IT-Sicherheit für Senioren

Ein umfassender Leitfaden für einen sicheren digitalen Alltag

IT-Sicherheit für Senioren

Ein umfassender Leitfaden für einen sicheren digitalen Alltag

Vorwort

Liebe Leserinnen und Leser, die digitale Welt eröffnet uns viele neue Chancen – doch sie bringt auch Herausforderungen mit sich. Mit dieser Broschüre möchte ich Ihnen Mut machen, diese Welt sicher und selbstbewusst zu entdecken. IT-Sicherheit muss kein Hindernis sein, sondern kann ein Schlüssel zu mehr Freiheit und Lebensqualität werden.

Als Bürger unserer schönen Gemeinde Eching ist es mir ein persönliches Anliegen, Sie auf diesem Weg zu unterstützen. Vertrauen Sie auf sich, bleiben Sie neugierig – und lassen Sie sich die Möglichkeiten der digitalen Welt nicht entgehen!

Falls Sie den Verdacht haben, dass jemand Ihre Daten missbraucht oder Sie Opfer eines Betrugs geworden sind, heißt es: keine Panik – aber schnell handeln! Wir haben für Sie eine unkomplizierte Schritt-für-Schritt-Anleitung zusammengestellt, die Ihnen in dieser Situation weiterhilft – klar, verständlich und direkt umsetzbar.

Herzliche Grüße und viel Erfolg auf Ihrer digitalen Reise!

Martin W. Steinbach
Eching / Weixerau

Gemeinde Eching

Verantwortlich für den Inhalt und redaktionelle Bearbeitung

Jessica Stauber
Quartiersmanagement
Hauptstraße 12
84174 Eching

Telefon 08709 9247-35
Fax 08709 9247-28
Web www.eching-ndb.de
Mail: gemeinde@eching-ndb.de
Ansprechpartner: jessica.stauber@eching-ndb.de

Verantwortlich für den Inhalt
Martin W. Steinbach
Eching / Weixerau
Telefon 0176 2215 3430
Mail: martinwsteinbach@gmail.com

Willkommen zu Ihrer Reise in die sichere digitale Welt!

Ob Computer, Tablet oder Smartphone – digitale Geräte sind aus unserem Alltag kaum mehr wegzudenken. Sie ermöglichen uns den Kontakt zu Familie und Freunden, erleichtern Bankgeschäfte, bieten Zugang zu Informationen und Unterhaltung. Doch mit den vielen Möglichkeiten wachsen auch die Risiken: **Betrüger** versuchen, persönliche Daten zu stehlen, geben sich als Verwandte aus oder locken mit falschen Versprechungen. Besonders ältere Menschen werden dabei gezielt ins Visier genommen.

Diese Broschüre wurde speziell für **Seniorinnen** und **Senioren** entwickelt und gibt Ihnen einen verständlichen Überblick über die wichtigsten Themen der IT-Sicherheit. Sie lernen nicht nur, wie Sie sich am Computer und im Internet schützen, sondern auch, wie Sie sicher mit dem Smartphone umgehen, betrügerische Anrufe und WhatsApp-Nachrichten erkennen und darauf reagieren.

Sie begleitet Sie Schritt für Schritt durch wichtige Themen der digitalen Sicherheit. Sie lernen zum Beispiel, wie Sie eine sichere Internetverbindung erkennen, worauf Sie bei Passwörtern achten sollten und wie Sie sich vor Betrugsmaschen wie Phishing, falschen Anrufen oder dem Enkeltrick schützen können – am Telefon und im Internet. Auch die sichere Nutzung von sozialen Netzwerken, Apps und Geräten kommt nicht zu kurz.

Zudem geben wir Ihnen praktische Ratschläge, wie Sie im Notfall richtig reagieren, hilfreiche Einstellungen vornehmen und Ihre Geräte absichern können. Fallbeispiele, eine Sicherheits-Checkliste und wichtige Kontaktstellen runden das Angebot ab.

Unser Ziel ist es, Ihnen mehr Sicherheit, Orientierung und Vertrauen im digitalen Alltag zu geben – ganz ohne Fachchinesisch, dafür mit viel Praxisnähe und klaren Erklärungen.

