Verbraucherzentrale
Rheinland-Pfalz

Medien sicher nutzen
Modul 5

Daten- und Accountsicherheit

Medien sicher nutzen

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

Gefördert durch das
Ministerium für Familie, Frauen, Kultur
und Integration (MFFKI)

RheinlandPfalz
MINISTERIUM FÜR
FAMILIE, FRAUEN, KULTUR
UND INTEGRATION

Die Materialien stehen auch auf Schulcampus,
dem Bildungsserver Rheinland-Pfalz.
https://www.schulcampus-rlp.de

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

1. Grundlagen

Immer wieder kommt es vor, dass Firmen gehackt werden und deren Kundendaten anschließend im Internet kursieren. Neben den Nutzer:innen etwa des Mobile-Game-Herstellers Zynga waren im August 2019 beispielsweise auch Zehntausende Mastercard-Kund:innen von einem Datenleck betroffen. Beim Bonusprogramm „Priceless Specials“ wurden persönliche Informationen wie Name, E-Mail-Adresse, Geburtsdatum, Geschlecht, Handy-/Telefonnummer oder Postanschrift abgegriffen. Selbst vollständige Kreditkartennummern kursierten im Netz.[1]

Auch die deutsche Chat-Community des unter Jugendlichen beliebten Flirt-Chats Knuddels wurde angegriffen:[2] 2018 drangen Hacker:innen in die Datenbank des Anbieters aus Karlsruhe ein und entwendeten sensible Daten der Nutzer:innen. Betroffen waren insgesamt rund 800.000 E-Mail-Adressen, ebenso Passwörter, Klarnamen und Wohnortangaben.[3]

Ende 2019 wurden die Daten von 267 Millionen Facebook-Nutzer:innen gehackt. Eine Datenbank mit Basisinformationen der Nutzer:innen befand sich rund zwei Wochen lang auf einem ungesicherten Server im Internet. Darunter waren Namen, Telefonnummern und die dazugehörigen User-IDs.[4]

Bei solchen Hacks, deren Liste sich um zahlreiche Beispiele verlängern ließe, und den davon betroffenen Daten, die dann im Netz für Angreifer:innen verfügbar sind, liegt das Problem zuallererst bei den Anbietern. Diese sichern die Passwörter und Datenbanken nicht ausreichend beziehungsweise belassen Passwörter im Klartext, anstatt diese „gehasht“, also vereinfacht gesagt verschlüsselt, abzuspeichern. Dadurch können die Passwörter von Kriminellen ausgelesen und ins Internet gestellt werden.

Ebenfalls problematisch ist das Passwortverhalten der Nutzer:innen. Wird für jeden Account dasselbe oder nur ein leicht abgewandeltes Passwort verwendet, stehen nach einem solchen Angriff nicht nur die Zugangsdaten zum gehackten Dienst im Netz, sondern gleich für alle Nutzerkonten der jeweiligen Person. So können Hacker:innen dann weitere Accounts auch bei nicht gehackten Anbietern übernehmen.

Da die Datensicherheit also nicht nur bei den Nutzer:innen, sondern vor allem auch bei den Dienstanbietern unzureichend ist, stellt jeder Account auch immer ein Sicherheitsrisiko dar. Es sollte daher stets überlegt werden, ob ein Account wirklich notwendig ist, und im Zweifel lieber

[1] https://www.verbraucherzentrale-rlp.de/aktuelle-meldungen/geld-versicherungen/datenleck-bei-mastercard-was-kreditkartenbesitzer-jetzt-tun-sollten-39272, Stand: 06/2023.

[2] https://www.computerbild.de/artikel/cb-News-Internet-Hack-Knuddels.de-22375657.html, Stand: 06/2023.

[3] https://www.sicher-im-netz.de/plattform-knuddelsde-wurde-gehackt, Stand: 06/2023.

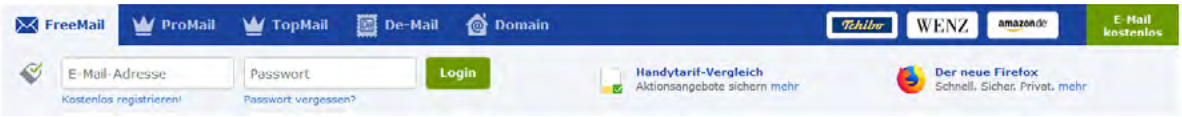
[4] https://www.heise.de/newsticker/meldung/Daten-von-267-Millionen-Facebook-Nutzern-offen-im-Netz-4621213.html, Stand: 06/2023.

kein Nutzerkonto angelegt werden. Wenn die Möglichkeit besteht, einen Dienst ohne Account zu nutzen, ist diese Variante die sicherere Wahl.

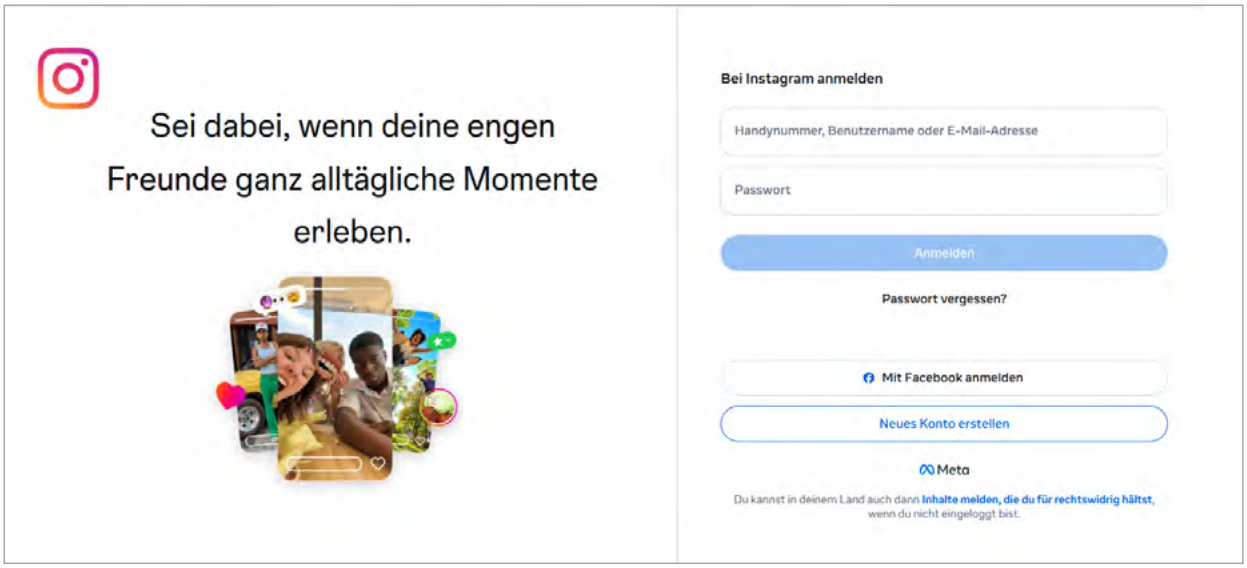
1.1 Was ist ein Account?

Um Onlinedienste wie Instagram, Amazon oder auch Google nutzen zu können, wird ein Account (auch „Konto“ genannt) benötigt. Ein Account ist ein „(Be-)Nutzerkonto“. Laut Duden bedeutet es Zugangsberechtigung, zum Beispiel zum Internet, einer Datenbank, einem Netzwerk oder ähnlichen Diensten.[5] Ein solches Nutzerkonto besteht aus einem Benutzernamen, der sehr häufig eine E-Mail-Adresse ist, und einem Passwort. Hat man einen Benutzernamen und ein Passwort angelegt, kann man sich mit diesen Zugangsdaten immer wieder auf der jeweiligen Internetseite in seinen Account einloggen.

Beispiel für einen Freemail-Account bei www.gmx.net[6]



Beispiel für einen Instagram-Account[7]



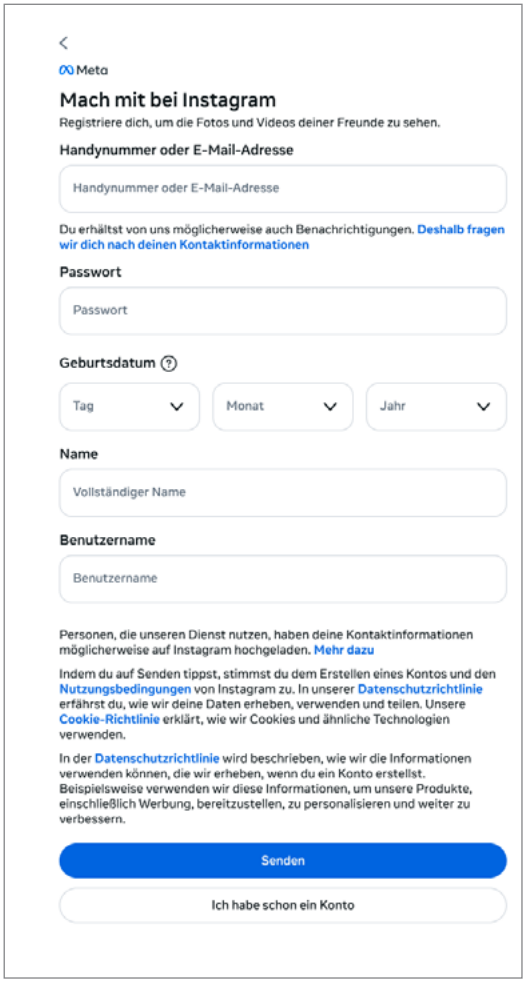
[5] https://www.duden.de/rechtschreibung/Account, Stand: 06/2023.

[6] https://www.gmx.net/, Stand: 06/2023.

[7] https://www.instagram.com, Stand 2026https://www.instagram.com, Stand 2026

Der jeweilige Onlinedienst speichert die von der Nutzerin oder dem Nutzer angegebenen Daten, sodass diese:r nach der Anmeldung immer wieder auf die Daten zugreifen kann, ohne sie erneut eingeben zu müssen. Das könnte beispielsweise die Adresse für den Onlineeinkauf oder den Navigationsdienst sein. Dabei sollte der Grundsatz der Datensparsamkeit immer beachtet werden. Je mehr Daten bei einem Onlinedienst hinterlassen werden, desto transparenter macht man sich.

Beispiel der erforderlichen Daten für einen Facebook-Account[8]



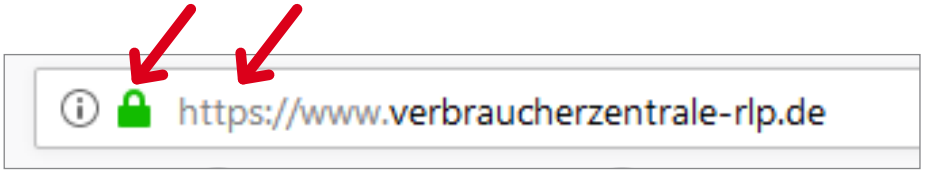
[8] https://de-de.facebook.com/, Stand: 06/2023.

Identifikation und Authentifizierung des Benutzers beziehungsweise der Benutzerin

Um sich in den eigenen Account einzuloggen, ist die Anmeldung mithilfe des Benutzernamens und des Passwortes notwendig. Auf diese Weise authentifiziert man sich als Besitzer:in des Kontos. Manche Anbieter legen begrüßenswerterweise genaue Vorgaben fest, die ein Benutzername und/oder Passwort erfüllen müssen, beispielsweise, dass ein Passwort Sonderzeichen, Zahlen sowie Groß- und Kleinschreibung enthalten soll.

Prinzipiell gilt, dass man ein kluges und vor allem langes Passwort auswählen sollte. Wie ein kluges Passwort aussieht, wird später in Abschnitt 6.2, „Sichere Passwörter“, genauer erklärt.

Außerdem sollten Nutzer:innen darauf achten, dass die Verbindung zum Onlinedienst verschlüsselt ist. Das erkennt man am „http**s**“ (statt „http“) in der Adresszeile des Browsers. Gängige Browser zeigen auch ein Schlosssymbol für sichere Verbindungen beziehungsweise umgekehrt eine Warnung, wenn die Seite nicht SSL-verschlüsselt ist. Unverschlüsselte Verbindungen erlauben es potenziellen Angreifer:innen, Benutzernamen und Passwort mitzulesen. Auf diese Weise könnten sie den Account dann mithilfe der ausgelesenen Zugangsdaten für eigene Zwecke missbrauchen.



Sollten Angreifer:innen die Zugangsdaten eines Onlinedienstes mitgelesen haben, besteht die Gefahr, dass mithilfe dieser Zugangsdaten auch bei anderen Diensten ein Missbrauch stattfinden könnte. Aus diesem Grund sollten niemals für mehrere Accounts die gleichen Zugangsdaten gewählt werden.

Wichtiger Tipp:

Niemals ein Passwort für mehrere Accounts verwenden!!!

2. Privatsphäre und Datenschutz

2.1 Grundrechte der Europäischen Union

Der Datenschutz ist in der gesamten EU durch die Datenschutz-Grundverordnung[9] (DSGVO) geregelt. In Deutschland wurde sie durch das Bundesdatenschutzgesetz[10] (BDSG) umgesetzt. Kernpunkt des BDSG ist es, personenbezogene Daten, also alle Daten, die zur Identifizierung einer Person verwandt werden können, bei ihrer Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung) vor Missbrauch zu schützen.

Nahezu jeder Mensch besitzt mittlerweile eine sogenannte digitale Identität, die sich aus den unterschiedlichsten Nutzungsweisen digitaler Medien und Endgeräte zusammensetzt. Diese digitale Identität kann – wissentlich oder unwissentlich – von anderen Internetnutzer:innen oder Firmen zu Zwecken verwendet werden, die den betroffenen Personen nicht bekannt sind.

2.2 „Ich habe doch nichts zu verbergen!“

Dieses Totschlagargument schwirrt schon seit vielen Jahren durch die unzähligen Diskussionen über digitale Massenüberwachung oder die Datensammelwut der großen Internetkonzerne.

Dazu der als Whistleblower bekannt gewordene Edward Snowden:

„Einige sagen vielleicht: ‚Es ist mir egal, ob sie meine Privatsphäre verletzen; ich habe nichts zu verbergen.‘ Wir müssen solchen Menschen helfen, dass sie verstehen, dass sie den grundlegenden Charakter der Menschenrechte falsch verstehen. Niemand muss sich rechtfertigen, warum er ein Recht ‚braucht‘: Die Rechtfertigungslast liegt bei dem, der versucht, das Recht zu verletzen.“ [11]

[9] https://dsgvo-gesetz.de, Stand: 06/2023.

[10] https://dsgvo-gesetz.de/bdsg/, Stand: 06/2023.

[11] https://www.steinger.ch/de/blog/nichts-zu-verbergen-argument, Stand: 06/2023.

Durch den häufig recht sorglosen Umgang der Menschen mit ihren Daten werden die digitalen Profile fleißig gefüttert. Welche Daten tatsächlich im Hintergrund gesammelt und verarbeitet werden, an wen und zu welchem Zweck diese Daten dann verkauft werden, erfahren die Nutzer:innen in der Regel nicht.

Freiwillig würden wir unserer Nachbarin wohl kaum die PIN unserer Bankkarte nennen. Wir würden unseren Arbeitskollegen auch nicht den gesamten Chatverlauf auf unserem Smartphone präsentieren. Gegenüber uns bekannten Menschen verbergen wir also Informationen, die wir völlig unbekannten Empfänger:innen bereitwillig – wenn häufig auch unwissentlich – zur Verfügung stellen.

Gerade bei Veröffentlichungen in sozialen Netzwerken (siehe hierzu Modul 4, „Soziale Netzwerke“) sollte hinterfragt werden, ob die angegebenen Informationen tatsächlich für die Allgemeinheit gedacht sind oder ob es nicht doch besser wäre, bestimmte Inhalte nur für bestimmte Personen(kreise) öffentlich zu machen.

Ein Beispiel:

Eine Auszubildende begab sich trotz einer ärztlich attestierten Arbeitsunfähigkeit in einen Spontanurlaub nach Mallorca. Auf Facebook postete sie während ihres Aufenthalts auf der Insel Unmengen Fotos und kommentierte, dass sie diverse Diskotheken besucht und sich sogar hatte tätowieren lassen. Nach der Rückkehr aus dem Urlaub fand die Auszubildende natürlich die Kündigung im Briefkasten.

Fazit: Bei der Preisgabe von Daten und Informationen sollte immer zweimal überlegt werden!

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

3. Gefahren im Netz durch (legale) Datensammler

Mit der häufig unreflektierten Nutzung von sogenannten Smart Speakern (wie beispielsweise Alexa), Smart Wearables (wie Smart Watches und Fitnessarmbänder), Streamingdiensten (zum Beispiel Netflix), datenschutzrechtlich mindestens fragwürdigen Messengerdiensten (wie WhatsApp) und vielen anderen Endgeräten und Apps versorgen wir die großen Onlinedienste mit einer unfassbaren Menge an Daten über uns: unsere Gewohnheiten, unser Kaufverhalten, unsere Bewegungsmuster, unsere Psyche – all das wird verarbeitet und von künstlichen Intelligenzen (KI) mit komplexen Algorithmen ausgewertet.

Aus rechtlicher Sicht ist dieses Sammeln und Verarbeiten von Daten im weitesten Sinne auch legal, denn die Nutzer:innen haben den (meist sehr umfangreichen und umständlich formulierten) Nutzungsbedingungen der jeweiligen Geräte oder Apps im Vorfeld bereits zugestimmt.

3.1 Wer sammelt Daten?

Nahezu jeder Anbieter von digitalen Endgeräten oder Apps sammelt mehr oder weniger Daten über die Nutzer:innen. Als häufigstes Argument wird dafür die „Verbesserung der Dienste für die Nutzer:innen“ genannt. Diese Aussage ist zwar nicht falsch, verschleiert jedoch den Umfang der gesammelten Daten und wofür diese Daten zusätzlich genutzt werden.

Nachfolgend eine Aufzählung der weltweit dominierenden „Datenkraken“[12] mit dem zugehörigen Mutterkonzern:

[12] https://de.wikipedia.org/wiki/Datenkrake, Stand: 06/2023.

Anbieter	Mutterkonzern
Google YouTube	Alphabet Inc., Kalifornien (USA)
Facebook Instagram WhatsApp	Meta Platforms, Inc., Kalifornien (USA)
Amazon	Amazon.com Inc., Seattle (USA)
TikTok	ByteDance, Peking (China)
Netflix	Netflix, Inc., Kalifornien (USA)
Tencent QQ WeChat WeGame Foxmail	Tencent Holdings Ltd., Shenzen (China)

Die Apps der Tencent Holdings sind vorrangig im asiatischen Raum verbreitet, während der europäische Markt von den US-amerikanischen Konzernen dominiert wird (mit Ausnahme von TikTok).

Auch Spiele- oder Streaming-Apps (wie Netflix) sammeln fleißig Daten und werten diese aus.

Am Beispiel von Netflix lässt sich das Sammeln der Daten anschaulich erklären: Wer häufig Komödien schaut, erhält in der Liste mit von Netflix vorgeschlagenen Filmen überwiegend Komödien. Wer eine bestimmte Serie geschaut hat, erhält sofort eine E-Mail, wenn eine neue Staffel der Serie verfügbar ist.

Ein weiteres Beispiel ist das Werbetracking von Amazon: Wer einmal einen bestimmten Artikel bei Amazon angesehen oder sogar auf den Wunschzettel gepackt hat, wird diesen Artikel künftig beim Surfen auf anderen Webseiten immer wieder als Werbung präsentiert bekommen, falls er keinen sogenannten Adblocker (Werbeblocker) installiert hat.

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

3.2 Welche Daten werden gesammelt und was passiert damit?

Die im vorigen Abschnitt genannte Art der Datensammlung und deren Ergebnisse erscheinen für Nutzer:innen zunächst hilfreich und praktisch. Doch leider werden sehr viel mehr Daten über die User:innen und deren Nutzung gesammelt, als die Mehrzahl der Menschen auch nur erahnen kann. In erster Linie geht es dabei um die Ermittlung von …

- Gewohnheiten
- Surfverhalten
- Interessen (Musik, Hobbys, Videos)
- Bewegungsprofilen (Arztbesuche und Ähnliches)
- Konsum- beziehungsweise Kaufverhalten
- Lebensereignissen
- persönlichen Daten
- Kontaktdaten anderer
- Haushaltseinkommen
- genutzten Apps

Einen besonderen Stellenwert haben die sogenannten Metadaten[13], die permanent und in der Regel ohne Wissen der Nutzer:innen insbesondere von Messengerdiensten gesammelt werden.

Dies stellt sich beim mittlerweile passenderweise in Meta umbenannten Konzern (ehemals Facebook) beispielhaft wie folgt dar:

Wer WhatsApp oder Instagram nutzt und ständig online ist, liefert permanent Bewegungsdaten an Meta. Somit weiß Meta, wo man wohnt, wo man (gelegentlich) übernachtet, wohin man reist, ob man das WLAN zu Hause, bei Freund:innen oder im Hotel nutzt, in welchem Funknetz man eingewählt ist und so weiter. So entsteht ein äußerst genaues Bewegungsprofil. Darüber hinaus kennt Meta das soziale Umfeld: Neben dem Zugriff auf die Kontaktdaten weiß das Unternehmen auch, wann und wie oft man mit seinen Kontakten interagiert, woraus sich wiederrum ermitteln lässt, ob es sich um enge Freund:innen oder um flüchtige Bekanntschaften handelt.

So entstehen erschreckend genaue psychologische Profile von sämtlichen Nutzer:innen. Eine KI kann daraus Verhaltensmuster errechnen und sogar den aktuellen Gemütszustand des Nutzers oder der Nutzerin ermitteln.

Inwieweit diese Informationen ausschließlich dazu dienen, die angebotenen „Dienste zu verbessern“, darf an dieser Stelle bezweifelt werden. Mit diesen geballten Informationen ist es nicht nur möglich, einzelne Menschen, sondern ganze Gesellschaften zu beeinflussen und zu manipulieren (siehe Cambridge-Analytica-Skandal von 2018)[14].

[13] https://de.wikipedia.org/wiki/Metadaten, Stand: 06/2023.

[14] https://netzpolitik.org/2020/abschlussbericht-der-datenschutzbehoerde-nein-der-cambridge-analytica-skandal-faellt-nicht-in-sich-zusammen/, Stand: 06/2023.

3.3 Nicht alle Apps sammeln Daten – Alternativen

Tatsächlich gibt es auch zahlreiche Apps, die überhaupt keine oder nur sehr wenige Daten sammeln. Meistens handelt es sich dabei um „Open-Source-Entwicklungen“ oder kostenpflichtige Apps.

„Als Open Source (wörtlich aus dem Englischen übersetzt: „offene Quelle“) wird Software bezeichnet, deren Quelltext öffentlich und von Dritten eingesehen, geändert und genutzt werden kann. Open-Source-Software kann meist kostenlos genutzt werden.“

„Software kann sowohl von Einzelpersonen aus altruistischen Motiven zu Open-Source-Software gemacht werden wie auch von Organisationen oder Unternehmen, um Entwicklungskosten zu teilen oder Marktanteile zu gewinnen.“[15]

Eines der bekanntesten Beispiele für Open Source ist das alternative Betriebssystem Linux.

Auch bei kostenpflichtigen Apps kann man jedoch nicht grundsätzlich davon ausgehen, dass keine oder nur sehr wenige Daten gesammelt werden, daher empfiehlt sich auch dort immer ein genauerer Blick in die Nutzungsbedingungen.

Eine Einschätzung des Datensendeverhaltens einer App ermöglicht auch der Appchecker des Portals Mobilsicher (https://appcheck.mobilsicher.de).

