologie für die bei vielen ungeliebten Passwörter verbergen. FIDO2 funktioniert so, dass es kryptografische Verschlüsselungstechnologie auf einem physischen Computerchip (einem „FIDO2-Token“) in Verbindung mit Software-Sicherheitsschlüsseln („FIDO2-Keys“) einsetzt. Zudem kann das System den zusätzlichen Schutz der Zwei-Faktor-Authentifizierung integrieren, indem der Zugriff auf den → Token bei Bedarf durch Code-Eingabe oder die Abfrage biometrischer Daten geschützt wird. Rein praktisch kann man sich den Einsatz von FIDO2 so vorstellen, dass man bei einem Anmeldevorgang seinen Token hervorholt, dessen Chip sich in einem Schlüsselanhänger oder auch Smartphone befinden kann. Über das Lesegerät kann die Besitzerin oder der Besitzer des Tokens sodann die Authentifizierung bestätigen. Damit das nicht jeder Person möglich ist, die den Token in Händen hält, kann zusätzlich als biometrische Signatur etwa der Fingerabdruck oder das Gesicht gescannt oder die Eingabe eines Codes verlangt werden.

Passwortmanager erleichtern die Passwortflut

Hat man nur ein oder zwei Accounts, dann mag es gut möglich sein, dass man sich eine Handvoll sicherer Passwörter noch gut im Kopf merken kann. Die heutige Realität sieht bei den meisten aber anders aus, und nicht selten kommt man beim Nachzählen schnell auf eine mittlere zweistellige Zahl von Zugängen, die sicher verwaltet werden wollen. Da das eigene Gedächtnis hier abgesehen von beneidenswerten Ausnahmefälle meist an seine Grenzen stößt, empfiehlt es sich, auf Hilfsmittel zurückzugreifen. Hier kann man zwischen → analogen, → digitalen und cloudbasierten Lösungen unterscheiden.

Methode	Vorteil	Nachteil
Analoger Ansatz – Passwörter händisch in einem Buch notieren	Kein digitales Ausspähen möglich.	Handhabung und Anpassungen sind recht umständlich, ebenso wie Sicherheitskopien.
Digitaler Ansatz – Passwortmanager befindet sich zentral auf einem einzelnen Gerät	Passwörter müssen nicht mehr händisch verwaltet werden, und dennoch hat man die ausschließliche Kontrolle über die Daten.	Häufig ist die Handhabung etwas komplizierter und weniger nutzerfreundlich. Bei Lösungen ohne Sicherheitskopie droht der Totalverlust der Daten.
Cloudbasierter Ansatz – Passwortmanager wird über einen Dienstleister angeboten und ist geräteübergreifend synchron verfügbar	Die Handhabung und das Einrichten von Sicherheitskopien sind hier am einfachsten.	Die Datensicherheit ist gefährdet, wenn man sich auf einen unseriösen oder unsicheren Dienst einlässt. Eine sorgfältige Prüfung bei der Auswahl ist daher unerlässlich.

Während das händisch geführte Passwortbuch recht selbsterklärend ist, bedarf es bei den Passwortmanagern einiger Ausführungen. Passwortmanager kann man sich in ihrer Funktion wie einen Tresor vorstellen. Eingetragene Passwörter werden verschlüsselt, und nur wer das Masterpasswort kennt, erhält Zugriff auf die hinterlegten Passwörter. Da das Masterpasswort extrem wichtig ist, sollte dieses unbedingt mittels Zwei-Faktor-Authentifizierung doppelt abgesichert werden.

Bei der Auswahl des richtigen Passwortmanagers gilt es, die eigenen Bedürfnisse und Vorlieben genau abzuwägen. Neben kostenpflichtigen und kostenlosen Lösungen gibt es mittlerweile auch immer mehr Lösungen, die Nutzer:innen entweder von den Betreibern der einzelnen Betriebssysteme der Geräte direkt angeboten werden (insbesondere Microsoft, Apple und Google) oder die von unabhängigen Anbietern mittels eigenständiger Software funktionieren. Eine gute Hilfestellung bei der Auswahlrecherche kann hier die Stiftung Warentest bieten.