Sie brauchen keine technischen Vorkenntnisse – nur ein bisschen Neugier und die Bereitschaft, Neues zu lernen. Unser Ziel ist es, Ihnen Sicherheit und Selbstvertrauen im Umgang mit moderner Technik zu geben. Denn mit dem richtigen Wissen lassen sich viele Gefahren leicht vermeiden.

Lassen Sie uns gemeinsam einen Blick auf die digitale Welt werfen – sicher, informiert und mit einem guten Gefühl. Wir wünschen Ihnen viel Freude beim Lesen und Ausprobieren!

Inhalt

1. Was bedeutet IT-Sicherheit – und warum ist sie wichtig für mich? 8

1.1. Beispiele aus dem Alltag: 8

1.2. Warum ist IT-Sicherheit also wichtig? 8

1.3. Quellen & Empfehlungen: 8

2. Passwortsicherheit 9

3. Was bedeutet Passwortsicherheit? 9

3.1. Warum sollte gerade ich ein sicheres Passwort brauchen? 10

3.2. Wie erstelle ich sichere und leicht merkbare Passwörter? 10

3.3. Gefahren schwacher Passwörter 11

3.4. Beispiele für unsichere Passwörter 11

3.5. So machen Sie Ihr Passwort sicher: 11

3.6. Wie sicher ist Ihr Passwort? Eine Einschätzung 12

3.7. So machen Sie Ihr Passwort sicher: Techniken und Tipps 12

3.8. Sichere Passwörter 13

3.9. Beispiel für ein sehr sicheres Passwort 13

3.10. Passwort-Manager 14

3.11. Zusammenfassung und wichtigste Punkte 15

4. Was ist Zwei-Faktor-Authentifizierung und warum schützt sie mich? 16

4.1. Wie funktioniert Zwei-Faktor-Authentifizierung (2FA)? 16

4.2. Beispiele für gute Authenticator 18

4.3. Warum ist Zwei-Faktor-Authentifizierung wichtig? 20

4.4. Übersicht beliebter Konten mit TOTP 20

5. Sicherheitsmaßnahmen für mobile Geräte 22

5.1. Warum ist Sicherheit auf dem Smartphone wichtig? 22

5.2. Sichere Apps – darauf sollten Sie achten 22

5.3. Wie erkenne ich vertrauenswürdige Apps 22

5.4. Entsperr-Methoden – Ihr Handy vor fremdem Zugriff schützen 25

5.5. Anzahl möglicher gültiger Muster 25

5.6. Sicherheit von Entsperr-Codes 26

5.7. Wichtige Schutzmaßnahmen für Ihr Gerät 27

6. Wie kann ich sicher im Internet einkaufen? 28

6.1. Wie erkenne ich eine sichere Internetverbindung? 28

6.2. Häufige Bedrohungen und Betrugsarten 31

6.3. Unterschiedliche Arten von Bedrohungen 32

6.4. Achtung bei Shops außerhalb der EU 32

6.5. So erkennen Sie unseriöse oder gefälschte Internet-Shops 33

6.6. So erkennen Sie einen Fake-Shop 33

6.7. Verwendung von vertrauenswürdige Websites 34

6.8. Verwenden von sichere Zahlungsmethoden 34

6.9. Sichere Online-Shops und vertrauenswürdiges Einkaufen 34

6.10. Achten auf Sicherheitszeichen 36

7. Wie bezahle ich sicher mit PayPal oder anderen Online-Diensten? 38

7.1. Verwendung vertrauenswürdiger Online-Zahlungsdienste 38

7.2. Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA) 38

7.3. Nutzen Sie eine sichere Internetverbindung 39

7.4. Achten Sie auf die Adresse der Webseite (URL) 39

7.5. Zahlen Sie nur bei vertrauenswürdigen Händlern 39

7.6. Achten Sie auf die Sicherheit Ihrer PayPal- oder Kontoinformationen 39

7.7. Nutzen Sie die Käuferschutzfunktionen 39

7.8. Behalten Sie Ihre Kontobewegungen im Auge 40

7.9. Vermeiden Sie das Speichern von Zahlungsinformationen 40