[15] https://de.wikipedia.org/wiki/Open_Source, Stand: 06/2023.

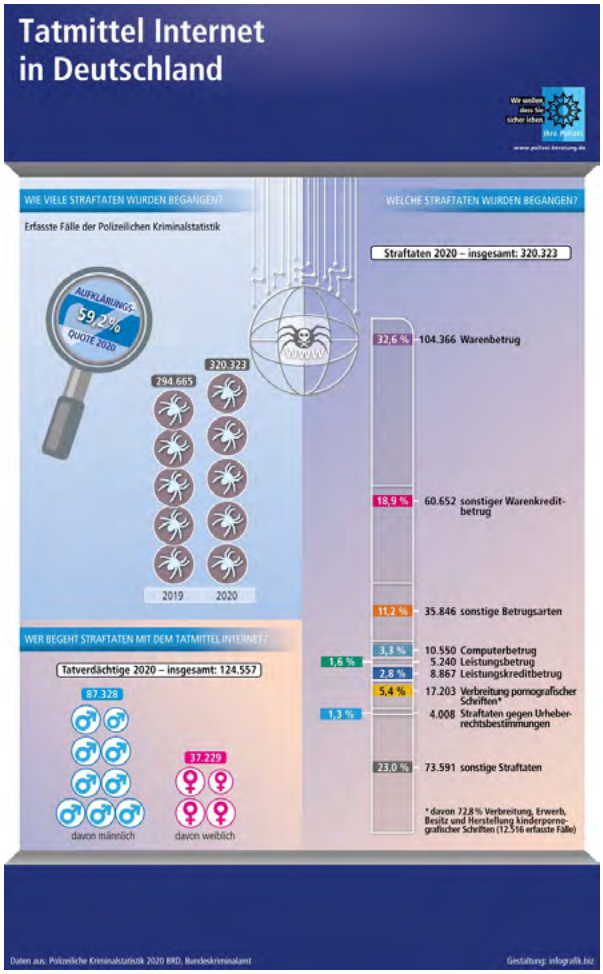
4. Gefahren im Internet durch Kriminelle

Die in den letzten Jahren stark zunehmenden Fallzahlen im Bereich Cyberkriminalität[16] vermitteln zwar zunächst einen anderen Eindruck – und die Methoden der Kriminellen werden tatsächlich immer ausgefeilter und trickreicher –, dennoch kann man sich verhältnismäßig einfach schützen.

Im Gegensatz zur Cyberkriminalität bei Unternehmen handelt es sich im privaten Bereich nur selten um gezielte Angriffe auf einzelne Personen, sondern um pauschale Betrugsversuche an bestimmten Nutzergruppen.

Wie aus der zuvor gezeigten Grafik zu entnehmen ist, handelt es sich bei etwas mehr als 70 Prozent der verfolgten Straftaten um Betrugsdelikte finanzieller Art.

Wie bereits erwähnt, ist in der Regel nicht eine bestimmte Person Ziel von Cyberkriminalität, sondern eine bestimmte Nutzergruppe. Der gezielte Angriff auf einzelne Privatpersonen wäre für eine:n Hacker:in viel zu aufwendig und führt nur selten zum Erfolg, deshalb ist eine große Anzahl von User:innen ein viel lohnenderes Ziel. Solche Hackversuche geschehen häufig durch E-Mail-Phishing (siehe Abschnitt 4.1, „E-Mail-Phising“) oder die meist heimliche Installation einer Schadsoftware auf dem PC, Laptop, Smartphone oder Tablet.



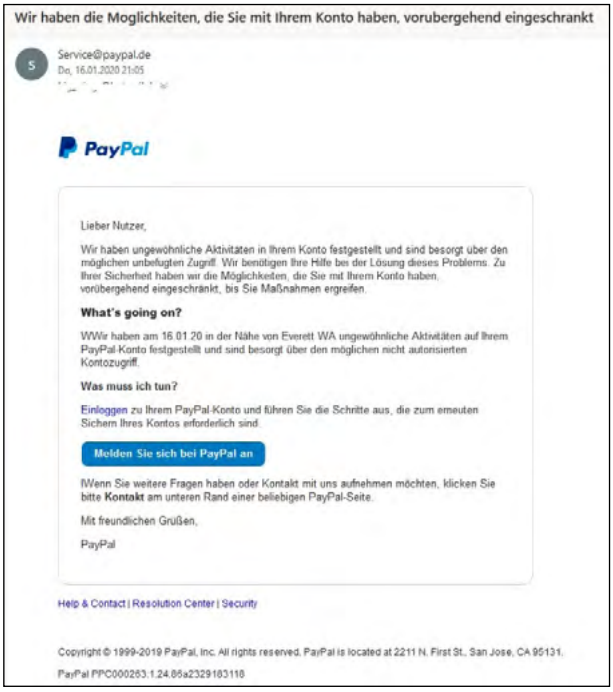
Quelle: Polizeiliche Kriminalprävention der Länder und des Bundes (http://www.polizei-beratung.de, Stand: 26.05.2023)

[16] https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html, Stand: 06/2023.

Ziel ist in den meisten Fällen das illegale Abgreifen von Zugangsdaten, zum Beispiel zu Bank- und E-Mail-Konten, Accounts von Zahlungsdienstleistern (wie PayPal) oder großen Shops (beispielsweise Amazon). Gelegentlich kommt es auch vor, dass Erpressungstrojaner die eigene Festplatte verschlüsseln und die Entschlüsselung an die Zahlung einer bestimmten Summe (meistens in einer bekannten Kryptowährung) gebunden wird. Letzteres findet man im privaten Bereich bisher aber nur sehr selten. Sollte es dennoch vorkommen, sollte man sich sofort bei der Polizei melden.

4.1 E-Mail-Phishing

Das Wort „Phishing“ setzt sich zusammen aus den englischen Begriffen „password harvesting“ (zu Deutsch etwa: „Passworternte“) und „fishing“ (zu Deutsch: „angeln“).


Wir haben die Moglichkeiten, die Sie mit Ihrem Konto haben, vorubergehend eingeschrankt

Service@paypal.de
Do, 16.01.2020 21:05

PayPal

Lieber Nutzer,

Wir haben ungewöhnliche Aktivitäten in Ihrem Konto festgestellt und sind besorgt über den möglichen unbefugten Zugriff. Wir benötigen Ihre Hilfe bei der Lösung dieses Problems. Zu Ihrer Sicherheit haben wir die Möglichkeiten, die Sie mit Ihrem Konto haben, vorübergehend eingeschränkt, bis Sie Maßnahmen ergreifen.

What's going on?

WWir haben am 16.01.20 in der Nähe von Everett WA ungewöhnliche Aktivitäten auf Ihrem PayPal-Konto festgestellt und sind besorgt über den möglichen nicht autorisierten Kontozugriff.

Was muss ich tun?

Einloggen zu Ihrem PayPal-Konto und führen Sie die Schritte aus, die zum erneuten Sichern Ihres Kontos erforderlich sind.

Melden Sie sich bei PayPal an

IWenn Sie weitere Fragen haben oder Kontakt mit uns aufnehmen möchten, klicken Sie bitte **Kontakt** am unteren Rand einer beliebigen PayPal-Seite.

Mit freundlichen Grüßen,

PayPal

Help & Contact | Resolution Center | Security

Copyright © 1999-2019 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.

PayPal PPC000263.1.24.66a2329183118

Beispiel für eine Phishing-E-Mail mit dem vermeintlichen Absender „PayPal“ (Screenshot vom 16.10.2020)

Wenn Spam-Mails mit gefälschtem Absender – beispielsweise als Bank, Internetanbieter oder Shop getarnt – die Empfänger:innen zur Aktualisierung von persönlichen Daten auffordern (zum Beispiel Nutzerdaten, Passwörter, Kontonummern und andere) und in der E-Mail auf einen bestimmten Link oder einen auffälligen Button geklickt werden soll, dann handelt es sich in den meisten Fällen um einen Phishing-Versuch. Gelockt wird häufig mit dem Vorwand, dass es einen Sicherheitsverstoß im Account gebe, eine Kreditkarte bald ablaufe oder eine Kontoaktualisierung erforderlich sei. Da die Kriminellen darauf spekulieren, dass eine große Anzahl der E-Mail-Empfänger:innen gleichzeitig auch Kund:innen der genannten Organisation sind, werden meistens bekannte Banken und Firmen wie Sparkassen, Volks- und Raiffeisenbanken, PayPal, Amazon und die großen Freemail-Anbieter wie Web.de, GMX und andere als Absender vorgetäuscht.

Die Phishing-Mails sind optisch von den „echten“ E-Mails der jeweiligen Organisationen kaum zu unterscheiden. Aufbau, Logo, Farben, Schriftart – all das erweckt zunächst den Eindruck der Echtheit. Klickt man im weiteren Verlauf auf den in der Phishing-Mail angezeigten Button oder Link, landet man oftmals auf einer Webseite, die optisch ebenso echt wirkt. Wenn man nun auf dieser gefälschten Webseite die geforderten Daten eingibt, haben die Betrüger:innen ihr Ziel erreicht.

Auch Posts in sozialen Netzwerken können auf gefälschte Webseiten führen. Hierbei sind weniger Banken oder große Dienstleistungsunternehmen das Ziel, sondern vor allem bekannte Markennamen. Das Ziel der Phishing-Betrüger:innen bleibt jedoch identisch: Vertrauen erschleichen und persönliche Daten abgreifen.

Wie man Phishing erkennt und sich davor schützen kann, ist im Abschnitt 6.10, „E-Mail- oder Nachrichten-Phishing erkennen“, detailliert beschrieben.

4.2 Schadsoftware per E-Mail

Schadsoftware verbreitet sich regelmäßig über den E-Mail-Verkehr. Dabei wird der Schadcode häufig in eine „.zip-Datei“[17] gepackt, um während der Übertragung nicht erkannt zu werden. Wird diese Datei auf dem Computer entpackt, installiert sich – meist unbemerkt – die Schadsoftware. Nutzer:innen werden über bestimmte Formulierungen in diesen Mails dazu verleitet, die Anhänge zu öffnen. In solchen E-Mails geht es beispielsweise um eine angebliche Urheberrechtsverletzung, eine getätigte Bestellung oder eine nicht beglichene Rechnung.

Ähnlich häufig sind die schädlichen Anhänge als Word-Dokumente (Endung „.doc“/„.docx“) oder Excel-Dateien (Endung „.xls“/„.xlsx“) getarnt. Beim Öffnen der Dateien werden dann entweder schädliche Makros[18] ausgeführt oder Links in den Dokumenten und Tabellen aktiviert, die wiederum den Rechner kontaminieren. Die neueren Formate mit den Endungen „.docx“ oder „.xlsx“ können laut Microsoft aber keine Markos mehr enthalten, sodass hier gegenüber den älteren Formaten ohne x eine deutlich geringere Gefahr besteht.

Häufige Vorwände, die zum Öffnen der Anhänge verleiten sollen

- **Abmahnung:**
  Personen werden beschuldigt, urheberrechtlich geschützte Dateien, Filme oder Ähnliches heruntergeladen zu haben. Genauere Angaben befänden sich in der Unterlassungserklärung, die im Anhang der Mail zu finden sei. Absender ist vermeintlich eine Staatsanwaltschaft. Aufgrund des Absenders sieht man sich gezwungen, der Aufforderung nachzukommen und den Anhang zu öffnen. Doch genau das sollte man nicht tun. Keine Staatsanwaltschaft oder sonstige öffentliche Stelle würde ein derartiges Dokument als Zip-Anhang verschicken.

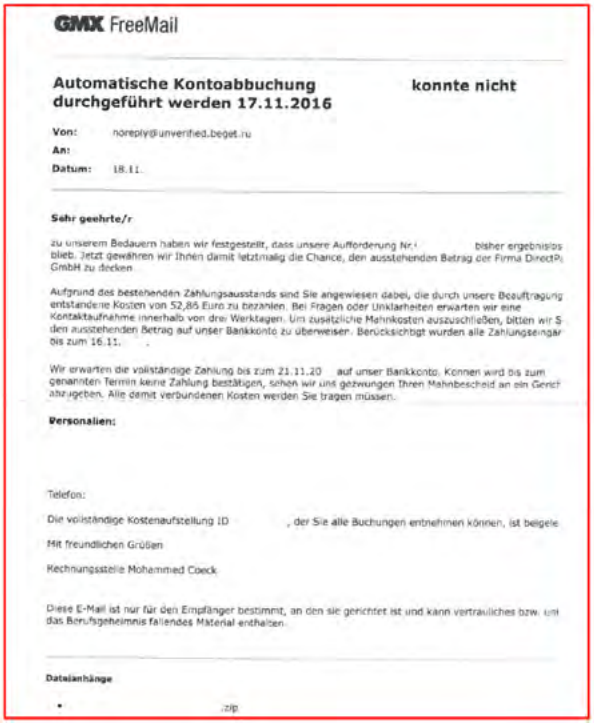
- **Bestellung:**
  Eine angeblich getätigte Bestellung wird bestätigt. Im E-Mail-Anhang befänden sich die Details zum angeblich erworbenen Produkt. Selbst wenn man sich sicher ist, keine Bestellung getätigt zu haben, ist man oft dennoch neugierig und öffnet den Dateianhang. Das sollte man aber gerade nicht tun.

[17] https://de.wikipedia.org/wiki/ZIP-Dateiformat, Stand: 06/2023.

[18] https://de.wikipedia.org/wiki/Makro, Stand: 06/2023.

- **Rechnung:**
  Ein Telefonanbieter stellt eine angebliche Forderung eines Drittanbieters in Rechnung. Die Empfängerin oder der Empfänger der E-Mail soll eine hohe Summe zahlen. Der Nachweis der Forderung sei dem Anhang zu entnehmen. Die Signatur erweckt den Eindruck, die Mail stamme vom Anbieter selbst. Tatsächlich ist die E-Mail aber eine Fälschung. Sollte der Telefonanbieter eine Forderung eines Dritten geltend machen, dann würde diese in der offiziellen Rechnung stehen und nicht in irgendeinem Dateianhang. Auch bei solchen Aufforderungen sollte man skeptisch sein und sich nicht zum Klick auf den Anhang verleiten lassen. Rechnungen können in der Regel auch über ein Kundenportal heruntergeladen werden.

Beispiel für versteckte Schadsoftware in einem E-Mail-Anhang:



GMX FreeMail

Automatische Kontoabbuchung konnte nicht durchgeführt werden 17.11.2016

Von: noreply@unverified.beget.ru
An:
Datum: 18.11.

Sehr geehrte/r

zu unserem Bedauern haben wir festgestellt, dass unsere Aufforderung Nr. bisher ergebnislos blieb. Jetzt gewähren wir Ihnen damit letztmalig die Chance, den ausstehenden Betrag der Firma DirectPa GmbH zu decken.

Aufgrund des bestehenden Zahlungsausstands sind Sie angewiesen dabei, die durch unsere Beauftragung entstandene Kosten von 52,86 Euro zu bezahlen. Bei Fragen oder Unklarheiten erwarten wir eine Kontaktaufnahme innerhalb von drei Werktagen. Um zusätzliche Mahnkosten auszuschließen, bitten wir S den ausstehenden Betrag auf unser Bankkonto zu überweisen. Berücksichtigt wurden alle Zahlungseingar bis zum 16.11.

Wir erwarten die vollständige Zahlung bis zum 21.11.20 auf unser Bankkonto. Können wird bis zum genannten Termin keine Zahlung bestätigen, sehen wir uns gezwungen Ihren Mahnbescheid an ein Gericht abzugeben. Alle damit verbundenen Kosten werden Sie tragen müssen.

Personalien:

Telefon:

Die vollständige Kostenaufstellung ID , der Sie alle Buchungen entnehmen können, ist beigele

Mit freundlichen Grüßen

Rechnungsstelle Mohammed Coeck

Diese E-Mail ist nur für den Empfänger bestimmt, an den sie gerichtet ist und kann vertrauliches bzw. un das Berufsgeheimnis fallendes Material enthalten.

Dateianhänge

• .zip

Beispiel für eine Spam-E-Mail mit dem vermeintlichen Absender „GMX“ (Screenshot vom 16.10.2020)

In diesem Beispiel wird suggeriert, dass bereits eine Aufforderung erfolgt sein soll. Dies ist aber in den meisten Fällen gerade nicht geschehen. Viele Menschen lassen sich dennoch verunsichern, weil der Eindruck entsteht, es sei Eile geboten. Dies wird durch die Aussage verstärkt, dass bei Fragen oder Unklarheiten nur innerhalb der nächsten drei Werktage eine Klärung herbeigeführt werden könne. Wendet man sich per E-Mail an den Absender, ist keine Antwort zu erwarten, da es sich um eine „noreply@“-Adresse handelt. Um überhaupt Kontakt aufnehmen zu können, ist man also gezwungen, auf den Anhang zu klicken.

4.3 Schadsoftware durch Webseiten-Downloads

Schadsoftware erhält man jedoch nicht nur durch das unbedachte Klicken auf Anhänge in E-Mails. Auch im rechtlichen Graubereich angesiedelte Plattformen und Websites, die den kostenlosen Download von Videos, Kinofilmen, Software, Bildern, Spielen und so weiter anbieten, sind häufig mit Schadsoftware kontaminiert.

Doch selbst durch den Besuch einer legalen und seriösen Internetseite kann entsprechende Schadsoftware auf den Rechner gelangen, häufig durch sogenannte Drive-by-Downloads[19]. Die primäre Schwachstelle ist dabei der Browser. Aktive Funktionen wie Flash, Java, ActiveX – die eigentlich dem Komfort dienen – können das Laden und Starten von schädlichen Programmcodes auslösen.

Im Januar 2013 beispielsweise haben Unbekannte die Internetseite des Technikportals PC-Welt manipuliert und die Endgeräte Tausender Besucher:innen per Drive-by-Download infiziert. Der schädliche Code befand sich 24 Stunden unbemerkt auf der Website. Nur einen Monat später wurde die zentrale Internetseite der Sparkassen als Malware-Schleuder missbraucht. Auch hier kam ein Drive-by-Schädling zum Einsatz. Diese zwei Beispiele zeigen, dass auch sichere und vertrauenswürdige Internetseiten Drive-by-Viren verbreiten können.

Die Folgen von Drive-by-Downloads sind zum Beispiel die nach wie vor sehr beliebten Erpressungstrojaner. Diese geben vor, im Auftrag der Bundespolizei oder GEMA zu handeln, und behaupten, dass auf dem Computer des Opfers urheberrechtlich geschütztes Material oder sogar illegale Pornografie gefunden und der Computer aus diesem Grund gesperrt worden sei. Für die Freigabe des Computers soll, über anonyme Zahlungsmittel wie Bitcoin, Ukash oder Paysafecard, ein Betrag von 100 Euro und mehr gezahlt werden. Natürlich bleibt der PC auch nach Zahlung des geforderten Betrags gesperrt. Und dieses Geschäftsmodell funktioniert: Immer wieder zahlen Geschädigte – laut einiger Studien sogar bis zu einem Drittel der Betroffenen – den geforderten Betrag, um wieder an ihre Daten zu kommen.

Wie man sich davor schützen kann, ist in den Abschnitten 6.12, „Antivirenprogramme ja oder nein? – Jein!“, und 6.14, „Sinnvolle Browser, Suchmaschinen und Add-ons“, detailliert beschrieben.

[19] https://de.wikipedia.org/wiki/Drive-by-Download, Stand: 06/2023.

4.4 Besonders gefährlich: Identitätsdiebstahl

Fremde missbrauchen die Identitäten von Verbraucher:innen in diversen Bereichen. Mithilfe der ergaunerten Daten werden im Internet kostenpflichtige Abonnements zum Beispiel für Video-streamingdienste abgeschlossen, Nutzerkonten bei kostenpflichtigen Mail-Konten eingerichtet und im Namen der Geschädigten Waren bestellt.

Die Betroffenen erfahren meist erst vom Identitätsdiebstahl, wenn sie Rechnungen oder Inkasso-schreiben erhalten oder unbekannte Abbuchungen auf ihrem Konto vorfinden.[20]

Zehn Fakten:

1. **Identitätsdiebstahl ist der Missbrauch eurer Daten.**
   Beim Identitätsdiebstahl benutzt jemand eure Daten und täuscht vor, ihr zu sein. Häufig werden die Daten für betrügerische Handlungen missbraucht, vor allem im Internet. Die Täter:innen bestellen zum Beispiel Waren unter eurem Namen und greifen die Lieferungen ab. Oder es werden Profile unter eurer Identität in sozialen Medien oder auf Verkaufsportalen angelegt.

2. **Schon wenige Daten reichen aus.**
   Leicht zugängliche Daten wie Name, Adresse und Geburtsdatum reichen oft schon aus, um eine falsche Identität vorzutäuschen.

3. **Daten und Datendieb:innen sind überall.**
   Datendieb:innen nutzen viele Methoden: Schadprogramme auf PC oder Smartphone, Phishing per E-Mail oder Telefon, gehackte Social-Media-Accounts oder frei zugängliche Informationen im Internet. Sogar ein Blick auf das Klingelschild oder in die Papiermülltonne kann zum Erfolg führen.

4. **Alle Daten sind wertvoll.**
   Angriffe zielen häufig direkt auf wirtschaftlich nutzbare Informationen wie Bank- oder Log-in-Daten. Aber auch E-Mail- und Social-Media-Accounts sind oft betroffen. Hier finden sich massenweise private Informationen über euch wie auch über eure Freund:innen und Kommunikationspartner:innen.

5. **Datenlecks machen uns besonders verletzlich für weitere Angriffe.**
   Wer private Informationen über euch hat, kann andere Menschen oder euch selbst leicht täu-schen.

[20] https://www.verbraucherzentrale-rlp.de/wissen/digitale-welt/datenschutz/welche-folgen-identitaetsdiebstahl-im-internet-haben-kann-17750, Stand: 06/2023.

6. **Euer guter Ruf kann massiv Schaden nehmen.**
   Alles, was Datendieb:innen in eurem Namen tun, fällt zunächst auf euch zurück: egal, ob sie Unternehmen betrügen, auf Facebook pöbeln, Onlineabzocke betreiben oder ein Bankkonto eröffnen und für Geldwäsche nutzen.

7. **Eine Strafanzeige bei der Polizei ist unerlässlich.**
   Eine Strafanzeige ist also unbedingt notwendig, wenn ihr von Identitätsdiebstahl betroffen seid. Nur so könnt ihr euch gegen Ansprüche und Vorwürfe wehren.

8. **Technischer Datenschutz und Datensparsamkeit helfen.**
   Regeln der IT-Sicherheit beachten, Software aktuell halten, sichere Passwörter und Zwei-Faktor-Authentifizierung verwenden und Vorsicht bei der Nutzung ungesicherter Netzwerke und Verbindungen walten lassen – all das hilft beim Schutz vor Identitätsdiebstahl. Datensparsamkeit ist das A und O.

9. **Misstrauen ist gesund.**
   Ein kritischer Blick darauf, wer mein Gegenüber ist und warum ich persönliche Daten preisgeben soll, hilft ebenfalls, sich zu schützen.

10. **Kein Grund zu falscher Scham!**
    Auch wer noch so vorsichtig und datensparsam ist, kann letztlich zum Opfer werden. Datendieb:innen sind kriminell und nutzen unsere Schwachstellen ganz gezielt aus. Sprecht mit euren Eltern oder anderen Vertrauenspersonen, wenn ihr etwas Verdächtiges festgestellt habt.

Was ist zu tun, wenn ich Opfer eines Identitätsdiebstahls geworden bin?