Tipp

Wenn man sich Passwörter für eine Vielzahl von Accounts merken muss, kann ein Passwortmanager eine hilfreiche Lösung sein.

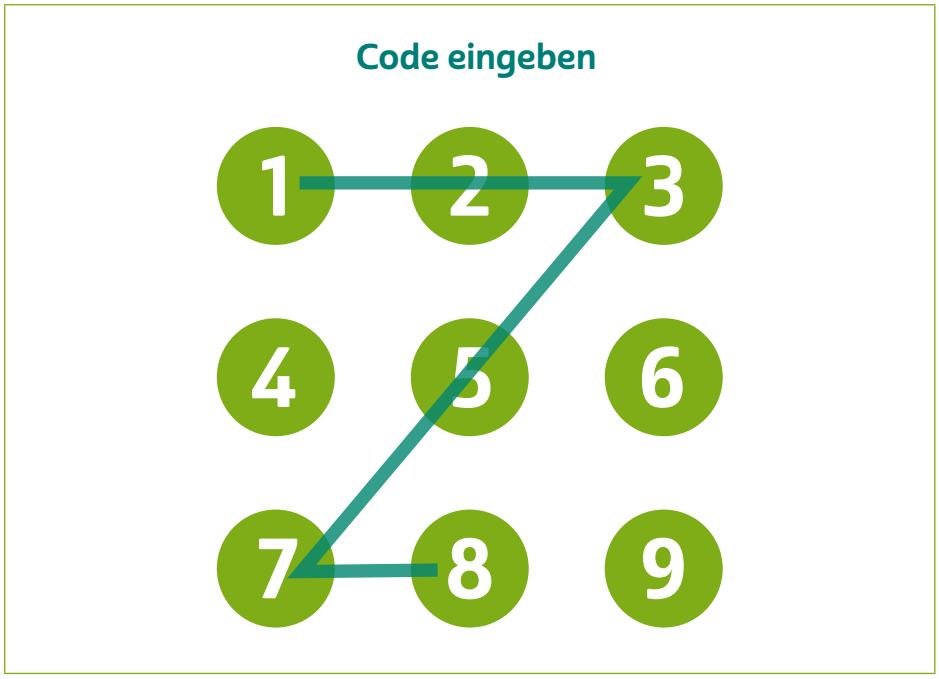
Passwörter können auch direkt im Internetbrowser gespeichert und automatisch beim Betreten der Website abgerufen werden. Dies ist bequem, sollte jedoch nur sehr zurückhaltend und keinesfalls bei sensiblen Accounts verwendet werden, da die Passwörter im Internetbrowser deutlich unsicherer gespeichert sind als in einem Passwortmanager.

Bildschirmsperren sind richtig wichtig

Gerade bei unseren kleinen mobilen Computern wie Smartphones und Tablets ist es wichtig, dass wir sie vor unbefugten Zugriffen schützen. Besonders Smartphones, die ständig herumgetragen werden, enthalten eine Vielzahl von sensiblen Informationen. Dazu gehören etwa die Kontaktdaten unseres sozialen Umfelds, aber auch gefährliche Zugriffsmöglichkeiten, wie zum Beispiel Einkaufs-Apps, Banking-Apps, Apps sozialer Netzwerke usw. Damit Daten nicht missbraucht werden können, wenn etwa das Gerät durch Verlust oder Diebstahl in falsche Hände gerät, ist es sinnvoll, den Zugriff auf das Gerät mit einer Bildschirmsperre zu versiegeln.

Bei der Auswahl der gewünschten Bildschirmsperre kann zunächst grundsätzlich zwischen einem Code in Form einer Ziffernfolge und biometrischen Daten, etwa Fingerabdruck, Gesichts- oder Retinascan (Retina ist die Netzhaut im Auge eines Menschen) unterschieden werden.