8. Bekannte Betrugsmethoden und Maßnahmen 41

8.1. Woran erkenne ich eine Phishing-E-Mail? 41

8.2. Dringender Handlungsbedarf oder Drohungen 41

8.3. Ungewöhnliche Absenderadresse 41

8.4. Links, die zu gefälschten Webseiten führen 41

8.5. Grammatik- und Rechtschreibfehler 41

8.6. Unpersönliche Anrede 41

8.7. Aufforderung zur Eingabe sensibler Daten 42

8.8. Wie reagiere ich richtig auf verdächtige E-Mails und Nachrichten? 43

8.9. Was steckt hinter betrügerischen Anrufen? 45

8.10. Wie funktioniert der Enkeltrick – am Telefon und über WhatsApp? 47

8.11. Fallbeispiel: Ein betrügerischer Anruf 49

8.12. Welche Warnzeichen deuten auf Betrug oder Datendiebstahl hin? 50

8.13. Was sollte ich beim Umgang mit sozialen Netzwerken beachten? 53

9. Einstellungen auf den Geräten 58

9.1. Welche Einstellungen auf den Geräten erhöhen die Sicherheit 58

9.2. Wie schütze ich…? 59

9.3. Sicherheits-Checkliste: Bin ich gut geschützt? 61

9.4. Was tun im Notfall? – Erste Hilfe bei Betrugsverdacht 62

10. Nützliche Links, Telefonnummern und weitere Hilfsangebote 65

11. Sichern und Wiederherstellen mit Smartphones 67

11.1. Was bedeutet Datensicherung (Backup) und warum ist sie wichtig 67

11.2. Fotos und Videos sicher speichern und wiederherstellen 68

11.3. Kontakte, Kalender und Nachrichten zuverlässig sichern 71

11.4. Kalenderdaten sichern: Automatische Synchronisierung und Wiederherstellung 71

11.5. Chats sichern WhatsApp &Co 72

11.6. Datensicherung bei Telegram 73

11.7. Das gesamte Smartphone sichern und wiederherstellen 73

12. Digitaler Daten-Nachlass 77

12.1. Online Bezahldienste 78

12.2. Sozialer Netzwerke im digitalen Nachlass 84

12.3. Strategien für den verantwortungsvollen Umgang mit dem digitalen Nachlass 98

13. Was ist Linux – eine sichere, kostenlose Alternative für Ihren PC 100

14. Zusammenfassung 103

15. Schlusswort 105

16. Stichwort-Verzeichnis 106

17. Abbildungsverzeichnis 109

1. Was bedeutet IT-Sicherheit – und warum ist sie wichtig für mich?

IT-Sicherheit – oder ausgeschrieben Informations- und Telekommunikationssicherheit – beschreibt alle Maßnahmen, die dazu dienen, unsere Geräte (wie Computer, Smartphones oder Tablets) und unsere persönlichen Daten vor unerlaubtem Zugriff, Missbrauch, Betrug oder Verlust zu schützen.

Im Alltag bedeutet das konkret: Wenn Sie z. B. mit Ihrem Smartphone Fotos verschicken, E-Mails lesen, Online-Banking nutzen oder bei Amazon einkaufen, hinterlassen Sie digitale Spuren. Diese Spuren können von Kriminellen ausgenutzt werden – etwa durch sogenanntes Phishing-E-Mails, falsche Anrufe, unsichere WLAN-Verbindungen oder schadhafte Apps.

Gerade ältere Menschen sind häufiges Ziel solcher Betrugsmaschen, da sie oft weniger technische Erfahrung haben oder im Umgang mit neuen Medien unsicher sind. Laut einer Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI, 2023) wurden in Deutschland allein im vergangenen Jahr mehrere tausend Fälle gemeldet, bei denen Senioren durch betrügerische E-Mails oder Anrufe um Geld betrogen wurden.