Wer von einem Identitätsdiebstahl betroffen ist, sollte schnellstmöglich betroffene Accounts sperren lassen und die Zugangsdaten ändern, um weitere Schäden zu verhindern. Außerdem sollte geprüft werden, ob weitere Accounts betroffen sind. Auch sollten andere Betroffene wie Firmen, bei denen eingekauft wurde, oder Freund:innen, an die gefälschte Nachrichten verschickt wurden, schnellstmöglich informiert werden.

Weitere Tipps und vertiefte Hinweise finden sich auf der Website der Verbraucherzentrale.[21]

[21] https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/welche-folgen-identitaetsdiebstahl-im-internet-haben-kann-17750, Stand: 06/2023.

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

5. Weitere Gefahrenquellen

5.1 Datenlecks bei Anbietern

Von einem Datenleck (englisch: „leak“) spricht man, wenn private Daten, die Personen bei einem Unternehmen hinterlegt haben, absichtlich (zum Beispiel durch Kriminelle) oder unabsichtlich (zum Beispiel durch technische Schwachstellen) öffentlich gemacht werden. Besonders anfällig für solche Hacks sind ungesicherte Datenbanken mit Kundendaten.

Abgesehen haben es die Cyberkriminellen meist auf folgende Daten:

- **Benutzernamen und Passwörter**
  Unternehmen sollten sensible Informationen wie Passwörter nicht im Klartext, sondern „gehasht“ (also verschlüsselt) speichern. Da sie das jedoch nicht immer tun oder das Niveau der Verschlüsselung teilweise nicht ausreichend hoch ist, kommt es immer wieder zur Offenlegung von Passwörtern, so auch bei dem eingangs erwähnten Angriff auf den Chat-Anbieter Knuddels im Jahr 2018. Mit den so erhaltenen Zugangsdaten versuchen Cyberkriminelle dann, Zugriff auf andere Dienste zu erlangen.

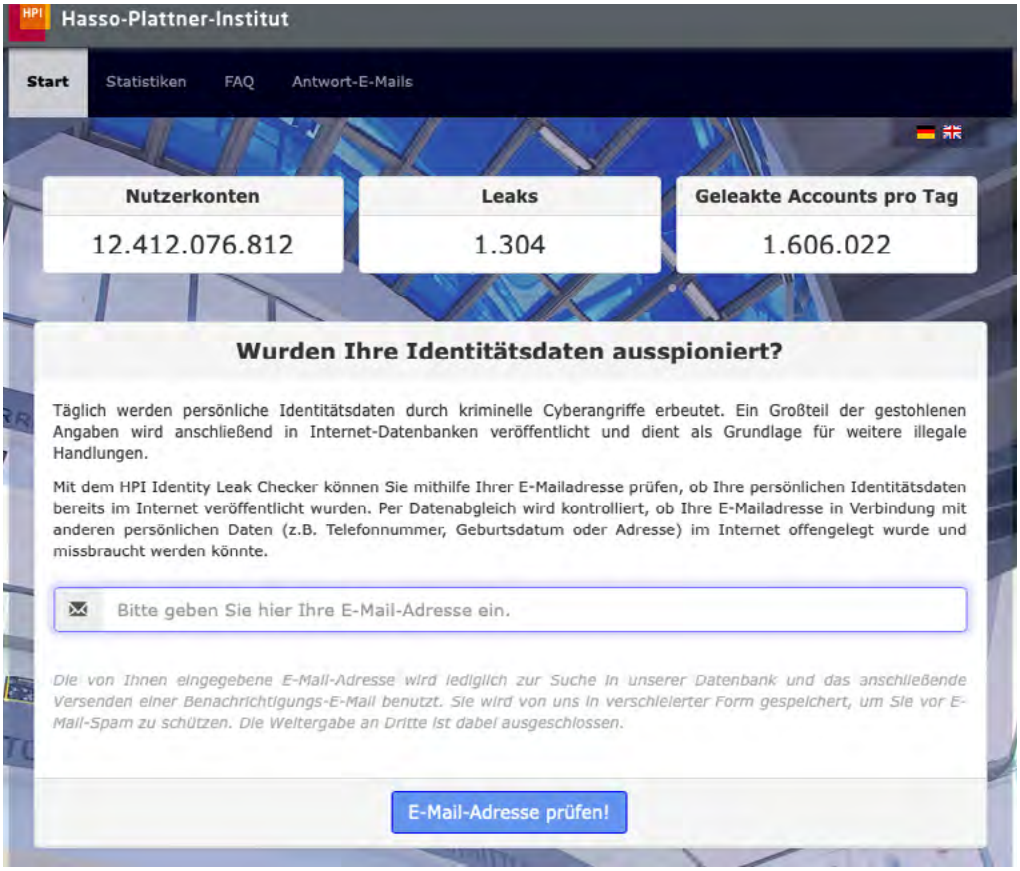
- **E-Mail-Adressen**
  Wenn eine E-Mail-Adresse mitsamt Passwort in die falschen Hände gerät, kann sie für Spam-, Phishing- oder Erpresser-Mails verwendet werden. Außerdem dienen die E-Mail-Adressen als Benutzername bei zahlreichen Internetdiensten.

- **Persönliche Daten**
  Es gibt noch viele weitere persönliche Daten, die gestohlen und missbraucht werden können, zum Beispiel Adressen, Geburtsdaten und so weiter. Mit diesen Informationen können Kriminelle Identitätsdiebstahl betreiben und beispielsweise unter falschem Namen Geschäfte im Internet abschließen (siehe Abschnitt 4.4, „Besonders gefährlich: Identitätsdiebstahl“).

Wie lässt sich feststellen, ob man von einem Datenleck betroffen ist?
Gerade bei großen und öffentlichkeitswirksamen Datenlecks werden die „geleakten“ Daten von zahlreichen Anbietern gesammelt und in entsprechende Datenbanken integriert. Mit einer entsprechenden Anfrage lässt sich dann herausfinden, ob die eigene E-Mail-Adresse(n) von dem Leak betroffen ist beziehungsweise sind.

HPI Identity Leak Checker (https://sec.hpi.de/ilc/)

Der Identity Leak Checker des Hasso-Plattner-Instituts überprüft durch einen Datenabgleich, ob eine E-Mail-Adresse in Verbindung mit persönlichen Daten wie Adresse, Geburtsdatum oder Telefonnummer im Netz offengelegt wurde. Nach Eingabe einer E-Mail-Adresse erhält man eine Tabelle zugeschickt, in der steht, welche Daten bei welchen Diensten betroffen waren.



Quelle: https://sec.hpi.de/ilc/ (Screenshot 04.08.2021)

Weitere Leak-Checker:

- Have I been pwned (https://haveibeenpwned.com)
  nur auf Englisch verfügbar

- Experte.de E-Mail Check (https://www.experte.de/email-check)
  auf Deutsch übersetzte Abfrage von Have I been pwned

- Leak Checker der Universität Bonn (https://leakchecker.uni-bonn.de/)
  deutschsprachig mit separater Datenbank

Was ist zu tun, wenn man von einem solchen Datenleck betroffen ist?

Zunächst ist in jedem Fall umgehend das Passwort des betroffenen Accounts zu ändern. Anschließend sollten die Passwörter bei allen Diensten mit demselben Passwort ebenfalls geändert werden.

Idealerweise sollte man für jeden Account ein anderes, einmaliges Passwort verwenden!

Sollte es nach einem solchen Datenleck vermehrt zu Phishing- oder Spam-Mails kommen, gibt es nur zwei Möglichkeiten: ignorieren oder eine neue E-Mail-Adresse anlegen.

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

5.2 Fehlende Jugendschutzeinstellungen

Allzu häufig geschehen ungewollte Onlinekäufe über Eltern-Accounts, weil keine Schutzmaßnahmen getroffen wurden. Typischerweise erfolgt der Missbrauch hier über Familiengeräte, wie gemeinsam genutzte Tablets, die ohne weitere Hürden Käufe in Apps ermöglichen (siehe Modul 2, Abschnitt 1.2, „Wie finanzieren sich kostenlose Apps?“). Aber auch Smartphones der Kinder, die ohne ausreichende Umsicht eingerichtet wurden, sind eine immer wiederkehrende Ursache für ungewollte Rechnungen bei den Eltern. Denn ohne Einschränkungen und sichere Passwörter besteht ein schrankenloser Zugriff auf Papas oder Mamas Kreditkarte.

Ein typischer Beispielfall aus dem Beratungsalltag der Verbraucherzentralen:

Ein Vater wandte sich an die Verbraucherzentrale, weil von seiner Kreditkarte rund 600 Euro abgebucht wurden. Er berichtete, dass sein minderjähriger Sohn am Wochenende bei ihm gewesen sei. Da er noch arbeiten musste, ließ er seinen Sohn auf seinem Tablet spielen. Da er seine Kreditkarte als Zahlungsmittel hinterlegt hatte und keine Sicherheitsvorkehrung für die Auslösung eines Bezahlvorgangs eingestellt hatte, konnte der Junge durch einen einfachen Klick Zubehör für sein Onlinegame erwerben.

Fazit: Der App-Store wies die Reklamation mit dem Hinweis zurück, dass der Vater Schutzvorkehrungen hätte einrichten müssen. Letztlich erstattete der App-Store die Hälfte der entstandenen Kosten. Die Bearbeitung und die damit verbundene Hoffnung auf Erstattung der abgebuchten Beträge ist oftmals schwierig, weshalb die Accounts der Eltern und insbesondere die Zahlungsmodalitäten unbedingt abgesichert sein sollten.

Mehr dazu findet man im Modul 2, Abschnitt 1.4 „Wie bezahlt man kostenpflichtige Apps?/Minderjährige und Verträge“.

Tipp: Die Kaufmöglichkeiten sollten durch Passwortsperren geschützt werden oder am besten nur Prepaidkarten als Zahlungsmittel hinterlegt werden.

Schritt-für-Schritt-Anleitungen zur Einrichtung auf Smartphones mit Android und iOS sowie unter Windows 10 und auch in YouTube finden sich hier:

- Für Android: https://www.heise.de/tipps-tricks/Android-Kindersicherung-einrichten-3984668.html, Stand: 06/2023.
- Für iOS: https://www.heise.de/tipps-tricks/iPhone-Kindersicherung-einrichten-so-geht-s-4423697.html, Stand: 06/2023.

5.3 Unsichere Netzwerke

Ungesicherte beziehungsweise schlecht abgesicherte WLAN-Netze ermöglichen es Kriminellen, den Datenverkehr einfach mitzuschneiden und somit auf persönliche Nutzerdaten zuzugreifen. Insbesondere das auf den Routern oder deren Verpackung aufgedruckte WLAN-Passwort stellt eine erhebliche Sicherheitslücke dar. Im Internet finden Angreifer Listen mit den Passwörtern der einzelnen Router-Hersteller und können sich so unter Umständen schnell Zugriff auf das WLAN unbedarfter Haushalte verschaffen. Aus diesen Gründen sollte der heimische Router geschützt werden.[22]

Informationen zum Schutz von heimischen Routern findet man hier:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Router-WLAN-VPN/Sicherheitstipps-fuer-privates-und-oeffentliches-WLAN/sicherheitstipps-fuer-privates-und-oeffentlicheswlan_node.html, Stand: 06/2023.

[22] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Router-WLAN-VPN/Sicherheitstipps-fuer-privates-und-oeffentliches-WLAN/sicherheitstipps-fuer-privates-und-oeffentliches-wlan_node.html, Stand: 06/2023.

6. Wie kann man sich und seine Daten schützen?

Das Wichtigste in aller Kürze:

- Absoluten Schutz gibt es nicht, trotzdem ist Vorsorge besser als Nachsorge, um das Risiko von Datenklau zu reduzieren.
- Vorsorge bedeutet insbesondere:
  - Sichere Passwörter verwenden!
  - Jeder Account bekommt ein eigenes Passwort.
  - Passwortmanager helfen beim Verwalten vieler Passwörter.
- Mit Zwei-Faktor-Authentifizierung (2FA) sollte man alle Zugänge zusätzlich absichern, auf jeden Fall aber den Passwortmanager, den E-Mail-Dienst sowie weitere besonders gefährdete Zugänge.
- Eine automatisierte regelmäßige Datensicherung schützt im Fall der Fälle.
- Misstrauen und Datensparsamkeit schützen im Netz vor vielen Gefahren.
- Um sich vor Spam-Mails zu schützen, empfiehlt es sich, eine Zweit-E-Mail-Adresse zu verwenden. Diese kommt immer dann bei der Registrierung bei einem neuen Dienst zum Einsatz, wenn man sich unsicher ist, ob der Anbieter die E-Mail-Adresse nicht unberechtigt weitergibt.
- Die Nutzung von unbekannten oder öffentlichen WLANs zur Übertragung sensibler Daten wie bei Onlinebanking oder -shopping sollte man vermeiden.
- Auch wer Daten oder E-Mails verschlüsselt, verwehrt Unberechtigten den Zugriff.
- Jugendschutzeinstellungen sind wichtig, sollten von Eltern aber nicht als Druckmittel eingesetzt werden.
- Mit alternativen Apps ist man häufig datensparsamer unterwegs.
- Standard-Antivirensysteme wie Microsoft Defender (Windows) und Co. sind meist ausreichend, wenn man regelmäßig die Sicherheitsupdates installiert. Allerdings sammeln sie selbst Daten zu Analysezwecken und werten sie aus – dessen sollte man sich bewusst sein.

Eines sei vorab gesagt: Sich und seine Daten zu schützen ist nicht besonders schwer. Man benötigt dafür weder eine Ausbildung noch ein IT-Studium. Entscheidend ist der achtsame Umgang mit den eigenen Daten und vor allem das aufmerksame Lesen von Hinweisen und Nutzungsbedingungen – frei nach dem Motto: „Erst lesen, dann klicken!“

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

Im Folgenden werden grundsätzliche und relativ einfache Methoden beschrieben, mit denen man den Schutz seiner Daten bereits auf ein sehr hohes Niveau heben kann.

Hundertprozentigen Schutz gibt es nicht
Allerdings muss an dieser Stelle darauf hingewiesen werden, dass es einen hundertprozentigen Schutz nicht gibt. Wenn ein:e Hacker:in es auf Daten abgesehen hat, dann wird er oder sie auch an die Daten herankommen – entscheidend ist, welcher Aufwand dafür betrieben werden muss.

Auch im professionellen Bereich der IT-Sicherheit findet immer eine solche Abwägung zwischen Risiko und Aufwand statt. Im privaten Bereich ist das Ziel, mit bestimmten Verhaltensweisen ein hohes Maß an Sicherheit zu gewährleisten.

6.1 Grundsätzlich misstrauisch sein

Was im realen Leben gilt, sollte auch im Internet beachtet werden.

Sieht man im Geschäft einen unschlagbar günstigen Artikel, stellt man sich in der Regel die Frage nach dem Grund für den niedrigen Preis: zweite Wahl? Fehlerhaft? Fälschung? Genau diese Vorsicht sollte man auch im Internet walten lassen. Hinter vermeintlich günstigen Artikeln mit sagenhaften Rabatten stecken häufig sogenannte Fake Shops. Besonders verdächtig sind diese Shops dann, wenn der Artikel in anderen Shops bereits ausverkauft ist und hier dennoch mit unglaublichen Rabatten beworben wird. Hier hilft oft der Blick ins Impressum der Website – sofern es überhaupt vorhanden ist. Existiert ein solches nicht, kann man fast sicher sein, dass es sich um einen Fake Shop handelt.

Versprechen von „garantierten“ und „fantastischen“ Gewinnen bei diversen Onlinegewinnspielen sollte man getrost ignorieren. Auch im Internet ist nichts umsonst – man zahlt immer mindestens mit den persönlichen Daten, die zur Teilnahme hinterlegt werden müssen. Mehr dazu findet sich in Modul 2, Abschnitt 1.8, „Gewinnspiele, Tracking und Co.“.

Auch wenn ein Onlineshop per E-Mail über ein Sicherheitsproblem mit dem dortigen Nutzerkonto informiert und man in der Nachricht aufgefordert wird, auf einen bestimmten Button oder Link zu klicken, um das Problem zu lösen, sollten sofort alle Alarmglocken läuten (mehr dazu unter Abschnitt 4.1, „E-Mail-Pishing“).

Hausbanken verschicken in der Regel keine E-Mails. Eine Nachricht von einer Bank im E-Mail-Postfach ist daher höchstwahrscheinlich ebenfalls nicht echt. Mitgeschickte Links sollten auf keinen Fall angeklickt werden.

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

6.2 Sichere Passwörter

Ein schlecht gewähltes Passwort ist nach wie vor die am meisten genutzte Sicherheitslücke im Internet. Denn Hacker:innen können es mithilfe automatischer Programme, die Tausende Einträge aus Wörterbüchern in Verbindung mit Zahlenkombinationen in Sekundenschnelle testen, rasch herausfinden.

Forschende der Universität Potsdam haben mehr als 67 Millionen Zugangsdaten mit E-Mail-Adresse auf die Endung „.de“ untersucht[23], die aus Datenlecks im Jahr 2019 stammen und im Internet frei verfügbar sind. Das Ergebnis: In Deutschland ist derzeit das Passwort „123456“ am beliebtesten, gefolgt von „123456789“ und „12345678“. Unsicherer als mit solchen Passwörtern geht es kaum!

Für jeden Dienst sollte ein eigenes Passwort genutzt werden. Gibt es bei einem der Portale eine Sicherheitslücke, können sich Kriminelle wenigstens nicht in alle anderen Accounts einloggen.

Grundsätzlich gilt: Je länger das Passwort, desto sicherer.
Ein Passwort sollte mindestens acht Zeichen lang sein – dann aber auch komplex, das heißt aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (etwa §, $, %, &, !, ?) bestehen.

Ein langes Passwort, das 20 bis 25 Zeichen oder länger ist, kann hingegen weniger komplex sein und aus zwei Zeichenarten bestehen.

Fachartikel der VZ unter: https://www.verbraucherzentrale-rlp.de/wissen/digitale-welt/datenschutz/sichere-passwoerter-so-gehts-11672, Stand: 23.05.2023.

Ein Passwort sollte sicher sein und sich nicht leicht erraten lassen.
Es sollte ein K L U G E S Passwort sein.

- **Kryptisch:**
  Das Passwort sollte keinen erkennbaren Sinn ergeben und nicht in Wörterbüchern vorkommen. Auch gängige Buchstabenfolgen auf der Tastatur wie „asdfg“, „qwertz“ oder Zahlenfolgen wie „123456“ sind tabu. Es ist außerdem nicht empfehlenswert, einfache Ziffern am Ende des Passwortes anzuhängen oder eines der üblichen Sonderzeichen wie $, !, ? oder # am Anfang oder Ende eines ansonsten simplen Passwortes zu ergänzen.

[23] https://hpi.de/news/jahrgaenge/2019/die-beliebtesten-deutschen-passwoerter-2019.html , Stand: 06/2023.

- **Lang:**
  Ein Passwort sollte **mindestens acht bis zehn Zeichen** lang sein. Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) gilt grundsätzlich: je länger, desto besser. Bei Verschlüsselungsverfahren für WLAN, wie zum Beispiel WPA und WPA2, sollte das Passwort sogar mindestens 20 Zeichen lang sein.

- **Unpersönlich:**
  Es sollten keine Namen von Familienangehörigen, Haustieren oder Lieblingsstars verwendet werden.

- **Geheim:**
  Das Passwort sollte weder auf einem Zettel an den Computer geklebt noch im Browser gespeichert sein.

- **Einmalig:**
  Es sollte niemals dasselbe Passwort für mehrere Zugänge verwendet werden.

- **Super zu merken:**
  Damit der Überblick zumindest über die wichtigsten Passwörter nicht verloren geht, sollten diese gut zu merken sein. Dabei kommt das sogenannte Leetspeak in Betracht. Der grundsätzliche Gedanke des Leetspeak ist es, einzelne Buchstaben oder ganze Wörter durch Zahlen oder gar Sonderzeichen zu ersetzen. Zum Beispiel wird aus „Nacht“ „n8“, also „n“ und „acht“ zusammengesetzt. Oder es werden nur einzelne Buchstaben gegen andere Zeichen getauscht, die eine optische Ähnlichkeit mit dem Buchstaben aufweisen: Aus „Gamer“ wird so „G4m3r“. Aber auch Angreifer:innen kennen Leetspeak und binden dieses in die Wörterbuchattacken direkt mit ein.

Vorteilhaft sind sogenannte Passphrasen. Dafür überlegt man sich beispielsweise einen Satz, der einem immer wieder einfallen wird und von dem jeweils nur die ersten Buchstaben der einzelnen Wörter sowie die Satzzeichen genutzt werden.

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

Am besten ist, wenn man einen solchen Satz frei erfindet und nicht irgendwo gelesen hat.

Beispiel: *Am liebsten esse ich Pizza mit vier Zutaten und extra Käse!*

Auf der Webseite https://checkdeinpasswort.de/ kann man die Sicherheit verschiedener Passwörter einfach und unkompliziert testen. Auch wenn laut deren Angaben keinerlei Daten gespeichert werden, sollte man dort nicht unbedingt das eigene Passwort testen, sondern lieber ein ähnlich aufgebautes.

Weitere Infos des BSI finden sich unter:
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Umgang-mit-Passwoertern/umgang-mit-passwoertern_node.html, Stand: 06/2023.

Der Flyer „Sicheres Passwort“ der Verbraucherzentrale Rheinland-Pfalz ist erhältlich unter:
https://www.verbraucherzentrale-rlp.de/sites/default/files/2018-09/Marktcheck-Passworte-bei-Onlinediensten-vzrlp_0.pdf, Stand: 06/2023.

6.3 Zwei-Faktor-Authentifizierung (2FA)

Immer mehr Shops, Banken und andere Internetportale bieten die Zwei-Faktor-Authentifizierung an. Dabei handelt es sich um eine zusätzliche Sicherheitsmaßnahme, die dem Schutz von Accounts dient. Nach dem Log-in per Benutzername und Passwort muss eine zusätzliche Sicherheitskomponente – in der Regel ein Zahlencode – eingegeben werden. Dies ist dann der zweite Faktor.

Die Person, die sich einloggen möchte, erhält den Code dann – je nach Anbieter und Verfahren – entweder per SMS an die eigene Handynummer oder mittels eines Codegenerators (zum Beispiel einer bestimmten App).

Der große Vorteil der Zwei-Faktor-Authentifizierung ist die Tatsache, dass unbefugte Personen, die im Besitz von fremden Benutzernamen und Passwörtern sind, sich nicht in die entsprechenden Accounts einloggen können, ohne auch über das fremde Smartphone zu verfügen.

Darüber hinaus gibt es noch weitere Verfahren (zum Beispiel per Smartcard oder Token), diese spielen im privaten Umfeld aber nur eine untergeordnete Rolle.

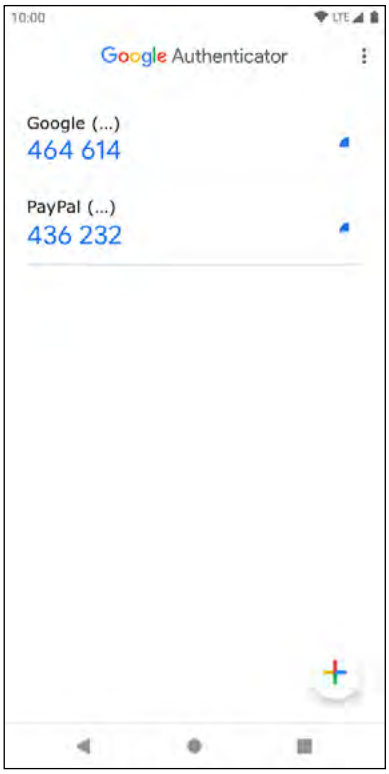
Folgende Darstellung zeigt den Ablauf des Anmeldeprozesses am Beispiel von Amazon:

Nachdem man sich mit seiner E-Mail-Adresse und seinem Passwort angemeldet hat, erhält man per SMS einen Code zugesendet, den man dann in das entsprechende Feld der Anmeldemaske einträgt.