Am weitesten verbreitet ist die Eingabe eines Zahlencodes von in der Regel vier bis sechs Ziffern. Bei der Auswahl des Codes greifen viele auf sogenannte Wischmuster zurück, die sich an der Anordnung der Zahlentastatur orientieren und durch die Wischbewegung eine Eselsbrücke bieten. Nach Möglichkeit sollte jedoch darauf verzichtet werden, da derartige Muster auch leichter von Kriminellen geknackt werden können, die beim Ausprobieren natürlich mit den am häufigsten verwendeten Mustern beginnen und die Wischspuren oft am Display erkennbar sind.



Wischmuster als Code-Sperren sind leichter zu knacken und sollten daher vermieden werden.

Neben den Zahlencodes ist auch die Verwendung von biometrischen Daten einen Gedanken wert – auf iPhones von Apple hat etwa die Verwendung des Gesichtsscans in den vergangenen Jahren rege Verbreitung gefunden, da das System bislang als sehr sicher gilt. Gleiches gilt auf vielen Geräten für Fingerabdrucksensoren. Sicherheit ist hier das entscheidende Stichwort. Da biometrische Daten hochsensible Informationen sind, muss sichergestellt sein, dass diese zuverlässig verschlüsselt auf dem Gerät gespeichert werden. Auch muss die verwendete Technologie zuverlässig Täuschungsversuche erkennen können. Dies ist leider nicht bei jedem Smartphone-Modell der Fall, da gerade bei günstigen Modellen die Leistungsfähigkeit der verwendeten Sensoren nicht immer das liefert, was die Werbung verspricht. Daher empfiehlt sich eine kritische Recherche von Testberichten zum eigenen Gerät, bevor man sich für die Verwendung biometrischer Daten entscheidet.

Silver Tipps!

Anleitungen zum Einrichten von Bildschirmsperren: https://s.rlp.de/hkyhe

Tipp

Als technisch besonders sicher haben sich die Fingerabdruckscanner-, aber auch aktuelle Gesichtsscanner-Verfahren erwiesen.

Mehr zum Thema auf mobilsicher.de: https://s.rlp.de/2VYLo

Diebstahlschutz

Trotz eingerichteter Bildschirmsperre gibt es für den Verlust oder Diebstahl des Geräts weitere Möglichkeiten zum Diebstahlschutz. So kann man versuchen, das Gerät aus der Ferne zu orten, um es wiederzufinden. Außerdem können auch per Fernzugriff alle Daten auf dem Gerät gelöscht werden. Derartige Einstellungen kann man entweder über Google und Apple direkt oder über Drittanbieter von Sicherheits-Apps vornehmen.

INTERVIEW MIT

Ulrike von der Lühe

Vorstand der
Verbraucherzentrale
Rheinland-Pfalz

„Wer die Risiken kennt und weiß, wie man sie meidet, kann sich im Internet gefahrlos bewegen.“

Was können Sie Verbraucher:innen raten, um nicht auf Abzocke im Netz hereinzufallen? Ihre drei wichtigsten Tipps:

Ulrike von der Lühe: Das Netz bietet viele gute und schöne Möglichkeiten, zum Beispiel für einen bequemen Einkauf von zu Hause aus. Leider tummeln sich aber auch dort zahlreiche Betrüger:innen. Wichtig ist deshalb immer eine gehörige Portion Skepsis, zum Beispiel bei Super-Sonderangeboten. Von Vorkasse rate ich generell ab, denn schlimmstenfalls ist das Geld weg und man steht mit leeren Händen da. Gütesiegel können hilfreich sein, um einen „guten Shop“ zu finden. Aber auch hier muss man genau hinschauen. Echte Gütesiegel wie etwa „Trusted Shops“ können gefälscht sein. Durch einen Klick auf das Emblem ist leicht zu prüfen, ob das Siegel mit einem Zertifikat des Siegelbetreibers verlinkt ist. Ohne den entsprechenden Link dürfte es nicht echt sein.