1.1. Beispiele aus dem Alltag:

- **Beispiel 1:** Sie bekommen eine E-Mail von Ihrer „Bank“, die Sie auffordert, Ihre Zugangsdaten einzugeben. Die Seite sieht echt aus – ist aber gefälscht. Wer hier seine Daten eingibt, verliert im schlimmsten Fall Geld vom Konto.
- **Beispiel 2:** Ein Anruf vom angeblichen „Enkel“, der sich in einer Notlage befindet und dringend Geld braucht. Dahinter steckt oft der sogenannte Enkeltrick, der über Telefon oder inzwischen auch über WhatsApp läuft.
- **Beispiel 3:** Sie installieren eine App, die vorgibt, ein Spiel zu sein – in Wirklichkeit aber heimlich Ihre Kontakte oder Passwörter ausliest.

1.2. Warum ist IT-Sicherheit also wichtig?

- Sie schützt Ihre Daten und Ihre Privatsphäre.
- Sie verhindert, dass Ihr Geld in falsche Hände gerät.
- Sie gibt Ihnen das gute Gefühl, sich sicher und selbstbestimmt in der digitalen Welt zu bewegen.

IT-Sicherheit ist keine Frage des Alters, sondern des Wissens. Und dieses Wissen möchten wir Ihnen mit dieser Broschüre an die Hand geben – Schritt für Schritt, leicht verständlich und praxisnah.

1.3. Quellen & Empfehlungen:

Bundesamt für Sicherheit in der Informationstechnik (BSI)	www.bsi-fuer-buerger.de
Polizeiliche Kriminalprävention	www.polizei-beratung.de
Verbraucherzentrale	www.verbraucherzentrale.de

2. Passwortsicherheit

das Thema **Passwortsicherheit** klingt auf den ersten Blick nach einem rein technischen Begriff, der vielleicht eher in die Welt der Computerexperten gehört. In Wahrheit betrifft es jedoch jeden Menschen, der heutzutage ein Smartphone, einen Computer oder das Internet nutzt – ganz gleich, wie oft oder wofür. **Passwortsicherheit bedeutet nichts anderes, als Ihre persönlichen Daten zu schützen**: Fotos, Nachrichten, Online-Banking, Einkäufe im Internet oder auch Ihre Gesundheitsdaten – all das liegt hinter Passwörtern. Sie sind der Schlüssel zu Ihrer privaten digitalen Welt.

Man kann es sich bildlich so vorstellen: **Ein Passwort ist wie der Haustürschlüssel** – je stabiler und sicherer dieser ist, desto besser schützt er Ihr Zuhause vor ungebetenen Gästen. Unsichere Passwörter hingegen sind wie eine unverschlossene Tür: Wer hineinwill, hat leichtes Spiel. Gerade im Internet gibt es leider Menschen, die gezielt versuchen, fremde Konten zu übernehmen, Geld zu erbeuten oder Identitäten zu stehlen. Deshalb ist es wichtig zu wissen, **wie man sichere Passwörter erstellt und wie man sie richtig verwaltet**, ohne sich dabei zu überfordern.

In diesem Kapitel erfahren Sie leicht verständlich und Schritt für Schritt, wie Sie Ihre digitalen Zugänge schützen – **ohne komplizierte Fachbegriffe und ohne Stress**. Ziel ist nicht, Ihnen Angst zu machen, sondern Ihnen **Sicherheit und Selbstvertrauen** im Umgang mit Passwörtern zu geben. Denn digitale Sicherheit ist kein Glück – sie ist Wissen.

3.Was bedeutet Passwortsicherheit?

Verwenden Sie ein sicheres, einzigartiges Passwort für jedes Ihrer Konten. Es sollte eine Kombination aus Buchstaben, Zahlen und Sonderzeichen sein.

Antivirus und Antimalware: Halten Sie Ihre Sicherheitssoftware stets auf dem neuesten Stand, um sich vor schädlicher Software zu schützen, die beim Online-Einkauf gefährlich werden könnte.

Seien Sie vorsichtig mit persönlichen Daten

Minimiere der Weitergabe persönlicher Informationen: Geben Sie nur die notwendigen Informationen an, die für den Einkauf erforderlich sind (z.B. Name, Adresse, E-Mail). Verzichten Sie darauf, zusätzliche Daten preiszugeben.

Phishing-Angriffe vermeiden: Seien Sie vorsichtig bei E-Mails oder Nachrichten, die Sie auffordern, auf Links zu klicken oder persönliche Daten einzugeben. Seriöse Anbieter fragen niemals per E-Mail nach sensiblen Daten.