Quelle: PC-Welt (Screenshot vom 27.08.2021)

Da SMS aber ein eher unsicheres Medium sind, empfiehlt sich die Nutzung einer separaten „Authenticator-App“. Die meisten Internetdienste bieten übrigens beide Möglichkeiten an.

Die folgende Abbildung zeigt die Codedarstellung am Beispiel der App Google Authenticator:



Quelle: Screenshot vom 27.08.2021

Nach dem Öffnen der App erscheinen die Konten, für die eine Zwei-Faktor-Authentifizierung eingerichtet wurde – in diesem Fall für Google und für PayPal. Die dort angezeigten Codes dienen als zweiter Faktor für das Einloggen bei dem entsprechenden Dienst. Hier ist grundsätzlich ein wenig Eile angesagt, denn die Codes werden alle 30 Sekunden neu generiert.

Neben dem Google Authenticator gibt es noch weitere Apps, die zur Zwei-Faktor-Authentifizierung genutzt werden können. Die gängigsten sind der Microsoft Authenticator und andOTP oder FreeOTP, die – wie auch der Google Authenticator – für iOS und Android zur Verfügung stehen.

Das Öffnen dieser Apps erfordert entweder die Eingabe eines Passwortes oder eines biometrischen Merkmals (Fingerabdruck oder Gesichtserkennung) und ist somit zusätzlich vor unbefugten Zugriffen geschützt.

Da die Einrichtung der Zwei-Faktor-Authentifizierung etwas mehr Aufwand erfordert, gibt es unter folgendem Link eine Schritt-für-Schritt-Anleitung:
https://www.heise.de/tipps-tricks/Google-Zwei-Faktor-Authentifizierung-aktivieren-4015730.html, Stand: 06/2023.

Grundsätzlich sollte man aber nur übergreifende Authenticator-Apps nutzen und um Apps, die ein Anbieter für seinen Log-in (und meist noch für die Nutzung seiner Dienste zeitgleich) anbietet, einen Bogen machen. Gerade im Bankingumfeld hat sich da ein bedenklicher Trend etabliert: Die Banking-App ist beim Onlinebanking für den zweiten Faktor nutzbar, bringt aber zusätzlich auch die restlichen Funktionen mit, sodass man auf den stationären PC verzichten kann. Dadurch hat man aber wieder nur einen Faktor, nämlich den Log-in auf dem Smartphone. Wenn man wirklich sichergehen möchte und es möglich ist, sollte man trotz Kosten Hardware-Authentifizierungssysteme als zweiten Faktor einsetzen, zum Beispiel ChipTAN, PhotoTAN, etc.

Fazit:
Die Zwei-Faktor-Authentifizierung bietet ein enormes Plus an Sicherheit und sollte daher für alle wichtigen Accounts wie Banken, Zahlungsdienstleister, Onlineshops, E-Mail-Dienste und so weiter eingerichtet werden. Bevorzugt sollte die Einrichtung mittels einer entsprechenden App erfolgen. Der Versand der Authentifizierungscodes per SMS ist aus Sicherheitsgründen nur dann zu empfehlen, wenn ein Dienst den Code per App nicht anbieten kann.

Weitere Informationen zur Zwei-Faktor-Authentifizierung sind hier zu finden:
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html, Stand: 06/2023.

6.4 Passwortmanager-Apps

Laut der Initiative „Deutschland sicher im Netz“[24] verfügt heute jeder Mensch in Deutschland durchschnittlich über 78 Onlinekonten, die meist mittels Benutzername und Passwort geschützt sind beziehungsweise geschützt sein sollten. Wenn man, wie im Abschnitt 6.2, „Sichere Passwörter“, beschrieben, für jeden Account ein einzigartiges und sicheres Passwort wählt, wird man kaum in der Lage sein, sich all diese Passwörter zu merken. Hier kann ein Passwortmanager sehr hilfreich sein.

Passwortmanager lassen sich am besten mit einem Tresor vergleichen. Zu jedem Account können im Passwortmanager Zugangsdaten wie Benutzername und Passwort gespeichert werden. Das gilt ebenso für Bankzugänge, PINs und andere Zugänge. Bei manchen Apps bekommt man auf Wunsch auch Passwörter vorgeschlagen. Diese Daten werden im Passwortmanager selbst verschlüsselt. Der Passwortmanager wiederum wird mit einem Passwort, dem sogenannten Masterpasswort, geschützt. Hier muss natürlich ein entsprechend starkes und sicheres Passwort

[24] https://www.sicher-im-netz.de/sicherer-login-online-konten-schützen, Stand: 06/2023.

verwendet werden, im Idealfall in Verbindung mit einer Zwei-Faktor-Authentifizierung. Denn wenn dieses Masterpasswort geknackt wird, sind alle dort gespeicherten Passwörter einsehbar.

Wenn alle Daten richtig eingetragen wurden, erkennt ein guter Passwortmanager, in welchen Account man sich gerade einloggen möchte, und schlägt das automatische Ausfüllen der Zugangsdaten vor. In dem Fall legitimiert man sich nur noch mit dem Masterpasswort, der Rest wird vom Passwortmanager übernommen. Bei einigen Anbietern kann der gewünschte Account auch direkt aus dem Programm heraus aufgerufen werden.

Passwortmanager gibt es in vielen Varianten: kostenlos als Freeware, kostenpflichtig, als Computerprogramm, als App für Smartphone und Tablet, integriert in diversen Antivirenprogrammen oder als Plug-in für verschiedene Internetbrowser.

Je nach Anbieter werden die Daten lokal auf dem Gerät, online in einer gesicherten Cloud oder sogar auf dem eigenen Server gespeichert. Das lokale Speichern auf dem Gerät ist zwar die sicherste Variante, hat aber den entscheidenden Nachteil, dass eine Nutzung des Passwortmanagers auf weiteren Geräten auch doppelte Datenpflege verursacht und neben einem Server auch ein gewisses Maß an IT-Kenntnissen erfordert. Das Speichern in der Cloud ist insoweit praktisch, als der Passwortmanager geräteübergreifend synchronisiert werden kann und die Zugänge somit überall und quasi jederzeit zur Verfügung stehen. Clouds sind jedoch immer mit einem gewissen Risiko behaftet, daher sollte man auf einen Anbieter setzen, der die Daten gemäß der europäischen Datenschutz-Grundverordnung speichert.

Ein Passwortmanager gehört zum Pflichtprogramm sicherheitsbewusster Nutzer:innen!

Die Anzahl der Passwortmanager am Markt ist riesig, die Entscheidung für einen bestimmten Anbieter hängt dabei stark von den persönlichen Präferenzen ab.

2025 hat das Bundesamt für Sicherheit in der Informationstechnik gemeinsam mit der Verbraucherzentrale Nordrhein-Westfalen zehn Passwort-Manager untersucht und auf ihre Sicherheit hin getestet. Das Ergebnis war ernüchternd: Nur drei Anwendungen haben den Test bestanden. Keinerlei Bedenken hatten die Tester lediglich bei drei Anwendungen KeepassXC, KeePass2Android und Mozilla Firefox. Gegen den Einsatz von 1Password hatten sie zwar keine grundsätzlichen Bedenken, merken aber an, dass der kanadische Anbieter sich die Auswertung von Nutzerdaten zu Marketingzwecken vorbehält.[25]

Im Internet finden sich darüber hinaus zahlreiche Tests, die bei der Entscheidung für einen geeigneten Anbieter weiterhelfen können. Da die einzelnen Tests aber häufig unterschiedliche Schwerpunkte setzen, gilt es auch hier zu vergleichen und den zu den eigenen Präferenzen passenden Anbieter auszuwählen. Empfehlenswert ist es aber, der Sicherheit dabei einen großen Stellenwert einzuräumen. Empfehlenswert ist es aber, der Sicherheit dabei einen großen Stellenwert einzuräumen.

[25] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/passwortmanager_sicherheit_datenschutz.html

Datensicherung – kein Back-up, kein Mitleid!

Als Back-up[26] wird eine Sicherungskopie von Datenträgern, Dateisystemen oder Dateien bezeichnet. Im Falle eines Systemausfalls, eines Geräte- oder Datenverlustes können die eigenen Daten zurückkopiert und/oder wiederhergestellt werden.

- Viele Computer, Smartphones und Tablets legen solche Sicherungskopien automatisch an. Die Daten und Einstellungen werden dabei häufig in einem Onlinespeicher synchronisiert. Vorsicht ist geboten bei Back-up-Lösungen von Dienstleistungsanbietern. WhatsApp zum Beispiel verschlüsselt zwar die Nachrichten, legt Back-ups aber unverschlüsselt an. Hierdurch wird die Ende-zu-Ende-Verschlüsselung der Chats umgangen, da nach dem Back-up die Chats unverschlüsselt gespeichert sind.

- Back-ups können auch manuell erstellt werden. Dafür gibt es spezielle Programme, die Speicher oder Festplatte des Gerätes auslesen und alle Daten sichern.

- Als Medium für ein Back-up eignet sich zum Beispiel eine externe Festplatte. Die interne Festplatte sollte nur im Notfall für Back-ups genutzt werden, denn wenn die Festplatte defekt ist, nützt auch das Back-up nichts mehr.

- Aber auch Clouddienste eignen sich für Back-ups. Sie bieten den Vorteil, dass die Daten vor Zerstörung durch Überschwemmung, Brand oder Einbruch in der Wohnung – anders als bei einer externen Festplatte – weiterhin geschützt sind. Allerdings ist gerade bei Anbietern von Clouddiensten der Datenschutz nicht zu vernachlässigen. Aus diesem Grund empfiehlt es sich, einen Cloudanbieter auszuwählen, der die Daten vor dem Upload verschlüsselt, sodass dieser selbst gar keinen Zugriff auf die Daten erhält. Zusätzlich können Daten vor dem Upload auch manuell verschlüsselt werden, etwa mit kostenlosen Programmen wie VeraCrypt. Ein weiterer Schwachpunkt der Clouddienste ist häufig die mangelnde Sicherheitsgarantie im Fall von Schäden an den Festplatten des Anbieters. Geht zufälligerweise ausgerechnet die kaputt, auf der die eigenen Daten gespeichert sind, kann die Back-up-Datei weg sein.

- Falls das Smartphone mal kaputt oder verloren geht, sind mit einem Back-up die Systemdaten sowie Kontakte, Bilder und Videos noch verfügbar. Das Gleiche gilt für PC oder Laptop, wenn Back-ups im Onlinespeicher angelegt wurden.

- Alle Daten wie Kontakte, Bilder und Videos können aus einem Back-up wiederhergestellt werden. Wenn beispielsweise das Smartphone kaputt ist und es repariert werden muss, wird es in der Regel komplett zurückgesetzt und alle Daten gelöscht. Spielt man dann das Back-up ein, sind die Dateien wieder vorhanden.

[26] https://praxistipps.chip.de/was-ist-ein-backup-einfach-erklaert_41415, Stand: 06/2023.

Ein Beispiel:
Viele stecken ihr Smartphone in die Hosentasche. Beim Gang auf die Toilette vergisst man das Handy und – schwupps – liegt es in der Kloschüssel. Das Gerät ist nass, geht aufgrund des Kurzschlusses sofort aus und lässt sich auch nicht mehr einschalten. Ohne ein Back-up sind sämtliche Kontaktdaten, Bilder, Videos und Chats verloren.

Wie wichtig eine Datensicherung ist, wird einem häufig erst dann bewusst, wenn man einmal Daten verloren hat. Der Verlust von WhatsApp-Chatverläufen, Browserhistorie, individuellen App-Einstellungen stellt für viele Nutzer:innen sicherlich noch kein allzu großes Drama dar, doch was ist mit dem Adressbuch, wichtigen Dokumenten und Daten oder – im Worst Case – der Verlust aller persönlichen Fotos, an denen häufig wichtige Erinnerungen hängen?

Die 3-2-1-Back-up-Regel

Man sollte mindestens drei Kopien haben, davon zwei auf unterschiedlichen Datenträgern und mindestens eine außer Haus.

Eine der Kopien kann das Original auf dem Rechner sein, eine zweite befindet sich auf einer externen Festplatte zu Hause und eine dritte auf einer, die im Büro oder bei einer Vertrauensperson gelagert ist.

Android-Smartphone und -Tablet

Auf Android-Endgeräten können gespeicherte Inhalte, Daten und Einstellungen direkt im Google-Konto gespeichert werden. Fotos und Videos sichert man schnell und unkompliziert in Google Fotos, Dateien und Ordner in Google Drive. Mithilfe der Google One App lassen sich automatische Back-ups einrichten, die alle wichtigen Daten in regelmäßigen Abständen sichern.[27] Wer seine Fotos und Dokumente nicht dem US-amerikanischen Konzern anvertrauen will, kann auch eine automatische Sicherung auf dem eigenen NAS-Laufwerk[28] einrichten. Die meisten NAS-Hersteller wie Qnap, Synology oder Western Digital bieten dazu passende Smartphone-Apps an, die die Sicherung übernehmen.

iPhone und iPad

Auch bei Apple-Geräten lassen sich Inhalte, Daten und Einstellungen direkt in der iCloud[29] sichern, das gilt auch für Fotos und Videos. Auch Apple-Nutzer:innen bieten die meisten NAS-Hersteller wie Qnap, Synology oder Western Digital dazu passende Apps an, die die Sicherung auf ihrem lokalen NAS übernehmen können, wenn sie private Daten nicht in der Cloud sichern wollen.

[27] https://support.google.com/android/answer/2819582?hl=de, Stand: 06/2023.

[28] https://www.heise.de/tipps-tricks/Ein-NAS-einrichten-so-geht-s-4180876.html, Stand: 06/2023.

[29] https://support.apple.com/de-de/HT211228, Stand: 06/2023.

Windows-PC oder -Laptop

Das Erstellen von Back-ups gehört nicht unbedingt zu den Stärken von Windows. Windows selbst bietet zwei Möglichkeiten der Sicherung[30] an. Bei der Erstellung eines Systemabbilds wird die gesamte Festplatte 1:1 mit Betriebssystem und allen dazugehörigen Einstellungen beispielsweise auf eine externe Festplatte kopiert. Leider ist es im Falle eines Crashs nicht immer möglich, die Daten des Systemabbilds wieder auf den PC/Laptop zu spielen.

Mithilfe der Windows-7-Sicherung, die ebenfalls Bestandteil von Windows 11 ist, lassen sich zum Beispiel die „Eigenen Dateien" sichern. Leider ist auch diese Methode nicht immer zuverlässig.

Wer seine Daten auf dem Windows-Rechner sicher und zuverlässig schützen möchte, muss sich zwangsläufig ein externes Back-up-Programm zulegen. Wie bei den in Abschnitt 6.4 erwähnten Passwortmanagern ist auch hier der Markt riesig, aber nahezu alle kostenpflichtigen Back-up-Programme tun das, was sie sollen: Daten sichern[31].

Apple Mac oder MacBook

Macs und MacBooks verfügen von Haus aus über die Back-up-Software Time Machine[32]. Man benötigt lediglich eine externe Festplatte, ein angeschlossenes NAS oder Apples Time Capsule, und mit wenigen Klicks ist eine automatische Datensicherung eingerichtet, die mehrfach täglich unbemerkt im Hintergrund alle gewünschten Daten sichert.

Fazit:
Ein Back-up ist notwendig und sinnvoll und sollte deshalb regelmäßig durchgeführt werden.

Weitere Infos unter folgendem Link:
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Datensicherung-und-Datenverlust/Datensicherung-wie-geht-das/datensicherung-wie-geht-das, Stand: 06/2023.

[30] https://www.heise.de/tipps-tricks/Backup-erstellen-mit-Windows-10-3858841.html, Stand: 06/2023.

[31] https://www.heise.de/download/specials/Die-beste-Backup-Software-Tools-fuer-Einsteiger-und-Profis-5052323, Stand: 06/2023.

[32] https://support.apple.com/de-de/HT201250, Stand: 06/2023.

6.5 Datensparsamkeit

Wenn wir uns im Netz bewegen, geben wir im Laufe der Zeit viele Daten von uns preis. Ob bei der Anmeldung zu Onlinediensten, beim Onlineshopping oder auch bei der Teilnahme an Gewinnspielen werden wir nach persönlichen Informationen gefragt. Auch Kundenkarten sammeln viele Informationen über unser Kaufverhalten.

Datensparsamkeit bedeutet in erster Linie: nur notwendige Daten angeben!

Bei Käufen in Onlineshops sollte man nur die Daten angeben, die für die jeweilige Bestellung wirklich nötig sind. Dazu gehören zwangsläufig der Name und die Anschrift. Bereits die Angabe des Geburtsdatums ist in den meisten Fällen jedoch unerheblich.

Ebenfalls Bestandteil der Datensparsamkeit ist das Widersprechen der weiteren Nutzung der eigenen Daten. Man sollte die eigenen Eingaben daher sorgfältig prüfen und auf die Zustimmung der Nutzung dieser Daten zu Werbezwecken verzichten. Ist eine solche Zustimmung zwingend erforderlich, beispielsweise um den Kauf abzuschließen, ist dies bereits ein Hinweis auf eine fragwürdige Seriosität des jeweiligen Dienstes. Möchte man diesen dennoch nutzen, sollte man im Anschluss von der Möglichkeit Gebrauch machen, der Verarbeitung und Weitergabe persönlicher Daten zu widersprechen. Das geht in der Regel in den Account-Einstellungen, ansonsten sollte man sich per E-Mail an den Anbieter wenden.

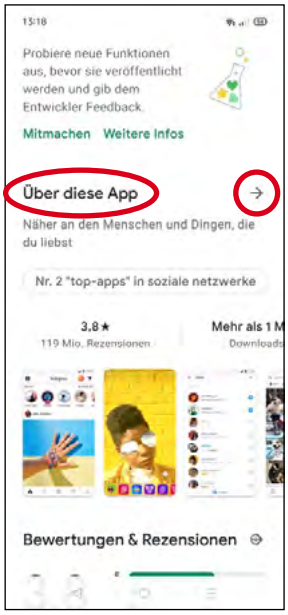
6.6 App-Berechtigungen und -Einstellungen prüfen und anpassen

Beim Herunterladen von Apps muss man zu deren Nutzung in der Regel einer Reihe von Berechtigungen zustimmen, zum Beispiel, ob die App auf das Mikrofon, die Kamera oder den Speicher des Smartphones zugreifen darf. In den meisten Fällen ist die uneingeschränkte Nutzung der App an die Zustimmung der nutzenden Person gebunden.

In den jeweiligen App-Stores kann man sich die Berechtigungen der einzelnen Apps anzeigen lassen. Die folgenden Abbildungen zeigen am Beispiel von Instagram in Google Play den Weg dorthin und welche Berechtigungen Instagram auf dem Smartphone hat.

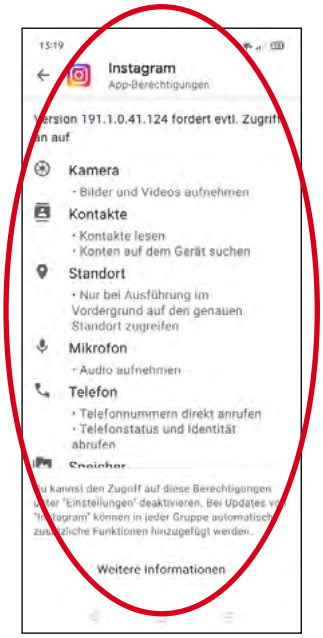
Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

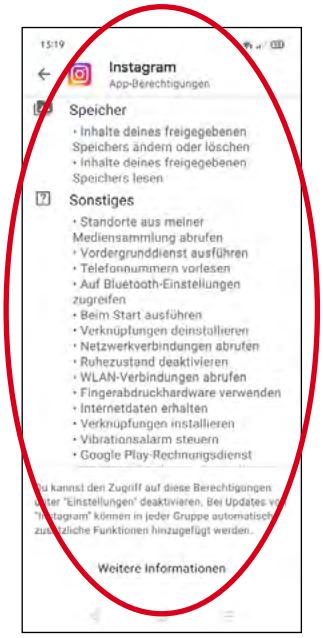
Beim Aufrufen der App in Google Play scrollt man bis ans Ende der Beschreibung und tippt auf den Pfeil neben „Über diese App“.



In der nächsten Ansicht scrollt man erneut nach unten und tippt auf „Weitere Informationen“, rechts neben dem Hinweis „App-Berechtigungen“.

Nun werden detailliert alle Funktionen des Mobilgerätes aufgelistet, auf welche die App zugreifen kann.



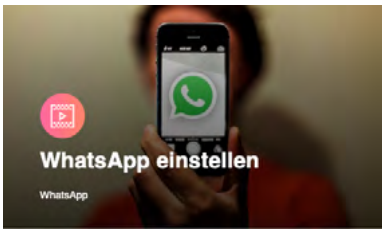


Quelle: Smartphone-Screenshots vom 05.08.2021

In den Einstellungen der jeweiligen App und/oder des Mobilgerätes sollte man nun die Berechtigungen deaktivieren, die für den Betrieb der App nicht erforderlich sind. So sollte die Koch-App beispielsweise nicht ohne gute Begründung Zugriff auf die Standortdaten mittels GPS erhalten und auch Spiele-Apps sollte kein Zugriff auf das eigene Notizbuch und die E-Mail-Adressen der Kontakte gewährt werden – mal abgesehen davon, dass Letzteres ohne deren vorherige Zustimmung schlicht illegal ist und zu Schadensersatzforderungen führen kann.

Ein weiterer wichtiger Punkt sind die Datenschutz- beziehungsweise Privatsphäre-Einstellungen in häufig genutzten Apps, insbesondere aus den Bereichen Social Media und Messenger. Meistens sind die Privatsphäre-Einstellungen auf „öffentlich“ voreingestellt. Dies ist gerade im privaten Bereich nicht sinnvoll, weshalb man die Privatsphäre- und Datenschutzeinstellungen in jeder App prüfen und anpassen sollte. Die Änderungen nimmt man häufig in den Einstellungen direkt in der App vor.

Auf der Website https://handysektor.de finden sich zu allen gängigen Apps Videoanleitungen, die kurz und prägnant erklären, welche Einstellungen in welchen Apps sinnvoll sind.



Quelle: https://handysektor.de (Screenshots vom 05.08.2021)

6.7 Apps zur Elternaufsicht installieren

Um Kinder grundsätzlich vor unangemessenen Inhalten, ungeeigneten und unsicheren Apps sowie In-App-Käufen zu schützen, kommt die Nutzung gängiger Jugendschutz-Apps, wie beispielsweise Googles „Family Link“ oder Apples „Bildschirmzeit“, infrage. Diese Apps lassen sich so konfigurieren, dass die Kinder und Jugendlichen bestimmte Apps nur mit expliziter Zustimmung der Eltern herunterladen und installieren können. Auch In-App-Käufe können mit den Schutz-Apps verhindert oder begrenzt werden. Zusätzlich lassen sich Uhrzeiten für die Nutzung von Smartphone und Co. festlegen und/oder bestimmte Tageslimits einrichten.