Grundsätzlich gilt: Egal ob seriöser Anbieter oder nicht, geben Sie nie mehr Daten an als notwendig.

Welche Erfahrungen machen Sie in den Beratungen der Verbraucherzentrale: Ist es besonders die Genration 50 plus, die in Fallen im Netz tappt?

Ulrike von der Lühe: Es ist keine Frage des Alters, wer im Netz hereingelegt wird. Es ist das fehlende Wissen darüber, wie man sich im Netz sicher bewegt, aber auch die Leichtgläubigkeit, wenn Betrüger:innen

mit supergünstigen Angeboten ködern oder seriöse Internetseiten imitieren. Auch hier ist eine gesunde Portion Misstrauen und sorgfältiges Prüfen unbekannter Anbieter oder Portale angesagt, um sich vor Abzockmaschen zu schützen. Die Verbraucherzentrale informiert und unterstützt alle Menschen, denen dieses Wissen fehlt. Wer die Risiken kennt und weiß, wie man sie meidet, kann sich im Internet gefahrlos bewegen und die vielen positiven Aspekte nutzen.

Ihr letzter Einkauf im Internet?

Ulrike von der Lühe: Ich persönlich kaufe nicht sehr häufig im Netz ein. Ich bin gern in der Innenstadt unterwegs und unterstütze den stationären Einzelhandel. Karten für Kulturveranstaltungen und Konzerte kaufe ich hingegen gern im Internet. Das ist einfach sehr bequem. Deshalb wird mein letzter Interneteinkauf sehr wahrscheinlich eine Konzertkarte oder Ähnliches gewesen sein.

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.

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.

Button-Lösung: Die sogenannte Button-Lösung (zu Deutsch „Schaltflächenlösung“) bezeichnet die gesetzliche Regelung über den Abschluss eines Kaufvertrages im Internet. Die Bestellung einer Ware im Inter-

net ist nur dann gültig, wenn diese Schaltfläche gut lesbar mit nichts anderem als den Worten „zahlungspflichtig bestellen“ oder mit einer entsprechenden eindeutigen Formulierung beschriftet ist. Nur wenn ein:e Verbraucher:in den Kaufvorgang mit Klick auf eine solche Schaltfläche bestätigt, kann ein wirksamer Vertrag entstehen.

Datenbank: Datenbanken dienen dazu, große Mengen an Informationen, wie zum Beispiel ganze Adresssätze, verwaltbar zu machen. Ähnlich einer Bank, die Geld im Tresor lagert, lagert eine Datenbank, etwa auf einem Server im Internet, Informationen ein und hält diese für autorisierte Abfragen bereit. In Tabellenform, also in Zeilen und Spalten, werden unterschiedlichste Informationen erfasst und zum Beispiel für Websites, soziale Netzwerke und Onlinebanking zur Verfügung gestellt.

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.

Einzugsermächtigung: Als Einzugsermächtigung bezeichnet man die Erlaubnis des Käufers, dass der Verkäufer die Rechnungssumme per Lastschrift vom Konto des Käufers einziehen darf. Bei diesem Verfahren hat der Käufer das Recht, ohne Angabe von Gründen die Lastschrift zurückzugeben.

FIDO2: Dabei handelt es sich um ein fortschrittliches Authentifizierungsverfahren, das in Zukunft die Passwörter ersetzen könnte.

Firmware: Der Begriff „Firmware“ beschreibt die Software, die in bestimmten Geräten wie beispielsweise einem Router von Haus aus installiert ist. Einige Geräte erlauben ein sogenanntes Firmware-Update, bei dem die Software auf den neuesten Stand gebracht wird.