Überprüfen Sie den Online-Shop regelmäßig

Prüfen Sie Bewertungen und Rezensionen: Sie können Ihnen helfen, die Qualität der Ware und die Zuverlässigkeit des Verkäufers zu bewerten.

Suchen Sie nach Erfahrungen von anderen Käufern: Lesen Sie Erfahrungsberichte auf unabhängigen Seiten oder in Foren.

Behalten Sie Bestellungen im Auge

Bestellbestätigung aufbewahren: Bewahren Sie alle Bestellbestätigungen und Rechnungen auf, um im Fall von Problemen mit der Lieferung oder Rückerstattungen einen Nachweis zu haben.

Verfolgen Sie Lieferungen: Nutzen Sie die Sendungsverfolgungen, um sicherzustellen, dass Ihre Bestellung angekommen ist und keine Probleme bei der Lieferung auftreten.

Indem Sie diese Maßnahmen befolgen, können Sie sicherer und unbesorgter im Internet einkaufen.

3.1. Warum sollte gerade ich ein sicheres Passwort brauchen?

Viele Menschen glauben, dass vor allem staatliche Stellen oder große Firmen versuchen, an ihre Daten zu kommen. Das stimmt nur zum Teil. In Wirklichkeit haben es Kriminelle meistens auf normale Menschen abgesehen, so wie Sie und mich. Hacker zielen dabei nicht auf einzelne Privatpersonen ab; stattdessen arbeiten sie nach dem „Gießkannen-Prinzip" und setzen automatisierte Methoden ein, um Hunderttausende von Nutzern gleichzeitig zu erreichen.

Warum? Weil privat sehr viel über Computer, Tablet und Handy gemacht wird:

- Man schreibt E-Mails und Nachrichten
- Man verwendet Online-Banking
- Man kauft im Internet ein
- Man speichert Fotos, persönliche Dokumente oder Passwörter
- Man nutzt soziale Netzwerke wie Facebook oder WhatsApp

IT-Sicherheit bedeutet, sich vor Betrug, Datenklau und Schadprogrammen zu schützen. Es geht darum, zu verhindern, dass jemand:

- … auf Ihr Bankkonto zugreift,
- … Ihre Identität stiehlt (z. B. Konto in Ihrem Namen eröffnet),
- … Ihr Gerät sperrt und Geld fordert (Erpressung mit sogenannter „Ransomware"),
- … private Daten ausspioniert,
- … oder Sie mit falschen Nachrichten und Anrufen täuscht (z. B. „Enkeltrick", WhatsApp-Betrug oder falsche Polizisten).

Viele Angriffe sind leicht zu verhindern, wenn man ein paar Grundregeln kennt. Genau darum geht es in diesem Kurs: Wir wollen gemeinsam lernen, wie man sich im Internet sicher bewegt, Betrug erkennt und seine Geräte schützt, ohne Angst haben zu müssen.

3.2. Wie erstelle ich sichere und leicht merkbare Passwörter?

Passwörter sind die **Schlüssel** zu Ihren wichtigsten digitalen Türen im Internet: E-Mail-Postfächer, Online-Shops, Bankkonten oder soziale Netzwerke. Je **besser** und komplexer Ihr Passwort ist, desto **schwieriger** wird es für Betrüger, Zugriff auf Ihre Daten zu bekommen.

Doch viele Menschen verwenden **zu einfache Passwörter** – oft, weil sie sich komplizierte Varianten nicht merken können. Genau das nutzen Kriminelle aus.

Ein echtes Fallbeispiel:

Frau Müller, 73 Jahre alt, nutzte für alle ihre Konten das Passwort **„123456"**. Eines Tages erhielt sie eine Nachricht: Jemand hatte versucht, sich in ihr E-Mail-Konto einzuloggen. Der Grund: Ihr Passwort war **sehr einfach** – und wurde von Betrügern **in wenigen Sekunden** geknackt. Über ihre E-Mail konnten die Angreifer dann versuchen, auch andere Dienste (z. B. Online-Shops) zu übernehmen.

Wie sicher ist Ihr Passwort?