Eltern sollten bei aller berechtigter Sorge jedoch auch das Recht ihrer Kinder auf Privatsphäre im Auge behalten. Was über Einstellungen für Sicherheit und Schutz hinausgeht, stellt häufig einen übertriebenen Eingriff in die Privatsphäre von Kindern dar. Überwachung auf Schritt und Tritt oder das Mitlesen von Nachrichten sind in aller Regel unangemessen. Mit zunehmendem Alter und steigender Medienkompetenz von Jugendlichen empfiehlt es sich daher, Regeln für den Medienkonsum gemeinschaftlich auszuhandeln, gegebenenfalls mit professioneller Unterstützung. Dies stärkt aufseiten der Jugendlichen auch die Akzeptanz für die aufgestellten Regeln. Wer hingegen

einseitig versucht, durch Softwarebeschränkungen Verbote durchzusetzen, wird womöglich nur allzu schnell merken, dass über kurz oder lang jede Begrenzung durch einen Hack überwunden werden kann und die How-to-Anleitung auf YouTube dem eigenen Nachwuchs weit früher bekannt wurde als den Eltern.

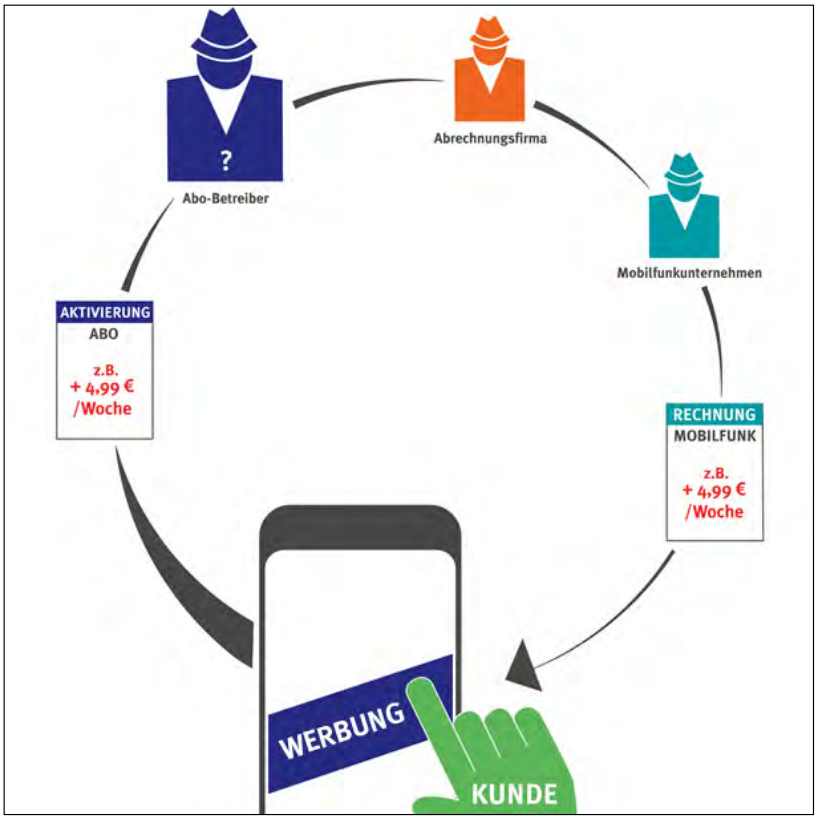
Anleitung zur Einrichtung von Family Link (Google) unter:
https://families.google.com/intl/de/familylink/, Stand: 06/2023.

Anleitung zur Einrichtung von Bildschirmzeit (Apple) unter:
https://support.apple.com/de-de/guide/ipad/ipadb15cb886/ipados, Stand: 06/2023.

Außerdem sollte man auf Apps des Betriebssystemherstellers (Google, Apple oder Microsoft) zurückgreifen und nicht auf (dubiose) Drittanbieter-Apps. Diese können technisch bedingt nicht den gleichen Funktionsumfang wie die Apps der Betriebssystemhersteller abbilden. Hier wird auch gerne mal vorsichtigen Eltern eine (Abo-) Falle gestellt beziehungsweise das Geld aus der Tasche gezogen.

6.8 Drittanbietersperre einrichten

Vor Abofallen, die per Telefonrechnung bezahlt werden, wie zum Beispiel Abos für Games (hier genügt häufig nur ein Kick auf eine Werbeanzeige), schützt eine sogenannte Drittanbietersperre.



Quelle: www.verbraucherzentrale.de, Stand 06/2023

Alle deutschen Mobilfunkanbieter sind gesetzlich dazu verpflichtet, eine Drittanbietersperre auf Wunsch kostenfrei einzurichten. Je nach Provider kann diese im Kundenmenü aktiviert oder über eine Kundenhotline beauftragt werden.

Weitere Infos dazu bei der Verbraucherzentrale unter:
https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/drittanbieter-sperre-schutz-vor-ungewollten-abos-12613, Stand: 06/2023.

6.9 E-Mail- oder Nachrichten-Phishing erkennen

Fremde können einem selbst, aber auch anderen Personen im eigenen Namen Phishing-E-Mails oder -SMS schicken oder anrufen. Diese Kontaktversuche können aufgrund der persönlichen Daten, die die Täter:innen unter Umständen nutzen, sehr überzeugend wirken. Deshalb sollte man besonders vorsichtig sein, wenn man Nachrichten erhält oder angerufen wird und darum gebeten wird, verdächtige Links anzuklicken, sensible Daten wie Passwörter herauszugeben oder Accountdaten zu ändern.

So manch betrügerische E-Mail sieht täuschend echt aus. Jedoch gibt es einige Hinweise, die erkennen lassen, dass Übeltäter:innen ihre Angel ausgeworfen haben, beispielsweise um an Bankdaten heranzukommen:[33]

- **Grammatik- und Rechtschreibfehler**
  Am einfachsten zu durchschauen sind E-Mails, die in fehlerhaftem Deutsch geschrieben sind. Meistens wurden sie nicht auf Deutsch verfasst, sondern sind mit einem Übersetzungsdienst aus einer anderen Sprache übersetzt worden. Ein weiterer Hinweis auf solche E-Mails sind etwa kyrillische Buchstaben im Text oder auch fehlende Umlaute.

- **Mails in fremder Sprache**
  Ebenfalls schnell als Phishing zu erkennen sind E-Mails, die auf Englisch oder Französisch verfasst sind. Sollte man selbst nicht gerade Kundin oder Kunde einer Bank mit Sitz im Ausland sein, kann man sicher sein, dass (wenn überhaupt) E-Mails von der eigenen Bank nur auf Deutsch verschickt werden.

- **Fehlender Name**
  Die eigene Bank und andere Vertragspartner wie zum Beispiel Onlinezahlungsdienste sprechen ihre Kund:innen in E-Mails grundsätzlich mit ihrem Namen an und niemals mit „Sehr geehrte Kundin“ oder „Sehr geehrter Nutzer“. Sehr raffinierte Phishing-Täter:innen haben aber oftmals auch schon den Namen herausgefunden und schicken deshalb E-Mails mit persönlicher Ansprache, zum Beispiel „Sehr geehrte Frau Meier“ oder „Sehr geehrter Herr Müller“.

[33] https://www.verbraucherzentrale-rlp.de/wissen/digitale-welt/phishingradar/merkmale-einer-phishingmail-6073, Stand: 06/2023.

Damit versuchen Kriminelle, der E-Mail eine höhere Glaubwürdigkeit zu verleihen. Sollte man sich nicht sicher sein, ob die E-Mail und die darin enthaltene Aufforderung tatsächlich echt sind, lohnt sich eine Nachfrage bei der Bank oder dem entsprechenden Anbieter.

- **Dringender Handlungsbedarf**
  Wenn in einer E-Mail die Aufforderung steckt, ganz dringend und innerhalb einer bestimmten (kurzen) Frist zu handeln, sollte man ebenfalls stutzig werden. Insbesondere, wenn die Aufforderung mit einer Drohung verbunden ist – beispielsweise, dass sonst die Kreditkarte oder der Onlinezugang gesperrt werden.

- **Eingabe von Daten**
  Die Aufforderung, persönliche Daten sowie möglicherweise PIN oder TAN einzugeben, ist ein weiterer Hinweis auf betrügerische Absichten. Banken und Onlinezahlungsdienste würden niemals um die Eingabe solcher Daten per E-Mail bitten. PIN und TAN werden von Geldinstituten niemals telefonisch oder per E-Mail abgefragt – dies zählt zu den wesentlichen Sicherheitsregeln.

- **Links oder eingefügte Formulare**
  Banken versenden in der Regel keine E-Mails, sondern Briefe. Falls doch E-Mails von der Bank eingehen, so werden diese keine Dateianhänge (wie Formulare, über die eine Eingabe gemacht werden muss) enthalten. Banken und andere Dienstleister versenden nur in Ausnahmefällen E-Mails mit Links, auf die der Empfänger oder die Empfängerin klicken soll. Dann geht es beispielsweise um neue AGB, niemals aber um das Einloggen ins Kundenkonto. Besser ist ohnehin immer, die Internetseite selbst aufzurufen, indem man diese in das Adressfeld des Browsers eintippt. Besonders gefährlich sind Links, deren Adresse besonders lang und kryptisch ist. Darin ist zum Teil – extrem raffiniert – die Adresse des betrügerischen Servers versteckt. Selbst fortgeschrittene Nutzer:innen können das leicht übersehen, zumal die angesurfte falsche Internetadresse den echten Seiten der Bank zum Verwechseln ähnlich sieht.

- **Mail-Header**
  Manche Phishing-Mails sind sehr gut gemacht. Die Absender-E-Mail-Adresse scheint vertrauenswürdig, der Link im Text auch, das Deutsch ist flüssig? Trotzdem muss diese E-Mail nicht echt sein. Auch Absenderangaben von E-Mails lassen sich fälschen. Wenn man – um letzte Zweifel auszuräumen – die E-Mail prüfen will, muss man sich den sogenannten Mail-Header[34] anschauen. Dort steht die IP-Adresse des Absenders oder der Absenderin. Nur diese ist fälschungssicher und gibt Aufschluss über die Person, die die Mail verschickt hat. Allerdings ist das eher ein Tipp für erfahrene Nutzer:innen, denn die Analyse der Header-Daten ist nicht so einfach.

Zusammengefasst sollte man sich auf jeden Fall merken, dass kein Kreditkarteninstitut, keine Bank und auch kein seriöser Anbieter per E-Mail dazu auffordern würde, vertrauliche Daten preiszugeben.

[34] https://www.verbraucherzentrale-rlp.de/wissen/digitale-welt/phishingradar/so-lesen-sie-den-mailheader-6077, Stand: 06/2023.

6.10 Mehrere E-Mail-Adressen verwenden

Wer hat die folgende Situation nicht schon mindestens einmal erlebt?

Man registriert sich mit seiner E-Mail-Adresse bei einem Shop oder anderen Portal, setzt das Häkchen zum Erhalten von Newslettern explizit nicht und erhält dennoch einen Newsletter nach dem anderen. Anschließend nutzt man den Link im Newsletter, um sich nun endgültig abzumelden. Trotzdem erhält man nicht nur diesen einen Newsletter weiterhin, auch E-Mails von anderen Anbietern landen mit zunehmender Häufigkeit im eigenen Postfach.

Das ist leider nichts Ungewöhnliches, sondern gängige Praxis, da ein Großteil der Anbieter recht sorglos mit den Daten der Kundschaft umgeht und diese auch gerne mal gegen Geld weiterveräußert. Besonders ärgerlich ist das, wenn die einzige E-Mail-Adresse, die man hat, so täglich mit immer mehr Spam zugemüllt wird.

Grundsätzlich vermeiden lässt sich das nicht, mit folgenden Verhaltensweisen kann man die Spam-Flut aber zumindest eindämmen:

1. **Freemail-Adresse für das „öffentliche“ Internet**
   Die Adresse, die man primär für Shops, Portale und andere Anmeldungen im Internet nutzt, erstellt man einfach bei einem sogenannten Freemail-Anbieter, zum Beispiel Gmail (Google), Web.de oder GMX.de.

2. **Eine weitere Adresse für die private und sensible Kommunikation**
   Eine solche Adressen ist bei seriösen Anbietern wie posteo.de, mailbox.org oder tutanota.com erhältlich. Der monatliche Preis für eine solche E-Mail-Adresse liegt bei etwa einem Euro, bietet dafür im Vergleich zu den meisten Freemail-Anbietern aber einige Zusatzdienste, etwa Verschlüsselung, werbefreies Postfach, Zwei-Faktor-Authentifizierung und Ähnliches. Diese Adresse sollte man ausschließlich für die private Kommunikation und beispielsweise den Kontakt zu Behörden und öffentlichen Stellen nutzen.

6.11 Antivirenprogramme: ja oder nein? – Jein

Windows 11 hat mit dem Microsoft Defender Antivirus bereits eine sehr gute Antivirensoftware integriert. Trotz des vermeintlich schlechten Rufs erreicht der Microsoft Defender bei unabhängigen Tests stets die Höchstpunktzahl und liegt gleichauf mit den kommerziellen Anbietern von Antivirensoftware. Wichtig ist, dass das automatische Einspielen von Updates bei Windows aktiviert ist, da der Microsoft Defender mindestens einmal täglich die Virendefinitionen aktualisiert.

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

Die Nutzung einer zusätzlichen Antivirensoftware unter Windows ist also nicht grundsätzlich notwendig. Kommerzielle Antivirenprogramme bieten jedoch häufig einige Zusatzfunktionen, wie zum Beispiel Anti-Banner, kostenlose VPN, sicheren Zahlungsverkehr, Webcam-Schutz und einige mehr. Wer eine gewisse Extrasicherheit sucht, kann beispielsweise auf der Webseite av-test.org alle zwei Monate die aktuellen Ergebnisse der kommerziellen Anbieter vergleichen. Außerdem gibt es regelmäßig Tests der Stiftung Warentest, die in der Vollversion allerdings kostenpflichtig sind.[35]

Apple-Nutzer:innen benötigen in der Regel keinen zusätzlichen Virenschutz. Von Haus aus verfügen Apple-Produkte über eine integrierte Antivirussoftware nach Branchenstandard, um Schadsoftware zu blocken und zu entfernen.

Generell sind Antivirenprogramme – egal auf welchem System – nur als Ergänzung zu folgenden Verhaltensweisen zu verstehen:

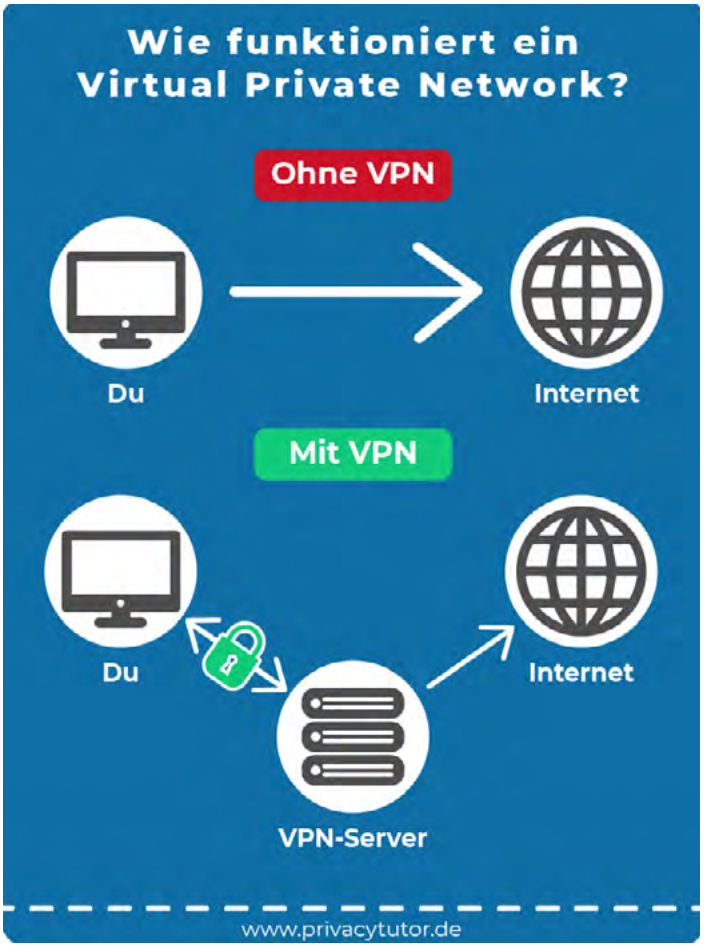
1. **Keine Apps und Programme aus unbekannten Quellen installieren.**
2. **Das Betriebssystem und alle Programme sollten immer auf dem aktuellen Stand sein.**
3. **Sichere Passwörter verwenden.**
4. **Regelmäßige Back-ups erstellen.**
5. **Wachsam sein und den gesunden Menschenverstand nutzen.**

[35] https://www.test.de/Antivirenprogramme-im-Test-4993310-5850702/, Stand: 06/2023.

6.12 VPN = Virtual Private Network

Vollständige Anonymität im Internet ist quasi unmöglich. Dennoch ist das Verbergen der eigenen IP-Adresse ein wichtiger Schritt in diese Richtung. Dazu kann man den kostenlosen TOR-Browser nutzen, doch dieser ist recht langsam. Um sich anonym und dazu noch schnell im Internet zu bewegen, benötigt man daher einen sogenannten **VPN-Dienst**.

Wie funktioniert ein VPN?



Ohne VPN verbindet man sich per WLAN oder per Mobilfunknetz direkt mit dem Internetprovider. Die IP-Adresse ist dabei eindeutig, und alle Daten werden unverschlüsselt übertragen, es sei denn, der Anbieter nutzt seinerseits ein verschlüsseltes Webprotokoll.

Mit VPN nutzt man zwar die gleiche Leitung wie ohne VPN, allerdings läuft der gesamte Datenverkehr zunächst über die Server des VPN-Anbieters und ist zusätzlich auch noch verschlüsselt. Somit wird umgangssprachlich ein abhörsicherer und anonymer Tunnel durch das Internet gegraben, der keine Rückschlüsse auf die eigene IP-Adresse zulässt.

Quelle: https://privacytutor.de (Screenshot vom 25.08.2021)

Ein umfangreicher Leitfaden über VPN und dessen Einsatzmöglichkeiten finden sich unter folgendem Link: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Router-WLAN-VPN/Virtual-Private-Networks-VPN/virtual-private-networks-vpn_node.html, Stand: 06/2023.

Benutzt man einen VPN-Zugang, wird man allerdings für den VPN-Anbieter völlig transparent. Er kann jegliche Verbindung ins Internet, die über das VPN aufgebaut wird, sehen. Man muss also seinem Anbieter dahingehend vertrauen, dass er selbst nicht zur Datenkrake wird.

6.13 Sinnvolle Browser, Suchmaschinen und Add-ons

Eine wichtige Rolle beim sicheren Surfen im Internet spielt auch die Wahl des Browsers.

Marktanteile der führenden Browser (Desktop und Notebook ohne Smartphones und Tablets) weltweit:

1. Chrome: 51,4 Prozent
2. Firefox: 16,9 Prozent
3. Edge: 15,2 Prozent
4. Safari: 7,6 Prozent

Quelle: Statista (Stand: 01/2026)[36]

Google Chrome ist unbestritten der schnellste und benutzerfreundlichste Browser. Lange Zeit galt Google Chrome aber auch als die Datenkrake schlechthin. Aufgrund des schlechten Rufs hat Google viel in die Sicherheit seines Browsers investiert und diese massiv erhöht. Mittlerweile lässt sich die Sicherheit auch durch zusätzliche Add-ons (Hilfsprogramme, mit denen eine Anwendung erweitert wird) verbessern und individualisieren.

Apples Safari bietet grundsätzlich ein recht hohes Schutzniveau und beruht auf eigenen Entwicklungen von Apple. Da der Quellcode aber nicht öffentlich zugänglich ist, ist eine Prüfung der Sicherheit durch unabhängige Expert:innen nicht möglich.

Microsoft Edge als Nachfolger des Internet Explorer ist wie Safari nicht Open Source und somit für externe Expert:innen nicht zugänglich. Ein großer Nachteil ist, wie selten Edge seine Sicherheitseinstellungen aktualisiert (alle zwei bis vier Wochen), wohingegen die Aktualisierungsintervalle bei Chrome und Firefox nur wenige Tage betragen.

Mozilla Firefox gilt als der Privatsphäre-Browser schlechthin. Mit einer riesigen Anzahl verfügbarer Add-ons lässt sich die Sicherheit individuell anpassen und mitunter massiv ausbauen.

[36] https://de.statista.com/statistik/daten/studie/828151/umfrage/meistgenutzte-browserfamilien-im-internet-in-deutschland / Stand 2026

Folgende Add-ons sind sinnvoll, um die Sicherheit zu optimieren:

- **NoScript:** verhindert die Ausführung von Schadsoftware, die automatisch beim Öffnen des Browsers startet, ohne dass man dies bestätigen muss
- **uBlock Origin:** blockiert automatisch Werbung und Tracker (Anwendungen, die Nutzer:innen verfolgen und aufzeichnen, was diese im Netz tun)
- **Nervenschoner:** unterdrückt nervige Cookie-Banner[37]

Anleitungen zur Installation von Add-ons für Google Chrome und Firefox finden sich unter folgenden Links:
https://support.google.com/chrome_webstore/answer/2664769?hl=de, Stand: 06/2023.
https://support.mozilla.org/de/kb/addons-finden-und-installieren-und-firefox-anpassen, Stand: 06/2023.

Neben der Wahl des Browsers nimmt auch die verwendete Suchmaschine einen großen Einfluss darauf, wie viele und welche Daten getrackt werden.

Die Nutzungsanteile der Suchmaschinen (Desktop) sind schnell beschrieben:

- Google: 95,2 Prozent
- bing (Microsoft): 11,8 Prozent
- Yahoo: 3,01 Prozent
- Yandex (Russland): 2,0 Prozen
- Baidu (Indien): 0,6 Prozen

Quelle: Statista (Stand: 06/2023)[38]

Google dominiert den Markt der Suchmaschinen so eindeutig, dass sich der Begriff „googeln“ zum Synonym für das Suchen nach Informationen im Internet etabliert hat. Auch andere Anbieter wie beispielsweise t-online.de nutzen für ihre Suchmaschine die Google-Plattform, was die Reichweite von Google zusätzlich erhöht. Nachdem Microsoft mit Edge wieder einen konkurrenzfähigen

[37] https://www.verbraucherzentrale-bayern.de/digitale-welt/browserplugin-nervenschoner-endlich-ungestoert-surfen-74152, Stand: 06/2023.

[38] https://de.statista.com/infografik/29264/weltweite-marktanteile-der-groessten-suchmaschinen/, Stand 2026

Browser auf den Markt gebracht hat, nimmt auch der Marktanteil der eigenen Suchmaschine bing wieder ein wenig Fahrt auf. Der frühere Branchenprimus Yahoo spielt heute nur noch eine untergeordnete Rolle.

Google weiß übrigens nicht alles, aber sehr viel über seine Nutzer:innen. So kann der Dienst bereits im Voraus erahnen, was Interessent:innen suchen, welche Routen sie nutzen, welche Begriffe sie verwenden und so weiter. Denn Google lernt ständig dazu, die Interessen und das Verhalten seiner Nutzer:innen genauer einzuschätzen. Dementsprechend besser, das heißt auf die individuelle Person angepasster, werden im Laufe der Zeit dann auch die angezeigten Suchergebnisse. Doch so hilfreich Google sein mag, neben den positiven Seiten gibt es auch Argumente, die gegen eine Nutzung dieser Suchmaschine sprechen.

Wie bereits in Kapitel 3, „Gefahren im Netz durch (legale) Datensammler“, beschrieben, sammelt auch Google eine unglaubliche Menge an Daten über seine Nutzer:innen. Durch die Verknüpfung mit den gesammelten Daten von YouTube (gehört ebenfalls zu Google) entsteht so ein sehr genaues Profil der Nutzer:innen. Auch hier ist das offizielle Ziel, individualisierte Werbung auszuspielen.