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

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

Impressum: Wie das Impressum bei Printprodukten zeigt auch das Impressum von Websites an, wer für die Inhalte rechtlich verantwortlich ist. Ein vollständiges Impressum enthält folgende Informationen: Firmenname; Anschrift mit postalischer Adressierung (kein Postfach); weitere Kontaktmöglichkeiten über Telefon, Fax, E-Mail; eine als verantwortlich für die Seite angegebene natürliche Person (Name); Handelsregistereintrag und/oder Steuernummer.

Internetbezahldienste: Mit Internetbezahldiensten sind die verschiedenen bargeldlosen Bezahlmöglichkeiten im Internet gemeint. Bezahldienste sind unabhängig von einem bestimmten Onlineshop und bieten eine größere Sicherheit beim Kauf. Die Anbieter reichen hier von PayPal über Klarna bis hin zu giropay.

IP-Adresse: „**I**nternet-**P**rotocol“-Adressen sind die digitalen Fingerabdrücke im Netz. Jeder PC im Internet erhält seine eigene, nur einmal vorhandene IP-Adresse. Vergleichbar ist diese mit der Postanschrift. Nur können mit IP-Adressen Computer untereinander Daten austauschen und Informationen hin- und herschicken.

LAN: Die Abkürzung „LAN“ steht für den englischen Begriff „**L**ocal **A**rea **N**etwork“ (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 „**W**ireless **L**ocal **A**rea **N**etwork“, 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.

Mobile Banking: Mobile Banking bezeichnet die Nutzung des Onlinebanking-Services einer Bank über ein mobiles Endgerät. Dabei wird beispielsweise eine spezielle App auf dem Smartphone installiert, die den Zugriff auf das Bankkonto ermöglicht.

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.

Phishing: Beim Phishing geht es darum, mit gefälschten E-Mails und anderen Nachrichtenformen an Daten von Nutzer:innen zu kommen. Dabei werden Nutzer:innen auf gefälschte Websites gelockt, um dort ihre Daten preiszugeben. Beispielsweise erhält man eine E-Mail, in der man dazu aufgefordert wird, die eigenen Bankdaten auf einer Website anzugeben. Die entsprechende Seite sieht der Originalseite der Bank sehr ähnlich, ist allerdings eine Betrugsseite. Der Begriff „Phishing“

setzt sich zusammen aus den Wörtern „fishing“ (zu Deutsch „angeln“) und „Passwort“. Phishing ist also das Angeln nach Passwörtern.

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.

Provider: Als „Provider“ bezeichnet man den Dienstanbieter für den Internetzugang. Dieser ist häufig zugleich der Telefonanbieter.

Retinascan: Ein Retinascan ist eine Methode zum (Ent-)Sperren eines mobilen Endgeräts, wie beispielsweise eines Tablets oder Smartphones. Dabei wird die Netzhaut der Nutzer:innen erfasst, welche bei jeder Person ein individuelles Muster der Blutgefäße aufweist.

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.

SIM-Karte: Die Abkürzung „SIM“ stammt vom englischen „**S**ubscriber **I**dentity **M**odule“ (zu Deutsch „Teilnehmeridentitätsmodul“). Die SIM-Karte ist eine kleine Chipkarte, die man von seinem Mobilfunkanbieter erhält und die in ein Mobiltelefon eingesteckt werden muss. Über die darauf gespeicherten Daten und Informationen können die Nutzer:innen im Netz identifiziert werden. Durch eine veränderbare PIN kann die SIM-Karte vor unbefugter Benutzung geschützt werden.

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.

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.

Streaming: „Streaming" (englisch für „fließen", „strömen", in diesem Fall in Bezug auf einen Datenstrom) bedeutet, dass eine direkte Datenübertragung etwa von einem Streamingdienst oder von den Mediatheken öffentlich-rechtlicher oder privater Sendeanstalten stattfindet. Durch diese kann ein bereitgestelltes Video direkt online angesehen werden. Ein häufig mit dem „Streamen" auftauchender Begriff ist „Video-on-Demand". Dabei handelt es sich um die dauerhafte Bereitstellung von Videos durch einen Anbieter in einem Onlinedienst. Der Begriff „Streamen" beschreibt die Datenübertragung beim Anschauen des Videos.