Übrigens, selbst wenn man nicht in Google angemeldet ist, sammelt und speichert Google über Cookies [38] alles, was man sucht und besucht!

Wer nicht als Datenlieferant:in herhalten möchte, muss sich anderer Suchmaschinen bedienen. So wirbt beispielsweise DuckDuckGo[40] damit, keine persönlichen Informationen zu sammeln, und dennoch ähnlich gute Ergebnisse zu liefern wie Google.

Von Stiftung Warentest ausgezeichnet wurde der Anbieter startpage.com[41], der mit der Kombination von guten Suchergebnissen und einem sehr hohen Privatsphäreschutz den vorherigen Branchenprimus vom Testthron gestoßen hat.[42]

4.1 E-Mails verschlüsseln

Aber egal, welchen Browser und welche Suchmaschine man wählt – entscheidend ist vor allem das eigene Nutzungsverhalten. Wer unaufmerksam ist und allem zustimmt, macht auch einen sicheren Browser angreifbar!

[39] https://de.wikipedia.org/wiki/HTTP-Cookie, Stand 06/2023

[40] https://duckduckgo.com/, Stand: 06/2023.

[41] https://startpage.com/, Stand: 06/2023.

[42] https://www.test.de/Suchmaschinen-im-Test-Eine-schlaegt-Google-5453360-0/, Stand: 06/2023.

„E-Mails sind wie Postkarten – jede:r kann sie lesen.“ Diese Aussage beschreibt treffend die Sicherheit eines Kommunikationskanals, der allein in Deutschland täglich circa zwei Milliarden Mal genutzt wird. Zwar setzen die meisten E-Mail-Anbieter beim Versand von Mails auf das sogenannte TLS(Transport-Layer-Security)-Protokoll, wodurch die E-Mails während des Transports verschlüsselt sind. Auf ihrem Weg von der sendenden zur empfangenden Person kann eine E-Mail jedoch eine Vielzahl an Servern und Knotenpunkten passieren, wo dieses Protokoll nicht greift und die Nachricht somit im Klartext vorliegt.

Heutige Mailserver und insbesondere die Teilnehmer von „E-Mail – Made in Germany“ (GMX / Web.de / T-Online /1und1 / Freenet) versenden ihre Mails allerdings auf direktem Weg an den Empfänger-Mailserver. Bei der Verwendung von Transportverschlüsselung liegt hier ein direkter und sicherer Übergabeweg vor.

Während Behörden und Unternehmen daher zunehmend mit vollständig verschlüsselten E-Mails arbeiten, gibt es für Privatpersonen noch keine wirklich überzeugend niedrigschwellige Technik, sodass E-Mail-Verschlüsselung in der breiten Masse der Bevölkerung bislang nicht genutzt wird. Man sollte also besser keine wichtigen Daten in einer E-Mail verschicken, sondern ein verschlüsseltes System verwenden.

4.2 Daten verschlüsseln

Bei der Verschlüsselung (Kryptografie) von Daten und Dateien geht es darum, offene Daten mit einem geheimen Schlüssel umzuwandeln, sodass sie für niemanden mehr einsichtig sind. Um sie wieder zugänglich zu machen, benötigt man den Schlüssel. Der Schlüssel ist dabei entweder ein Passwort oder ein Zahlencode. Auf diese Weise behält man die volle Kontrolle über die eigenen Daten und entscheidet selbst, für wen sie zugänglich gemacht werden.

Verschlüsselung auf Windows und Mac
Mit dem bei einigen Windows-Versionen integrierten Bitlocker können Festplatten, Laufwerke oder Wechseldatenträger verschlüsselt werden. Wird der Rechner oder nur die Festplatte gestohlen, können Diebe ohne den Schlüssel beziehungsweise das Passwort nicht auf die Daten zugreifen. Nutzer:innen von **Windows 11 Home** haben leider keine Möglichkeit, den Bitlocker zu nutzen, und müssen auf externe Software zurückgreifen.

Als externe Software empfiehlt sich etwa die kostenlose Software VeraCrypt. Sie bietet eine relativ einfache Bedienung bei zahlreichen Möglichkeiten und einer großen Auswahl an Verschlüsselungsmethoden. VeraCrypt kann auch auf Macs genutzt werden, obwohl Apple von Haus aus bereits verschiedene Möglichkeiten der Verschlüsselung bietet.

Eine Anleitung für die Nutzung von VeraCrypt unter Windows findet sich unter folgendem Link:
https://www.heise.de/tipps-tricks/VeraCrypt-Alles-verschluesselt-4308944.html,
Stand: 06/2023.

Auf einem **Mac** lässt sich die Festplatte mit der integrierten Software FileVault einfach und unkompliziert verschlüsseln. Das Programm befindet sich in der Systemsteuerung. Die Funktionsweise ist ähnlich wie die des oben genannten Bitlockers. Darüber hinaus können am Mac auch einzelne Dateien oder Ordner verschlüsselt werden.

Eine Anleitung dazu gibt es unter folgendem Link:
https://www.heise.de/tipps-tricks/Dateien-verschluesseln-am-Mac-so-geht-s-3867459.html, Stand: 06/2023.

Verschlüsselung von Smartphone und Tablet

Auch die Daten auf Mobilfunkgeräten sollten nach Möglichkeit verschlüsselt sein.

Die Daten auf **Apple iPhones** und **iPads** werden ab dem Moment verschlüsselt, ab dem ein Code, Fingerabdruck oder die Gesichtserkennung zum Öffnen des Gerätes eingerichtet wurde. Diese Verschlüsselung ist so gut, dass selbst die US-amerikanischen Geheimdienste an der Entschlüsselung gescheitert sind und Apple per Klage dazu zwingen wollten, beim Knacken der iPhone-Sperre behilflich zu sein.

Da regelmäßige Back-ups des Systems und der Dateien in der iCloud abgelegt werden, sollte man nicht vergessen, auch für das Back-up die Option „iPhone-Backup verschlüsseln“ zu aktivieren.

Android-Smartphones bieten ebenfalls eine Verschlüsselung auf Dateisystemebene, solange das Smartphone gesperrt ist. Möchte man zusätzlich eine Verschlüsselung auf Dateiebene, erreicht man dies nur mit Drittanbieter-Apps, wie zum Beispiel EgoSecure Encryption.

Weitere Infos zur Installation und Nutzung finden sich hier:
https://www.heise.de/tipps-tricks/Android-Daten-verschluesseln-so-geht-s-4049575.html, Stand: 06/2023.

5. Erste Hilfe: Was tun im Fall von Datendiebstahl?

Viele Onlineaktivitäten dürfen bereits die Jüngsten ohne Aufsicht wahrnehmen: 20 Prozent der Erst- bis Viertklässler nutzen beispielsweise Messengerdienste ohne elterlichen Schulterblick, 51 Prozent der Siebt- bis Zehntklässler kontaktieren Freund:innen in den sozialen Medien unbeaufsichtigt – das sind die Ergebnisse einer Onlineumfrage im Auftrag des BSI, bei der 1000 Eltern von Kindern im Alter von sechs bis 17 Jahren befragt wurden.

Bei aller Selbstständigkeit sollten Eltern jedoch für die Orientierung ihres Nachwuchses sorgen, denn bei der Internetnutzung sind Kinder und Jugendliche den gleichen Gefahren ausgesetzt wie Erwachsene. Laut Umfrage sind die meisten Eltern mit ihren Kindern im Gespräch und legen Verhaltensregeln fest oder sprechen über Schutzmaßnahmen. Am häufigsten geht es um zu hohe In-App-Käufe (66 Prozent), gefolgt von ungeeigneten Inhalten (60 Prozent). Allerdings spricht nicht einmal die Hälfte der Befragten mit ihren Kindern über Spam-Nachrichten oder betrügerische E-Mails (47 Prozent), Schadprogramme (45 Prozent) und E-Mail-Account-Sicherheit (29 Prozent).[43]

Quelle: BSI (Screenshot vom 08.01.2020)

[43] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2019/Weltkindertag_190919.html, Stand: 07/2023.

Die am häufigsten vorkommenden Schadensereignisse entstehen durch E-Mail-Phishing und das „Einfangen“ von Schadsoftware durch das Anklicken von Links in dubiosen Phishing-SMS, in denen beispielsweise die Lieferung eines Paketes angekündigt wird. Im Folgenden die wichtigsten Sofortmaßnahmen, die im Fall der Fälle angebracht sind:

5.1 Sofortmaßnahmen

Ist man Opfer einer Phishing-Attacke geworden und hat seine Benutzerdaten, Passwort, PIN oder TAN auf einer betrügerischen Seite eingegeben, ist Geschwindigkeit der alles entscheidende Faktor.

1. Sofort Passwort oder PIN ändern (siehe Abschnitt 6.2, „Sichere Passwörter“).
2. Die Anbieter umgehend über die Attacke informieren.
3. Handelt es sich um eine Bank, einen Zahlungsanbieter oder Shop, den Zugang und/oder das Konto sperren lassen.
4. Die Phishing-Nachricht per Screenshot sichern und/oder ausdrucken, diese dient im weiteren Ermittlungsverfahren als Beweis und sollte deshalb auch nicht gelöscht werden[44].
5. Bei der Polizei Anzeige erstatten, denn Phishing ist eine Straftat.
6. Den Account im Blick behalten.

Zum Abschluss sei noch einmal explizit darauf verwiesen, dass der beste Schutz vor Internetkriminalität die eigene Achtsamkeit ist. Mit den in diesem Modul beschriebenen Möglichkeiten zum Schutz von Daten kann man die technische Sicherheit auf ein sehr hohes Level heben, ein gewisses Restrisiko bleibt aber immer: Ein einziger unachtsamer Klick und schon ist es passiert!

Die folgenden drei Sätze sollten einem in der virtuellen Welt daher immer präsent sein:

1. **Grundsätzlich misstrauisch sein!**
2. **So viele Daten wie nötig – so wenig Daten wie möglich!**
3. **Erst lesen – dann klicken!**

[44] https://www.verbraucherzentrale-rlp.de/wissen/geld-versicherungen/sparen-und-anlegen/phishing-onlinebanking-zieht-gauner-an-16638, Stand: 06/2023.

6. Links und weiterführende Informationen

6.1 Links

Die Internetseite des Bundesamtes für Sicherheit in der Informationstechnik informiert umfassend über Themen rund um Daten- und Accountsicherheit.	**www.bsi.bund.de**
Die Internetseite mobilsicher.de ist vom Bundesministerium der Justiz und für Verbraucherschutz gefördert und versteht sich als „Infoportal für mehr Sicherheit auf Smartphone und Tablet“.	**www.mobilsicher.de**
Handysektor ist ein Angebot der Landesanstalt für Medien Nordrhein-Westfalen und des Medienpädagogischen Forschungsverbundes Südwest. Hier gibt es Informationen zu verschiedensten Themen rund ums Handy. Auch Infografiken, die beispielsweise im Unterricht eingesetzt werden können, stehen zum Download bereit.	**www.handysektor.de**
Zur Unterstützung des technischen Jugendschutzes ist die Seite Medien kindersicher eine gute Anlaufstelle. Hier werden Schritt für Schritt Jugendschutzeinstellungen für alle gängigen Geräte gezeigt. Die Webseite ist ein Angebot unter anderem der Medienanstalt RLP und von Klicksafe.de	**www.medien-kindersicher.de**
Sowohl für SuS als auch für Lehrkräfte stellt die EU-Initiative Klicksafe Informationen rund um Handy, Smartphone und Co. zur Verfügung. Materialien wie zum Beispiel die Broschüre „Werbung und Kommerz im (mobilen) Internet“ ist in digitaler Form auf ihrer Website verfügbar und kann dort heruntergeladen, aber auch im Printformat bestellt werden.	**www.klicksafe.de**

6.2 Mögliche Verknüpfung mit weiteren Themenaspekten

Soziale Netzwerke: Auch soziale Netzwerke wie Instagram, Facebook und Co. sammeln Daten und sind nicht selten Ziel von Hackerangriffen. Sich beispielsweise die Privatsphäre-Einstellungen oder die für die Anmeldung nötigen Daten genauer anzuschauen, kann sinnvoll sein. Voraussetzung ist natürlich, dass die SuS die entsprechende Anwendung bereits zum großen Teil nutzen. Das Thema „Soziale Netzwerke“ wird in „Medien sicher nutzen“-Modul 4 behandelt.

Onlinewerbung: Daten werden nicht nur für kriminelle Handlungen verwendet, sondern vor allem auch für personenbezogene Werbung. Die beiden Themen lassen sich über die Frage, wofür Daten gesammelt, verkauft oder gestohlen werden, sehr gut verknüpfen. Das Thema Onlinewerbung wird in „Medien sicher nutzen“-Modul 2 behandelt.

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

7. Erarbeitungsphase

Ziele:

- Die SuS können ihre eigene Onlinepräsenz besser einschätzen und kennen Risiken.
- Die SuS können unterscheiden, was eine private und was eine öffentliche Information ist.
- Die SuS können einschätzen, welche Informationen sie mit Onlinediensten teilen und was diese daraus machen.
- Die SuS können Phishing-Mails erkennen.
- Die SuS wissen, was Datenlecks sind und welche Gefahren damit verbunden sind, und wissen, wie sie herausfinden können, ob Accounts betroffen sind.
- Die SuS wissen, wie man sichere Passwörter erstellt, und kennen verschiedene Arten, sie zu speichern,
- Die SuS sind sensibilisiert gegenüber Identitätsdiebstahl und wissen, wie sie sich davor schützen können,
- Die SuS kennen verschiedene Browser und können sie datenschutztechnisch bewerten.
- Die SuS wissen, was 2-Faktor-Authentifizierung ist und warum man sie anwenden sollte.

	Methode	Zeit (Minuten)	Arbeits- und Sozialform/Methode	Medien/ Material
① ② ③ 👁	01 Mein digitales Leben	20	Mindmap in Einzelarbeit, Diskussion im Plenum	Papier, Stifte, farbige Marker
① ② ③ 👁	02 Was gehört zu mir?	20	Einzelarbeit, dann Plenum	Papier, Stifte
① ② ③ 👁	03 Rate mal!	15	Gruppenarbeit, Plenum	Kartenset „Rate mal“
① ② ③ 👁 👆	04 Was teilst du?	15	Einzel- oder Gruppenarbeit	Arbeitsblatt „Was teilst du?“ oder Onlinequiz: https://learningapps.org/display?v=p0vzhk0z223
① ② ③ 👁	05 Nichts zu verbergen?	15	Gruppenarbeit	Argumente-Sammlung „Nichts zu verbergen“ für Lehrkraft
① ② ③ 👁	06 Leckere Kekse	20	Gruppenarbeit, Plenum	Kartenset „Leckere Kekse“
① ② ③ (👁 👆)	07 Echt oder Betrug?	20	Einzelarbeit, Gruppengespräch	Quiz „Echt oder Betrug?“, Stifte, Onlinequiz: https://phishingquiz.withgoogle.com/
① ② ③ 👁	08 Papier oder App?	30	Gruppenarbeit, Plenum	Arbeitsblatt „Papier oder App?“, Vor- und Nachteilsammlung „Papier oder App?“ für Lehrkraft
① ② ③ 👁 👆	09 Passwortprofis	30	Einzel-, Partner- oder Gruppenarbeit	Papier, Stifte,PC/Tablet
① ② ③ (👁 👆)	10 Identitätsdiebstahl	90	Gruppenarbeit, Plenum	Szenarien „Identitätsdiebstahl“
① ② ③ 👆	11 Hacker:innen auf der Spur	30	Einzel- und Gruppenarbeit	Arbeitsblatt „Hacker:innen auf der Spur“, Leakchecker: https://haveibeenpwned.com

①②③	12 Messenger-Contest	30	Einzel- oder Gruppenarbeit, Plenum	Arbeitsblatt „Messenger-Contest“
①②③	13 Zum Wegwerfen	25	Gruppenarbeit, Plenum	www.wegwerfmail.de oder www.trash-mail.com
①②③ (🖱)	14 Schütz dein Gerät	45	Einzel- und Gruppenarbeit	Quiz „Schütz dein Gerät“ oder Onlinequiz: https://learningapps.org/display?v=pnembxvxt23
①②③ (🖱)	15 Schütz dich vor Viren	45	Einzelarbeit, Gruppenarbeit, Plenum	Quiz „Schütz dich vor Viren“ oder Onlinequiz: https://learningapps.org/display?v=p99jxi7c523
①②③	16 Browser-detektive	20	Einzelarbeit, Plenum	Arbeitsblatt „Browserdetektive“
①②③🖱	17 Browserprofis	20	Gruppenarbeit, Plenum	Hintergrundinformationen aus dem Theorieteil
①②③ (🖱)	18 Doppelt hält besser	45	Gruppenarbeit	Szenarien „Doppelt hält besser“

Hinweise:

①②③ Schwierigkeitsstufen der jeweiligen Methoden. Zutreffendes ist rot gefüllt.
👁 sprachlich leicht zugänglich
🖱 Onlinematerial
SuS: Schülerinnen und Schüler

7.1 Mein digitales Leben

Dauer:	20 Minuten
Ziel:	Selbsteinschätzung der eigenen Onlinepräsenz und potenzieller Risiken
Schwierigkeit:	① ② ③
Material:	Papier, Stifte, eventuell farbige Marker
Technik:	keine
Sozialform:	Einzelarbeit, dann Gruppendiskussion
Umsetzung:	Die SuS erstellen eine Mindmap aller Orte, an denen sie online sind (zum Beispiel Social Media, Onlinespiele, Lernplattformen). Anschließend sollen sie markieren, wo sie bereits persönliche Informationen geteilt haben und in Gruppen oder im Plenum potenzielle Risiken diskutieren.
Hinweise:	Ermutigen Sie die SuS, ehrlich zu sich selbst zu sein und ihre echten Onlineaktivitäten zu berücksichtigen. Die Übung eignet sich generell für den Einstieg in das Thema Mediennutzung.

7.2 Was gehört zu mir?

Dauer:	20 Minuten
Ziel:	Erkennen von öffentlichen und privaten Informationen
Schwierigkeit:	① ② ③
Material:	Papier, Stifte
Technik:	keine
Sozialform:	Einzelarbeit, dann Plenum
Umsetzung:	Die SuS bekommen je einen Bogen Papier und Zeichenutensilien. Sie sollen auf der einen Seite Dinge zeichnen, die jeder wissen darf (zum Beispiel Haarfarbe, Lieblingsfarbe), und auf der anderen Dinge, die privat sind (zum Beispiel. Adresse, Telefonnummer). Danach erfolgt eine Besprechung der Ergebnisse im Plenum
Hinweise:	Ermutigen Sie die SuS auch an Informationen zu denken, die nicht direkt physisch sind, wie zum Beispiel Gefühle oder Geheimnisse.

7.3 Rate mal

Dauer:	15 Minuten
Ziel:	Erkennen, welche Informationen sicher geteilt werden können
Schwierigkeit:	1 2 3
Material:	Kartenset „Rate mal“
Technik:	keine
Sozialform:	Gruppenarbeit
Umsetzung:	Die SUS ziehen je eine Karte aus dem vorbereiteten Set, lesen den Inhalt vor und die anderen aus der Gruppe müssen raten, ob dies eine Information ist, die man teilen sollte oder nicht.

7.4 Was teilst du?

Dauer:	15 Minuten
Ziel:	Erkennen, welche Informationen sicher geteilt werden können
Schwierigkeit:	1 2 3
Material:	Arbeitsblatt „Was teilst du?“ oder Onlinequiz „Was teilst du?“: https://learningapps.org/display?v=p0vzhk0z223
Technik:	Bei Onlinequiz Computer oder Tablet, Internetzugang, Beamer/Smartboard
Sozialform:	Einzel- oder Gruppenarbeit, je nach Anzahl der Geräte
Umsetzung:	Die SuS bekommen das Arbeitsblatt oder den Link zum Onlinequiz und müssen entscheiden, ob bestimmte Informationen sicher geteilt werden können oder nicht.

7.5 Nichts zu verbergen?

Dauer:	15 oder 30 Minuten
Ziel:	Reflexion über das „Nichts zu verbergen“-Argument
Schwierigkeit:	① ② ③
Material:	Papier und Stifte für Notizen, Argumente-Sammlung „Nichts zu verbergen“
Technik:	keine
Sozialform:	Gruppenarbeit
Umsetzung:	In Gruppen diskutieren die SuS, warum manche Leute denken, sie hätten „nichts zu verbergen“. Sie listen Vor- und Nachteile auf und teilen ihre Ergebnisse mit der Klasse.
Erweiterung:	Die Übung kann auch als Debatte durchgeführt werden. Dafür wird die Klasse in zwei Gruppen geteilt: Eine Gruppe argumentiert, warum „Ich habe nichts zu verbergen“ ein gültiger Punkt ist, die andere argumentiert dagegen. Nach einer kurzen Vorbereitungszeit folgt eine Debatte, gefolgt von einer Abschlussdiskussion.
Hinweise:	Geben Sie den SuS Strukturhilfen für die Diskussion, Argumente finden Sie in der zur Übung gehörenden Argumente-Sammlung.

7.6 Leckere Kekse

Dauer:	20 Minuten
Ziel:	Verständnis der Funktionsweisen von Cookies und Erkennen von Vorteilen und möglichen Nachteilen
Schwierigkeit:	① ② ③
Material:	Kartenset „Leckere Kekse“, Stifte
Sozialform:	Gruppenarbeit, Plenum
Durchführung:	Die SuS werden in Gruppen aufgeteilt. Jede Gruppe bekommt Karten mit verschiedenen Szenarien, wie zum Beispiel: „Du besuchst eine Website und sie erinnert sich an deine Spracheinstellung.“ Die Gruppen müssen dann entscheiden, ob dies ein Vorteil oder Nachteil von Cookies ist und warum. Im Anschluss werden die Ergebnisse im Plenum besprochen.
Hinweise:	Die SuS sollten vorher wissen, was Cookies sind und wie sie funktionieren.

7.7 Echt oder Betrug?

Dauer:	20 Minuten
Ziel:	Grundverständnis von Spam und Phishing entwickeln und Erkennungsmerkmale von betrügerischen E-Mails und SMS identifizieren
Schwierigkeit:	1 2 3 (👁 ☝)
Material:	Für Schwierigkeitsgrad „einfach“: Quiz „Echt oder Betrug?“, Stifte Für Schwierigkeitsgrad „mittel“ bis „schwierig“: Onlinequiz: https://phishingquiz.withgoogle.com/
Technik:	Bei Onlinequiz Computer oder Tablet, Internetzugang, Beamer/Smartboard
Sozialform:	Einzelarbeit, kurzes Gruppengespräch
Durchführung:	Beginnen Sie mit einer kurzen Einführung, was Spam und Phishing sind. Dann können die SuS die Beispiele auf dem Arbeitsblatt durchgehen und diese als echt oder gefälscht markieren. Ältere SuS, die über etwas Vorwissen verfügen, können das Onlinequiz machen.

7.8 Papier oder App?

Dauer:	30 Minuten
Ziel:	Verständnis für das Speichern von Passwörtern entwickeln und Unterscheidung zwischen analogen und digitalen Speichermethoden
Schwierigkeit:	1 2 3 👁
Material:	Arbeitsblatt „Papier oder App?“, Vor- und Nachteilsammlung „Papier oder App?“
Technik:	Smartboard/Beamer (optional)
Sozialform:	Gruppenarbeit
Durchführung:	Die SuS sollen die Sätze auf der einen Seite des Arbeitsblattes den Optionen Passwortheft beziehungsweise Passwortmanager zuordnen. Anschließend können im Plenum Vor- und Nachteile der beiden Speichermethoden gesammelt und diskutiert werden.

7.9 Passwortprofis

Dauer:	30 Minuten
Ziel:	Verständnis für sichere versus unsichere Passwörter entwickeln und Techniken zur Erstellung von Passwörtern kennenlernen
Schwierigkeit:	1 2 3
Material:	Papier, Stifte, Tafel/Whiteboard
Technik:	Computer oder Tablet, Internetzugang, Beamer/Smartboard
Sozialform:	Einzel- und/oder Partnerarbeit
Durchführung:	Beginnen Sie mit Beispielpasswörtern auf Flipchart/Tafel (zum Beispiel „123456“, „passwort“, „geheim“, „999999“, „Max2009“) und fragen Sie die SuS, welche sie als sicher/unsicher einstufen würden. Danach führen Sie die SuS in Passworttechniken im jeweiligen Schwierigkeitsgrad ein. Im Anschluss sollen die SuS eigene Passwörter erstellen und diese dann entweder in Partnerarbeit oder online auf ihre Sicherheit hin überprüfen. **Schwierigkeitsgrad 1:** Einführung in einfache Techniken: Mischung von Groß- und Kleinbuchstaben, Zahlen und Symbolen. **Schwierigkeitsgrad 2:** Einführung in den Nutzen von Passwortphrasen (zum Beispiel „BlauerHundLachtImMondlicht!“) **Schwierigkeitsgrad 3:** Einführung in Akronym-Passwörter. (zum Beispiel: „Ich mag jeden Tag um 7 Uhr Eis!“ wird zu „ImjTu7UE!“) Webseite zur Überprüfung der Passwörter: https://checkdeinpasswort.de/
Hinweise:	Machen Sie den SuS deutlich, dass sie Übungspasswörter entwerfen und testen sollen, nicht echte eigene. Das gilt insbesondere dann, wenn die Passwörter in Partnerarbeit bewertet werden!

7.10 Identitätsdiebstahl

Dauer:	90 Minuten
Ziel:	Bewusstsein für die Gefahren von Identitätsdiebstahl schärfen, Wissen über den Schutz der eigenen Identität im Internet vermitteln, Diskussionsfähigkeit und Teamarbeit fördern
Schwierigkeit:	1 2 3 ()
Material:	Flipchart oder Tafel, Marker/Stifte, Papier für Notizen und Regelkatalog, Arbeitsblatt „Identitätsdiebstahl“
Technik:	Smartboard/Beamer (optional, für die Präsentation der Fallbeispiele), Computer mit Internetzugang (optional, zur Recherche)
Sozialform:	Gruppenarbeit (Diskussion und RegelkatalogeErstellung), Plenum (Präsentation der Regelkataloge und Diskussion)
Durchführung:	Teilen Sie die SuS in kleinere Gruppen (drei bis fünf SuS) auf. Jede Gruppe erhält ein oder mehrere Fallbeispiele aus dem Arbeitsblatt. Die Gruppen lesen und diskutieren die Beispiele und sollen im Anschluss eine bis drei Regeln formulieren, bei deren Einhaltung das Beispiel einen anderen und positiven Ausgang genommen hätte. Im Anschluss präsentiert jede Gruppe ihre Regeln im Plenum und die Klasse erstellt gemeinsam einen Regelkatalog. Dieser kann ausgedruckt und in der Klasse aufgehängt werden.

7.11 Hacker:innen auf der Spur

Dauer:	30 Minuten
Ziel:	Verständnis dafür, was Datenlecks sind und wie häufig sie vorkommen, Einführung in Tools wie HPI Identity Leak Checker oder haveibeenpwned.com
Schwierigkeit:	1 2 3
Material:	Arbeitsblatt „Hacker:innen auf der Spur“, Zugang zu einem der Leakchecker https://sec.hpi.de oder https://haveibeenpwned.com
Technik:	Computer mit Internetverbindung, optional Smartboard/Beamer
Sozialform:	Einzelarbeit, Plenum
Durchführung:	Die SuS sollen die E-Mail-Adressen in einem Leakchecker überprüfen. Diskutieren Sie dann im Plenum über die Ergebnisse und die Bedeutung von Datenlecks.
Hinweise:	Achten Sie darauf, dass SuS nicht ihre eigenen E-Mail-Adressen verwenden.

7.12 Messenger-Contest

Zeit:	30 Minuten
Ziel:	Tiefere Einsicht in die Funktion und den Datenschutz verschiedener Messenger-Apps
Schwierigkeit:	① ② ③
Material:	Arbeitsblatt „Messenger-Contest“, Stifte
Technik:	optional Computer oder Tablets, Smartboard/Beamer
Sozialform:	Einzel- oder Gruppenarbeit, Plenum
Durchführung:	Nach einer kurzen Präsentation über die drei Messenger-Apps und deren Datenschutzpraktiken erhalten die SUS entweder einzeln oder in Gruppen das Arbeitsblatt. Sie füllen es aus und sollen entscheiden, welchen sie als Sieger küren und erklären, warum. Anschließend erfolgt eine Diskussion der Ergebnisse im Plenum.

7.13 Zum Wegwerfen

Dauer:	25 Minuten
Ziel:	Die SuS sollen die Funktionsweise und den Zweck von Wegwerf-E-Mail-Adressen verstehen.
Schwierigkeit:	① ② ③
Material:	Zugang zur Webseite xyz
Technik:	PC/Tablet mit Internetzugang, Smartboard/Beamer
Sozialform:	Gruppenarbeit, Plenumsdiskussion
Durchführung:	Die SuS in Gruppen einteilen. Sie sollen eine Wegwerf-E-Mail-Adresse bei einem der deutschen Anbieter www.wegwerfmail.de oder www.trash-mail.com erstellen und diese für die Anmeldung auf der Seite xyz verwenden. Anschließend soll die Gruppe die Fragen auf dem Arbeitsblatt diskutieren. Nach Abschluss der Übung wird im Plenum darüber gesprochen, welche Vor- und Nachteile sie gesehen haben und wie sie sich dabei gefühlt haben.
Hinweise:	Nach Abschluss der Übung sollte den SuS klar sein, dass diese Dienste zwar praktisch sind, aber nicht für jeden Zweck. Man kann sie nutzen, um Spam zu vermeiden oder sich für Dienste zu registrieren, von denen man keine weiteren E-Mails erhalten möchte. Man sollte sie jedoch nicht für vertrauliche oder wichtige Kommunikationen verwenden und es ist ratsam, sich über die Sicherheitsrichtlinien und Nutzungsbedingungen des jeweiligen Dienstes zu informieren.

7.14 Schütz dein Gerät

Zeit:	30 Minuten
Ziel:	Unterscheidung verschiedener Schutzarten
Schwierigkeit:	① ② ③ (🖱)
Material:	Arbeitsblatt „Schütz dein Gerät“ oder Onlinequiz „Schütz dein Gerät“
Technik:	Smartboard/Beamer, Computer, eventuell Smartphones/Tablets
Sozialform:	Einzelarbeit, Gruppenarbeit, Plenum
Durchführung:	Die SuS bearbeiten das Quiz entweder auf dem Arbeitsblatt oder online. Anschließend Diskussion im Plenum über die Vor- und Nachteile der verschiedenen Schutzarten.

7.15 Schütz dich vor Viren

Zeit:	30 Minuten
Ziel:	Verständnis der Notwendigkeit von Virenschutz und VPN, kritisches Denken bei App-Berechtigungen
Schwierigkeit:	① ② ③ (🖱)
Material:	Arbeitsblatt „Schütz dich vor Viren “ oder Onlinequiz „Schütz dich vor Viren“
Technik:	Smartboard/Beamer, Computer, eventuell Smartphones/Tablets
Sozialform:	Einzelarbeit, Gruppenarbeit, Plenum
Durchführung:	Die SuS bearbeiten das Quiz entweder auf dem Arbeitsblatt oder Online. Anschließend Diskussion im Plenum über die Vor- und Nachteile der verschiedenen Schutzarten.

7.16 Browserdetektive

Zeit:	20 Minuten
Ziel:	Grundverständnis darüber erlangen, was ein Internetbrowser ist und warum man vorsichtig sein sollte
Schwierigkeit:	1 2 3
Material:	Arbeitsblatt „Browserdetektive“, Stifte
Technik:	Smartboard/Beamer (optional)
Sozialform:	Einzelarbeit, Plenum
Durchführung:	Die SuS bekommen das Arbeitsblatt mit den Bildern von verschiedenen Browser-logos und sollen den richtigen Namen zuordnen. Anschließend kurze Diskussion: „Was macht man mit einem Browser?“
Hinweise:	Die Übung lässt sich auch im Plenum durchführen. Dazu einfach die Logos zeigen und die SuS sollen sagen, welche sie kennen.

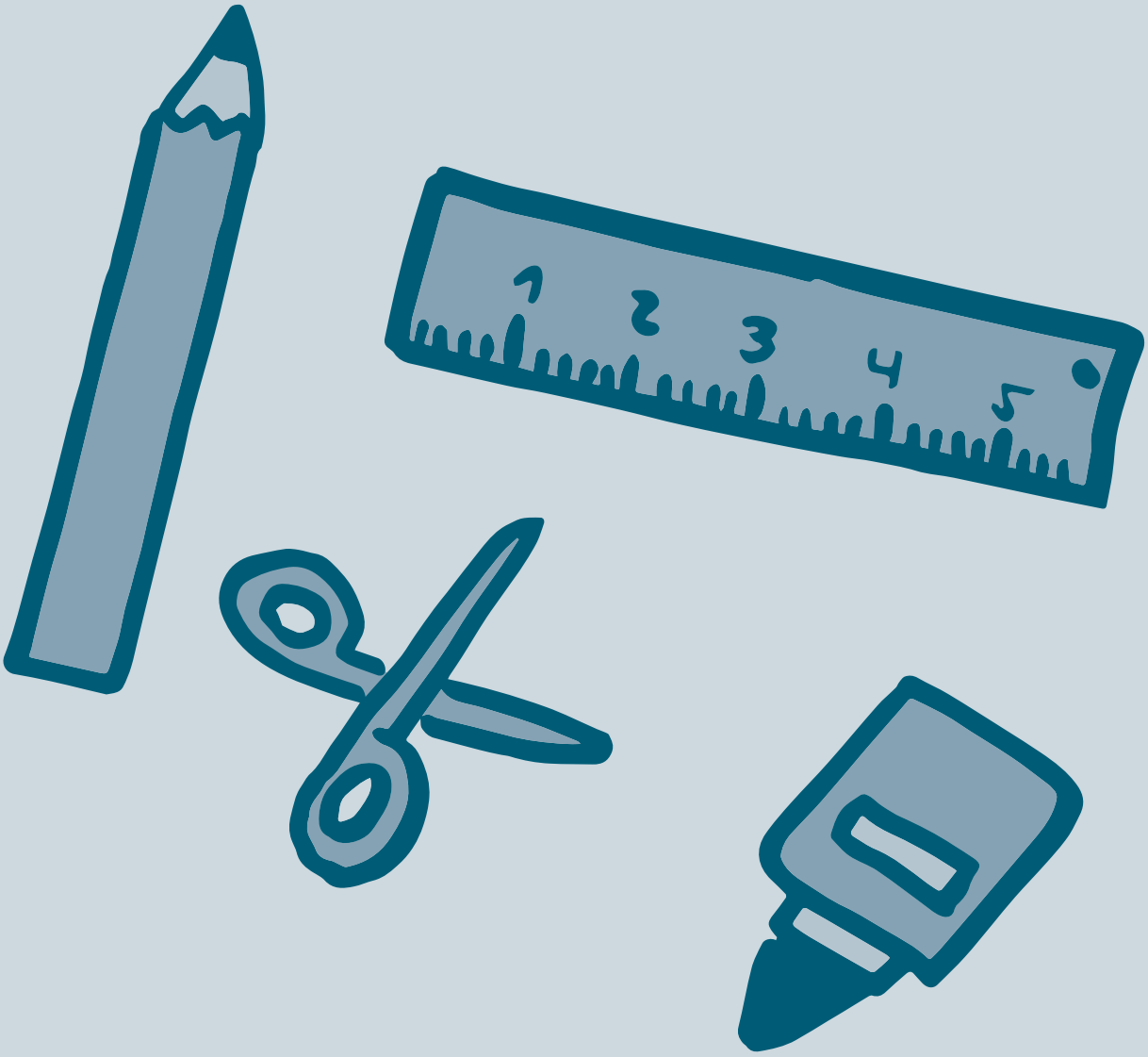
7.17 Browserprofis

Zeit:	30 Minuten
Ziel:	erweitertes Verständnis über Internetbrowser, Datenschutz und sicheres Surfen
Schwierigkeit:	1 2 3
Material:	Hintergrundinformation aus dem Theorieteil
Technik:	Computer mit Internetzugang, Smartboard/Beamer
Sozialform(en):	Gruppenarbeit, Plenum
Durchführung:	Die SuS werden in Gruppen aufgeteilt. Jede Gruppe bekommt einen Browser zugeteilt (zum Beispiel Chrome, Edge, Firefox, Safari, Brave, TOR) und recherchiert dessen Datenschutzfeatures. Die Gruppen präsentieren ihre Ergebnisse im Plenum. Anschließend wird diskutiert: „Welcher Browser scheint am sichersten zu sein und warum?“
Hinweise:	Die SuS sollten ausdrücklich zu kritischem Denken und der Analyse von Informationen angeregt werden.

7.18 Doppelt hält besser

Zeit:	45 Minuten
Ziel:	erweitertes Verständnis von 2FA und Identifizierung von Situationen, in denen sie nützlich ist
Schwierigkeit:	① ② ③ (🖱)
Material:	Arbeitsblatt „Doppelt hält besser“, Stifte
Technik:	Computer/Tablet (optional), Smartboard/Beamer
Sozialform:	Gruppenarbeit, Plenum
Durchführung:	Die SuS werden in Gruppen aufgeteilt. Jede Gruppe erhält eine Karte mit einem Szenario, in dem 2FA nützlich wäre. Die SuS diskutieren die darauf-stehenden Fragen in Gruppen und präsentieren dann der Klasse, warum 2FA in diesem Szenario wichtig ist.

8. Materialien zur Erarbeitungsphase



8.1 Kartenset „Rate mal“

„Ich habe blonde Haare.“

„Ich wohne in der Blumenstraße 7, 12345 Sonnenstadt.“

„Fußball ist mein Lieblingssport.“

„Meine Telefonnummer ist 01234 56789.“

„Ich habe einen großen Bruder und eine kleine Schwester.“

„Das Passwort für meinen Computer ist ‚Schokokuchen‘.“

„Meine Mutter heißt Susanne und arbeitet bei der Firma ‚Sonnenschein AG‘.“

„Mein Geburtstag ist am 15. August.“

„Meine beste Freundin und ich gehen nach der Schule immer zum Spielplatz in der Nähe des großen Supermarkts.“

„Ich trage gerne rote Schuhe.“

8.2 Quiz „Was teilst du“

Lies die Fragen sorgfältig durch und beantworte sie.

1. Welche Information sollte man NICHT in einem sozialen Netzwerk teilen?

A) Mein Lieblingstier ist der Delfin.

B) Meine Adresse ist Sonnenallee 10.

C) Ich mag Pizza.

D) Meine Lieblingsfarbe ist Blau.

Richtige Antwort: _____

2. Was solltest du tun, wenn dich jemand online nach deinem Passwort fragt?

A) Es ihm sofort mitteilen.

B) Es nur teilen, wenn es ein Freund ist.

C) Es niemandem mitteilen.

D) Ein neues Passwort erstellen und dieses teilen.

Richtige Antwort: _____

3. Was bedeutet es, wenn ein Schlosssymbol in der Adresszeile eines Browsers angezeigt wird?

A) Die Website verkauft Schlösser.

B) Die Website ist sicher und verschlüsselt.

C) Die Website hat ein Spiel über Schlösser.

D) Die Website ist nicht sicher.

Richtige Antwort: _____

4. Ein Freund schickt dir einen Link zu einem coolen Video, aber der Link sieht seltsam aus. Was solltest du tun?

A) Klicke sofort darauf, es ist ja von einem Freund.

B) Frage deinen Freund persönlich oder am Telefon, bevor du daraufklickst.

C) Teile den Link mit anderen Freunden.

D) Lösche deine gesamte Nachrichtenchronik.

Richtige Antwort: _____

5. Wenn du ein Onlinespiel spielst und jemand dich bittet, dich im echten Leben zu treffen, solltest du ...

A) zustimmen und ihn oder sie alleine treffen.

B) zustimmen, aber nur an einem öffentlichen Ort.

C) deinen Eltern oder einem anderen Erwachsenen davon erzählen, bevor du etwas tust.

D) deine Adresse geben, damit sie zu dir kommen kann.

Richtige Antwort: _____

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

8.3 Lösungsblatt „Was teilst du?“

Richtige Antwort 1: B) Meine Adresse ist Sonnenallee 10.

Richtige Antwort 2: C) Es niemandem mitteilen.

Richtige Antwort 3: B) Die Website ist sicher und verschlüsselt.

Richtige Antwort 4: B) Frage deinen Freund persönlich oder am Telefon, bevor du daraufklickst.

Richtige Antwort 5: C) Deinen Eltern oder einem anderen Erwachsenen davon erzählen, bevor du etwas tust.

8.4 Argumente-Sammlung „Nichts zu verbergen“

Pro-Argumente (für die Aussage „Ich habe doch nichts zu verbergen“):

- Wenn man nichts Unrechtes tut, muss man sich keine Sorgen um die Konsequenzen machen (Transparenz)
- Überwachung kann dazu beitragen, kriminelle Aktivitäten zu verhindern oder aufzudecken (öffentliche Sicherheit).
- Wenn man nichts zu verbergen hat, können Prozesse, zum Beispiel bei der Einreise an Flughäfen, schneller und reibungsloser ablaufen (Effizienz).
- Wenn alle ihre Daten teilen, könnten daraus Vorteile für die Allgemeinheit entstehen, zum Beispiel in der medizinischen Forschung (Nutzen für die Allgemeinheit).
- Viele Onlinedienste sind personalisiert und verbessern das Nutzererlebnis durch Datenanalyse (Komfort beziehungsweise Bequemlichkeit).
- Ein „Teilen“ von Informationen kann zu mehr sozialer Vernetzung und Gemeinschaftssinn führen (soziale Teilhabe).
- Einige Menschen vertrauen darauf, dass Regierungen und Organisationen die Daten hauptsächlich zum Schutz der Bürger:innen und im besten Interesse der Gesellschaft sammeln (Vertrauen in Institutionen).
- Ohne das Gefühl, Informationen verbergen zu müssen, erleben einige Menschen weniger Stress und fühlen sich freier in ihrem täglichen Leben (Lebensstil).

Contra-Argumente (gegen die Aussage „Ich habe doch nichts zu verbergen“):

- Selbst wenn man „nichts zu verbergen“ hat, sollte das Recht auf Privatsphäre geachtet werden (Grundrechte).
- Es besteht immer die Gefahr, dass gesammelte Daten missbraucht werden, sei es durch Unternehmen, Regierungen oder kriminelle Akteure (Missbrauch).
- Fehlerhafte Daten oder falsche Interpretationen können zu ungerechtfertigten Vorwürfen oder Diskriminierung führen (Fehldeutung).
- Das Wissen um ständige Überwachung kann Menschen davon abhalten, ihre Meinung zu äußern oder an bestimmten Aktivitäten teilzunehmen (Chilling Effect).
- Einmal geteilte Daten können oft nicht wieder zurückgeholt werden, und es ist unklar, wie sie in der Zukunft genutzt werden könnten (Kontrollverlust).
- Wenn Daten monetarisiert werden, entsteht ein Markt rund um persönliche Informationen, den der oder die Einzelne nicht kontrollieren kann (ökonomische Interessen).
- Durch umfangreiche Datensammlungen könnten Profile erstellt werden, die Vorurteile und Diskriminierung fördern (Profiling).
- Daten, die heute als harmlos angesehen werden, könnten in der Zukunft gegen Individuen verwendet werden, zum Beispiel bei politischen oder gesellschaftlichen Veränderungen (Unvorhersehbarkeit).

8.5 Kartenset „Leckere Kekse“

Du besuchst eine Website und sie erinnert sich an deine Spracheinstellung.

Du hast einen Artikel in einem Onlineshop in den Warenkorb gelegt, aber nicht gekauft. Einige Tage später erhältst du eine E-Mail-Erinnerung von diesem Shop über den nicht abgeschlossenen Kauf.

Du besuchst eine Online-buchhandlung und sie schlägt dir sofort Bücher basierend auf deinen letz-ten Suchanfragen vor.

Während du online nach Urlaub suchst, bemerkst du, dass die Preise steigen, jedes Mal wenn du die Seite erneut aufrufst.

Nachdem du im Internet nach Symptomen einer Krankheit gesucht hast, wirst du plötz-lich auf vielen Webseiten mit Werbung für Medikamente und Gesundheitsprodukte bombardiert.

Du schaust dir ein Video über ein neues Videospiel auf YouTube an. Danach werden dir auf fast jeder Webseite Werbeanzeigen für dieses oder ähnliche Spiele gezeigt.

Nachdem du dir online Turn-schuhe einer bestimmten Marke angesehen hast, wer-den dir überall Videos und Bil-der von Prominenten gezeigt, die genau diese Schuhmarke tragen.

Nachdem du online nach Tipps für ein bestimmtes Handyspiel gesucht hast, siehst du ständig Werbe-anzeigen für In-Game-Käufe in diesem Spiel.

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

8.6 Quiz „Echt oder Betrug?“

Lies dir die Nachrichten durch und entscheide, ob du sie für echt oder für Phishing hältst. Begründe danach, warum du so entschieden hast.

Von: Onlinespiel – MonsterWorld

Nachricht:
„Du hast 100 Coins in MonsterWorld gewonnen! Klicke auf den Link, um deinen Preis zu holen!“

☐ Echt ☐ Phishing

Wenn du Phishing gewählt hast: Was war das verräterischste Zeichen, dass die Nachricht ein Betrug war?

Von: Mama

Nachricht:
„Hallo Liebling, ich hole dich heute um 14 Uhr von der Schule ab. Pack bitte deinen Turnbeutel ein.“

☐ Echt ☐ Phishing

Wenn du Phishing gewählt hast: Was war das verräterischste Zeichen, dass die Nachricht ein Betrug war?

Von: BankDeutschland123

Nachricht:
„Dringend! Dein Bankkonto ist in Gefahr. Bitte sende uns sofort deinen Benutzernamen und dein Passwort, damit wir es schützen können.“

☐ Echt ☐ Phishing

Wenn du Phishing gewählt hast: Was war das verräterischste Zeichen, dass die Nachricht ein Betrug war?

Von: [Name deiner Schule] – Sekretariat

Nachricht:
„Hallo, bitte denk daran, das Einverständnisformular für den Schulausflug nächste Woche abzugeben. Das Formular findest du im Anhang."

☐ Echt ☐ Phishing

Wenn du Phishing gewählt hast: Was war das verräterischste Zeichen, dass die Nachricht ein Betrug war?

Von: KostenloseGeschenke

Nachricht:
„Glückwunsch! Du wurdest ausgewählt, ein kostenloses Handy zu erhalten. Klicke auf den Link und gib deine Adresse ein, um es zu bekommen!"

☐ Echt ☐ Phishing

Wenn du Phishing gewählt hast: Was war das verräterischste Zeichen, dass die Nachricht ein Betrug war?

Von: MaxMustermann@email.de

Nachricht:
„Hallo, ich habe diese coole Webseite gefunden. Schau sie dir an! [Link]"

☐ Echt ☐ Phishing

Wenn du Phishing gewählt hast: Was war das verräterischste Zeichen, dass die Nachricht ein Betrug war?