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.

TAN: Die Abkürzung „TAN" steht für „**T**rans**a**ktions**n**ummer". Diese Nummer ist eine Art Einmalpasswort und findet meist im Onlinebanking Anwendung.

Token: Als „Token" wird in der IT eine Erkennungsmarke bezeichnet, die die jeweiligen Träger:innen als Inhaber:innen einer Berechtigung ausweist.

Unterlassung: Mit dem Unterlassungsanspruch kann eine künftige Beeinträchtigung oder drohende Störung rechtlich abgewehrt werden.

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.

WLAN: siehe *LAN*

WPA/WPA2/WPA3-Verschlüsselung: „**W**i-Fi **P**rotected **A**ccess“ ist ein verbesserter und sichererer Nachfolger der WEP-Verschlüsselung. Heute ist WPA2 der gängige Standard bei der WLAN-Verschlüsselung. Inzwischen gibt es auch schon den WPA3-Standard, der momentan aber nur von wenigen Geräten unterstützt wird.

Zahlungsauslösedienst, PSD2 („Payment Services Directive 2“): Zahlungsauslösedienste nehmen Überweisungen zulasten eines Bankkontos vor. Dabei räumen Kontoinhaber:innen einem Drittdienst die Rechte zur Nutzung des Onlinebankings bei ihrer Bank ein. Mittels des PSD2-Verfahrens wird der Zugriff des Drittdienstes auf die Kontodaten beschränkt. Zudem gilt: Ohne Zustimmung des Kontoinhabers oder der Kontoinhaberin darf keine Zahlung ausgeführt werden.

Zwei-Faktor-Authentifizierung: Damit ist gemeint, dass der Zugriff zu einem bestimmten Dienst erst gewährt wird, wenn die Berechtigung des Nutzers oder der Nutzerin durch zwei voneinander unab-

hängige Identifikationsmethoden geprüft wurde. In der Regel können die Methoden aus folgenden Bereichen ausgewählt werden: Wissen (Passwort oder Code), Gerät (Chip-Lesegerät oder Smartphone) und biometrische Kennung (Fingerabdruck, Gesichts- oder Retinascan).

Autor:innen

Dr. Julia Gerhards arbeitet bei der Verbraucherzentrale Rheinland-Pfalz als Referentin für Verbraucherrecht und Datenschutz. Neben Aufklärung und Information der Verbraucher 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.

Miriam Raic arbeitet bei der Verbraucherzentrale Rheinland-Pfalz als Juristische Fachberaterin. Sie berät und vertritt Verbraucher:innen im Rahmen der allgemeinen Rechtsberatung in allgemeinen Verbraucherrechtsthemen. Vor ihrer Tätigkeit bei der Verbraucherzentrale Rheinland-Pfalz war sie bei der Zentrale zur Bekämpfung unlauteren Wettbewerbs e. V.

Impressum

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

Projektkoordination:
Verbraucherzentrale Rheinland-Pfalz e.V.
Laura Muth
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 Ulrike von der Lühe, Dr. Julia Gerhards, Michael Gundall, Maximilian Heitkämper, Miriam Raic: Laura Muth

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.

Diese Lernhilfe wurde erstellt von:

Das Projekt wurde gefördert durch:

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 interessierten 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:
Verbraucherzentrale Berlin e.V.
Ordensmeisterstr. 15-16
12099 Berlin
verbraucherzentrale-berlin.de

Bezugsadressen:
Verbraucherzentrale Berlin e.V.
Ordensmeisterstr. 15-16
12099 Berlin
verbraucherzentrale-berlin.de/smart-surfer-be

Smart Surfer | 2021