8.7 Lösungsblatt „Echt oder Betrug?“

Die richtigen Antworten sind:

- Phishing
- Echt
- Phishing
- Echt (aber immer darauf hinweisen, dass Anhänge von unbekannten Absendern nicht geöffnet werden sollten)
- Phishing
- Phishing

Die Haupterkenntnis für die SuS sollte sein, dass verdächtige Links, Angebote, die zu gut klingen, um wahr zu sein, und Nachrichten, die nach persönlichen Informationen fragen, oft Betrugsversuche sind. Die SuS sollten zudem lernen, dass selbst vertrauenswürdig erscheinende E-Mails gefälscht sein können. Aufforderungen zum Klicken auf Links, das Herunterladen von Anhängen oder das Teilen persönlicher Informationen sollten immer mit Vorsicht behandelt werden. Sie sollten auch die Bedeutung von Absenderadressen und der Prüfung offizieller Kanäle (zum Beispiel durch Anrufen der Bank oder direktes Einloggen auf der offiziellen Webseite statt Klicken auf Links) verstehen.

8.8 VOR- UND NACHTEILSAMMLUNG „Papier oder App?“

Damit man seine Passwörter nicht vergisst, sollte man sie speichern. Dafür kann man sie ganz einfach in ein Heft oder auf einen Zettel schreiben oder man speichert sie in einer Passwortmanager-App. Beide Methoden haben Vor- und Nachteile. Ordne die Vor- und Nachteile der jeweiligen Methode zu.

		
Hiermit kann man automatisch neue Passwörter erstellen.		
Das ist sicherer gegen Wasser.		
Das kann man auf dem Handy benutzen.		
Das kann man mit Farben oder Stickern gestalten.		
Hiermit findet man einzelne Passwörter besser, wenn man viele hat.		
Das muss man nicht aufladen.		
Das könntest du schneller verlieren.		
Das wird schneller geklaut.		
Das ist für Diebe schneller nutzbar, wenn sie es geklaut haben.		
Das warnt mich, wenn meine Passwörter nicht sicher sind oder gehackt wurden.		
Das kann mehr Geld kosten.		

8.9 Vor- und Nachteilsammlung „Passwortheft und Passwortmanager“

Passwortheft

Vorteile:
- kein Strom benötigt
- physisch greifbar
- unabhängig von Software

Nachteile:
- kann verloren gehen
- nicht verschlüsselt
- muss manuell aktualisiert werden

Digitaler Passwortmanager

Vorteile:
- verschlüsselt
- automatische Updates/Änderungen
- Cross-Plattform-Zugriff
- Passwortgenerierung

Nachteile:
- anfällig für Hacks
- benötigt Strom/Technik
- manchmal kostenpflichtig

8.10 Szenarien „Identitätsdiebstahl“

Lisa und das soziale Netzwerk:

Lisa erstellt ein Profil auf einem sozialen Netzwerk und teilt dort viele persönliche Informationen wie Geburtsdatum, Adresse und ihre Schule.

Ein Betrüger findet Lisas Profil und sammelt ihre Informationen. Er erstellt ein zweites Profil im Namen von Lisa und tritt mit ihren Freunden in Kontakt. Einige Freunde teilen vertrauliche Informationen oder leihen dem falschen Profil Geld.

Max und das Onlinespiel:

Max spielt ein Onlinespiel und möchte schnell Fortschritte machen. Er gibt seine Log-in-Informationen auf einer betrügerischen Webseite ein, um angeblich kostenlose In-Game-Währung zu erhalten.

Die Betrüger nutzen Max’ Log-in-Daten, um auf sein Spielkonto zuzugreifen.

Sie verkaufen seine virtuellen Gegenstände und geben echtes Geld aus, das Max’ Eltern später auf ihrer Rechnung finden.

Sophia und die E-Mail:

Sophia bekommt eine E-Mail, die so aussieht, als wäre sie von ihrer Bank. In der E-Mail wird sie aufgefordert, ihr Passwort zurückzusetzen.

Sophia klickt auf den Link in der E-Mail und gibt ihr altes und neues Passwort ein.

Betrüger nutzen Sophias Daten, um auf ihr Bankkonto zuzugreifen und Geld abzuheben.

Tom und das Onlineshoppen:

Tom kauft gerne Dinge online. Er findet ein tolles Angebot für ein neues Handy auf einer bisher unbekannten Website und gibt seine Kreditkartendaten ein.

Die Website ist betrügerisch und speichert Toms Kreditkarteninformationen.

In den folgenden Wochen werden unbekannte Abbuchungen von Toms Konto vorgenommen.

Anna und die Gratis-App:

Anna lädt eine neue App herunter, die verspricht, ihre Hausaufgaben zu erledigen. Sie benötigt jedoch fragwürdige Berechtigungen, einschließlich Zugriff auf ihre Kontakte und Fotos.

Die App sammelt Annas Daten und schickt diese an Dritte.

Annas Fotos und Kontakte werden später ohne ihre Zustimmung im Internet veröffentlicht.

Michael und das WLAN:

Michael verbindet sich in einem Café mit einem offenen WLAN namens „Free Café WiFi“, um schnell seine E-Mails zu checken.

Das WLAN ist eigentlich ein „Man-in-the-Middle“-Angriff. Alles, was Michael online tut, wird von einem Betrüger überwacht.

Der Betrüger erhält Zugang zu Michaels E-Mail-Konto und verschickt Spam an alle seine Kontakte.

Julia und das Passwort:

Julia benutzt dasselbe Passwort für mehrere Onlinedienste, da es einfach zu merken ist.

Eine der Webseiten, bei denen sie registriert ist, wird gehackt und Passwörter werden geleakt.

Betrüger verwenden Julias Passwort, um auf mehrere ihrer Konten zuzugreifen, darunter auch ihr E-Mail-Konto.

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

Jannik und das Quiz:

Jannik sieht auf einem sozialen Netzwerk einen Spaßquiz mit dem Titel „Finde heraus, welcher Superheld du bist!“. Um die Fragen zu beantworten, muss er Informationen wie Geburtsdatum, die Namen seiner Haustiere und den Namen seiner Grundschule eingeben.

Das Quiz ist ein Vorwand, um Antworten auf häufige Sicherheitsfragen zu sammeln.

Betrüger nutzen die gesammelten Antworten, um das Passwort von Janniks E-Mail-Konto zurückzusetzen und Zugang zu erhalten.

8.11 Arbeitsblatt „Hacker:innen auf der Spur“

Immer wieder erbeuten Hacker:innen eine große Menge an E-Mail-Adressen, mit denen sie im schlimmsten Fall Accounts hacken können. Wenn so etwas passiert, nennt man das „Datenleck“ oder auf englisch „data leak“. Mit sogenannten Leakcheckern kann man überprüfen, ob Mailadressen bereits in solchen Datenlecks aufgetaucht sind.

Aufgabe:
Besuche den Leakchecker https://haveibeenpwned.com und teste, ob die Beispieladressen betroffen sind.

Mailadressen:
admin@linkedin.com
info@dropbox.com
test@gmail.com
info@canva.com
info@tumblr.com
info@adobe.com
jason@myspace.com
michael@myspace.com
tom@yahoo.com
max.mustermann@example.com
anna.schmidt@example.net

Tipp: Wenn man seine eigene Mailadresse testet und diese betroffen ist, sollte man danach ein besonders starkes Passwort verwenden und all seine Accounts im Auge behalten. Oder gleich die E-Mail-Adresse ändern.

8.12 Arbeitsblatt „Messenger-Contest“

In der Tabelle findet ihr eine Gegenüberstellung der drei Messenger WhatsApp, Threema und Signal nach datenschutzrelevanten Kriterien.

Kriterium	WhatsApp	Threema	Signal
Unternehmenssitz	USA (gehört zu Meta)	Schweiz	USA
Ende-zu-Ende-Verschlüsselung	Ja	Ja	Ja
Open Source	Nein	Teilweise (Client)	Ja
Datensammlung	Sammelt umfangreiche Metadaten und hat Zugriff auf Kontakte	Kein Zugriff auf Kontakte nötig; zufällige IDs statt Telefonnummern	Minimal; speichert nur, wann du dich zuletzt angemeldet hast
Werbeanzeigen	Nein, aber Daten können für Werbezwecke innerhalb des Facebook-Ökosystems genutzt werden	Nein	Nein
Serverstandort	USA und andere	Schweiz	USA und andere

Beantwortet und diskutiert folgende Fragen in der Gruppe und entscheidet euch am Ende, welchen der Messenger ihr empfehlen würdet. Begründet eure Entscheidung.

Unternehmenssitz:
Warum könnte der Standort eines Unternehmens für den Datenschutz wichtig sein?
Welche Vorteile könnte ein Sitz in der Schweiz im Vergleich zu den USA bieten?

Ende-zu-Ende-Verschlüsselung:
Erkläre in deinen eigenen Worten, was Ende-zu-Ende-Verschlüsselung ist.
Warum ist sie für einen Messenger wichtig?

Open Source:
Was bedeutet „Open Source“?
Wie kann Open Source zum Datenschutz beitragen?

Datensammlung:

Welcher dieser Messenger sammelt deiner Meinung nach die meisten Daten? Und welcher die wenigsten?
Warum ist es wichtig zu wissen, welche Daten von einem Messenger gesammelt werden?

Reflexion:
Welchen dieser Messenger würdest du basierend auf den oben genannten Kriterien empfehlen und warum?
Was sind die möglichen Risiken, wenn ein Messenger nicht datenschutzfreundlich ist?

8.13 Arbeitsblatt „Zum Wegwerfen“

Legt euch über eine der folgenden Seiten eine Wegwerf-Mailadresse an:

- www.wegwerfmail.de
- www.mistmail.de

Besucht dann die Seite www.spielaffe.de und erstellt mit der Wegwerfadresse einen Account.

Beantwortet und diskutiert danach die folgenden Fragen in der Gruppe:

- Wie habt ihr euch beim Anlegen der Mailadresse gefühlt?
- Welche Vorteile bieten Wegwerf-E-Mail-Adressen?
- Gibt es Risiken bei der Verwendung?
- Wann sollte man seine echte E-Mail-Adresse verwenden und warum?

8.14 Quiz „Schütz dein Gerät“

Lies die Fragen sorgfältig durch und beantworte sie.

1. Wofür steht „PIN“ im Kontext von Handysicherheit?
A) Persönliche Identifikationsnummer
B) Private Internetnummer
C) Persönliche Instruktionsnummer

2. Welche der folgenden Zugriffschutzmethoden basiert auf einer Zeichnung oder einem Weg, den du auf deinem Bildschirm erstellst?
A) Face-ID
B) PIN
C) Muster

3. Was ist der Hauptvorteil von Face-ID gegenüber anderen Methoden?
A) Sie ist schneller als das Eingeben einer PIN.
B) Sie basiert auf den einzigartigen Merkmalen deines Gesichts.
C) Sie benötigt keinen zusätzlichen Code.

4. Welcher der folgenden Nachteile könnte bei einem Muster als Zugriffsschutz auftreten?
A) Es kann leicht vergessen werden.
B) Fingerabdrücke auf dem Bildschirm könnten den Pfad zeigen.
C) Es kann nur von der Person erkannt werden, deren Gesicht registriert ist.

5. Warum könnten manche Personen eine PIN gegenüber Face-ID bevorzugen?
A) Weil sie keinen Code eingeben möchten.
B) Weil sie denken, dass ihr Gesicht sich im Laufe der Zeit ändern könnte.
C) Weil sie sich Sorgen um Fingerabdrücke auf ihrem Bildschirm machen.

6. Welches potenzielle Problem könnte mit Face-ID auftreten, wenn man beispielsweise eine Sonnenbrille trägt oder einen Bart wachsen lässt?
A) Die Erkennung funktioniert möglicherweise nicht richtig.
B) Das Handy wird automatisch entsperrt.
C) Es wird nach einer PIN gefragt, auch wenn Face-ID aktiviert ist.

8.15 Quiz „Schütz dich vor Viren“

Lies die Fragen sorgfältig durch und beantworte sie.

1. Welches Betriebssystem ist immun gegen Viren?
A) iOS
B) Android
C) Keines der beiden

2. Was ist ein Trojaner im Kontext von Handyviren?
A) Ein Virenscannerprogramm
B) Ein nützliches Tool, das hilft, Viren zu entfernen
C) Ein schädliches Programm, das sich als nützliche Software tarnt

3. Welche der folgenden Methoden ist KEIN guter Weg, um dein Handy vor Viren zu schützen?
A) Regelmäßige Updates des Betriebssystems
B) Das Herunterladen von Apps aus unbekannten Quellen
C) Die Verwendung einer vertrauenswürdigen Antiviren-App

4. Wenn eine App behauptet, deinen Handyakku zu optimieren und es schneller zu machen, sollte man sie immer herunterladen.
A) Wahr
B) Falsch

5. Was sollte man tun, wenn man denkt, dass eine App auf dem Handy schädlich sein könnte?
A) Ignorieren und weiterhin verwenden
B) Sofort deinstallieren und ein Virenschutzprogramm laufen lassen
C) Sie an Freund:innen weiterempfehlen

6. Virenschutz-Apps sind nur für Computer und Laptops notwendig, nicht für Handys.
A) Wahr
B) Falsch

7. Es ist sicher, auf alle Links in SMS-Nachrichten oder E-Mails zu klicken, solange sie von einem bekannten Kontakt kommen.
A) Wahr
B) Falsch

8. Wie können Viren auf dein Handy gelangen?
A) Durch das Herunterladen infizierter Apps
B) Durch das Anklicken schädlicher Links in Nachrichten oder E-Mails
C) Beides

8.16 Lösungsblatt „Schütz dein Gerät“ und „Schütz dich vor Viren“

Richtige Antworten „Schütz dein Gerät“ :

1: A, 2: C, 3: B, 4: B, 5: B, 6: A

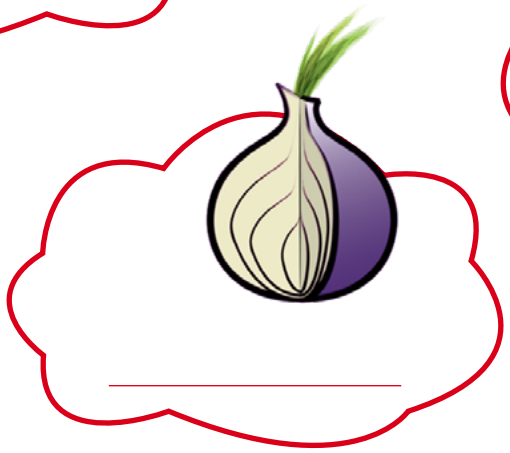
Richtige Antworten „Schütz dich vor Viren“:

1: C, 2: C, 3: B, 4: B, 5: B, 6: B, 7: B, 8: C

8.17 Arbeitsblatt „BrowseRDetektive“

Die Logos hast du bestimmt schon mal gesehen, aber kennst du die Namen der dazugehörigen Browser?

Schreibe den passenden Namen neben das Logo.



- Chrome
- Firefox
- Safari
- Edge
- Brave
- TOR

8.18 Szenarien „Doppelt hält besser“

E-Mail-Konto

Lisa hat das Passwort für ihre E-Mail auf einem Zettel in ihrem Zimmer. Ihr kleiner Bruder findet es und versucht, sich anzumelden. Was könnte Lisa helfen sicherzustellen, dass niemand außer ihr auf ihre E-Mails zugreift, selbst wenn jemand das Passwort kennt?

Onlinespiel

Max spielt ein beliebtes Onlinespiel und hat viele seltene Gegenstände gesammelt. Ein Mitspieler möchte diese Gegenstände stehlen und versucht, Max’ Passwort zu erraten. Wie könnte Max sein Konto sicherer machen, selbst wenn jemand sein Passwort erraten sollte?

Onlineshop

Sophie kauft gerne online ein. Jemand in ihrer Klasse sieht zufällig, wie sie ihr Passwort eingibt. Dieser Mitschüler möchte ohne Sophies Wissen Dinge bestellen. Was könnte Sophie tun, um sicherzustellen, dass niemand anderes Einkäufe in ihrem Namen tätigt?

Soziale Medien

Leon hat ein Profil auf einem sozialen Netzwerk. Er bekommt eine Nachricht, dass jemand versucht hat, sich von einem anderen Ort aus in sein Konto einzuloggen. Wie könnte Leon sein Profil vor solchen Zugriffsversuchen schützen?

Onlinebibliothek

Mia liebt es, Bücher aus der Onlinebibliothek ihrer Schule auszuleihen. Ihr Freund sieht zufällig ihr Passwort und denkt daran, einige Bücher auszuleihen, ohne es ihr zu sagen. Wie könnte Mia verhindern, dass jemand anders in ihrem Namen Bücher ausleiht?

9. Merkblätter

9.1 Merkblatt zur Kategorisierung von Accounts

Spaßaccounts (zum Beispiel Spiele, Foren, Fanseiten)

Risikoeinstufung: Niedrig bis mittel

Potenzielle Risiken: Verlust des Accounts, unerwünschte Nachrichten

Passwortstärke: Mittel (mindestens 8 Zeichen, Kombination aus Buchstaben und Zahlen)

Passwortablage: Passwortmanager oder analoges Passwortheft

Leak-Check: Jährlich

2FA: Empfohlen, wenn verfügbar

Passwort im Browser speichern?: Nur, wenn es sich um einen privaten Computer handelt

Social-Media-Accounts (zum Beispiel Instagram, TikTok, SnapChat)

Risikoeinstufung: Hoch

Potenzielle Risiken: Cybermobbing, Identitätsdiebstahl, Verletzung der Privatsphäre

Passwortstärke: Hoch (mindestens 12 Zeichen, Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen)

Passwortablage: Passwortmanager

Leak-Check: Halbjährlich

2FA: Dringend empfohlen

Passwort im Browser speichern?: Nein

Shopping-Accounts (zum Beispiel Amazon, ebay)

Risikoeinstufung: Hoch

Potenzielle Risiken: Finanzieller Verlust, Betrug

Passwortstärke: Hoch

Passwortablage: Passwortmanager

Leak-Check: Halbjährlich

2FA: Dringend empfohlen

Passwort im Browser speichern?: Nein

E-Mail-Accounts

Risikoeinstufung: Sehr hoch (Kontrolle über E-Mail bedeutet oft Kontrolle über viele andere Accounts)

Potenzielle Risiken: Identitätsdiebstahl, Betrug, Verlust der Privatsphäre

Passwortstärke: Sehr hoch (mindestens 16 Zeichen, Kombination aus allem)

Passwortablage: Passwortmanager

Leak-Check: Vierteljährlich

2FA: Unbedingt

Passwort im Browser speichern?: Nein

Finanz- und Banking-Accounts (zum Beispiel Onlinebanking, PayPal, Trading-Apps)

Risikoeinstufung: Sehr hoch

Potenzielle Risiken: Finanzieller Verlust, Betrug, Identitätsdiebstahl

Passwortstärke: Sehr hoch (mindestens 16 Zeichen, Kombination aus allem)

Passwortablage: Passwortmanager

Leak-Check: Vierteljährlich

2FA: Unbedingt

Passwort im Browser speichern?: Nein

Bildungs- und Arbeits-Accounts (zum Beispiel Schule, Portale)

Risikoeinstufung: Hoch

Potenzielle Risiken: Verlust von persönlichen oder beruflichen Daten, Cybermobbing

Passwortstärke: Hoch

Passwortablage: Passwortmanager

Leak-Check: Halbjährlich

2FA: Dringend empfohlen

Passwort im Browser speichern?: Nein

Cloud-Accounts (zum Beispiel Dropbox, GoogleDrive, iCloud)

Risikoeinstufung: Hoch

Potenzielle Risiken: Verlust von Daten, Verletzung der Privatsphäre

Passwortstärke: Hoch

Passwortablage: Passwortmanager

Leak-Check: Halbjährlich

2FA: Dringend empfohlen

Passwort im Browser speichern?: Nein

9.2 Merkblatt zur Organisation von Accounts und Passwörtern

Analoges Passwortheft

Einordnung: Ordne deine Accounts nach den oben genannten Kategorien ein.

Eintragung: Trage für jeden Account den Namen des Dienstes, deinen Benutzernamen und das Passwort ein.

2FA: Wenn 2FA aktiviert ist, markiere den Eintrag entsprechend. Bewahre 2FA-Wiederherstellungscodes an einem sicheren Ort auf.

Sicherheit: Bewahre das Heft an einem sicheren und geheimen Ort auf. Teile den Inhalt nicht!

Passwortmanager-App

Einrichtung: Wähle eine vertrauenswürdige Passwortmanager-App und richte sie mit einem sehr starken Hauptpasswort ein (Empfehlungen siehe unten).

Kategorisierung: Erstelle innerhalb des Managers Kategorien, wie oben beschrieben.

Eintragung: Füge für jeden Account den Namen des Dienstes, Benutzernamen und Passwort hinzu.

2FA: Viele Manager bieten auch die Möglichkeit, 2FA direkt zu integrieren. Ansonsten, wie oben, markiere und speichere die Wiederherstellungscodes sicher.

Sicherheitskopie: Mache regelmäßig Back-ups deiner Passwortdatenbank.

Generelle Tipps

- Ändere Passwörter regelmäßig.
- Verwende nie dasselbe Passwort für verschiedene wichtige Dienste.
- Sei vorsichtig bei Phishing-Versuchen – klicke nicht auf verdächtige Links und gib nie Passwörter auf unsicheren Webseiten ein.

Empfehlungen Passwortmanager-Apps

LastPass

Pro: Benutzerfreundlich, Cross-Plattform-Unterstützung, sichere Notizfunktion, digitales Erbe (Zugriff im Todesfall)

Contra: Kostenlos-Version hat Einschränkungen, in der Vergangenheit gab es Sicherheitsbedenken (wurden aber behoben)

1Password

Pro: Starke Sicherheitsfunktionen, Travel Mode (schützt Daten während Grenzkontrollen), lokale Datenspeicheroption

Contra: Keine permanente kostenlose Version, benötigt gelegentlich manuelle Synchronisation zwischen Geräten

Bitwarden

Pro: Open Source (der Code kann öffentlich überprüft werden), voll funktionsfähige Kostenlos-Version, Self-Hosting möglich

Contra: Interface ist weniger poliert als bei Konkurrenten, einige erweiterte Funktionen können technisches Wissen erfordern

Alle Passwortmanager bieten starke Verschlüsselung und haben sich im Laufe der Zeit als sicher erwiesen. Die Wahl hängt oft von persönlichen Vorlieben und spezifischen Anforderungen ab. Es ist immer ratsam, regelmäßig nach Updates und Sicherheitsberichten über die gewählte Software zu suchen.

Verbraucherzentrale
Rheinland-Pfalz

Impressum

Herausgebeben von:
Verbraucherzentrale Rheinland-Pfalz e.V.
Seppel-Glückert-Passage 10, 55116 Mainz
T +49 6131 28480
F +49 6131 284866
info@vz-rlp.de
verbraucherzentrale-rlp.de

Für den Inhalt verantwortlich:
Heike Troue, Vorständin der Verbraucherzentrale Rheinland-Pfalz e.V.

Redaktion und Text:
Max Heitkämper, Ruth Preywisch, Jeanine Wein, Verbraucherzentrale Rheinland-Pfalz e. V.

Gestaltung:
alles mit Medien

Lektorat:
WORDS IN FLOW

Bildnachweise:
Titel – iStock.com/Mladen Zivkovic

Stand:
01/2026

Gedruckt auf 100 % Recyclingpapier.

RheinlandPfalz
MINISTERIUM FÜR FAMILIE, FRAUEN, KULTUR UND INTEGRATION