Hier eine Übersicht, wie schnell moderne Computer einfache Passwörter knacken können:

Passwort	Knackdauer	Anmerkung
123456	Weniger als **1 Sekunde**	Sehr unsicher; niemals verwenden
passwort	Weniger als **1 Sekunde**	Sehr unsicher; leicht erraten
mariasommer	Weniger als **1 Sekunde**	Namen + Begriffe sind unsicher
M@r!a2024	Einige **Stunden**	Mittelmäßig sicher
!T7pRk#9qF2	**Jahrhunderte**	Sehr sicher (zufällige Zeichen)

(Quelle: Statista 2024 / BSI)

3.3. Gefahren schwacher Passwörter

Risiken schwacher Passwörter Schwache Passwörter sind anfällig für Angriffe und können leicht erraten werden, was ein hohes Risiko darstellt.

„Brute-Force" Angriffe Cyberkriminelle verwenden Brute-Force-Angriffe, um Passwörter zu knacken und unbefugten Zugriff auf Konten zu erhalten.

Komplexe und einzigartige Passwörter Es ist entscheidend, komplexe und einzigartige Passwörter zu verwenden, um die Sicherheit von Konten zu gewährleisten.

3.4. Beispiele für unsichere Passwörter

Häufige unsichere Passwörter

Häufig genutzte, unsichere Passwörter (bitte vermeiden!)

🚫 „**123456**" 🚫 „**passwort**" 🚫 „**qwertz**" 🚫 „**Sommer2024**" 🚫 „**MeinName**"

🚫 „**Geburtsdatum**"

Quelle: NordPass Top 200 Most Common Passwords 2023https://nordpass.com/most-common-passwords-list/

Erforderliche Passwortstärke

Ein starkes Passwort sollte eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Dies erhöht die Sicherheit.

3.5. So machen Sie Ihr Passwort sicher:

- **Mindestens 12 Zeichen**
- **Groß- und Kleinbuchstaben**, **Zahlen** und **Sonderzeichen** verwenden
- Keine **Namen**, **Geburtstage** oder **einfache Wörter**
- Für **jeden Dienst ein eigenes Passwort**

💡 **Tipp: Merksätze statt schwerer Passwörter**

Kombination aus Wörtern

Ein sicheres Passwort kann durch die Kombination von zwei oder mehr nicht verwandten Wörtern erstellt werden, um die Sicherheit zu erhöhen.

"ZebraKaffee"

Zahlen und Symbole hinzufügen

Das Hinzufügen von Zahlen und Symbolen zu einem Passwort erhöht die Komplexität und macht es schwieriger zu knacken.

"Wald!Fisch_87"

3.6. Wie sicher ist Ihr Passwort? Eine Einschätzung

Sicherheitsüberprüfung

Es gibt viele Tools, die helfen, die Sicherheit von Passwörtern zu überprüfen und Schwachstellen zu identifizieren.

Link: sec.hpi.uni-potsdam.de/leak-checker/search

Link: https://leakchecker.uni-bonn.de/

Link: haveibeenpwned.com

3.7. So machen Sie Ihr Passwort sicher: Techniken und Tipps

Verwendung von Passphrasen

Eine Passphrase ist ein langes, sicheres Passwort aus mehreren Wörtern. Sie ist leichter zu merken als ein kompliziertes Passwort und schützt viel besser vor Hackerangriffen. Passphrasen sind länger und komplexer, was die Sicherheit erhöht und es Hackern erschwert, sie zu knacken.

Kombination von Zeichen

Die Kombination von Buchstaben, Zahlen und Symbolen macht Passwörter schwieriger zu erraten und erhöht die Sicherheit.

Regelmäßige Passwortänderung

Regelmäßiges Ändern von Passwörtern minimiert das Risiko eines Angriffs und schützt persönliche Informationen.

In der nachstehenden Tabelle können Sie erkennen, wie lange Hacker benötigen, um Ihre Password zu knacken. Dabei wird ein Hochleistungscomputer vorausgesetzt.

Wie lange brauchen Hacker, um Ihr Password zu hacken?				
Anzahl Zeichen	**Nur Kleinbuchstaben**	**Mindestens 1 Großbuchstabe**	**mindestens 1 Großbuchstabe + Zahl**	**mindestens 1 Großbuchstabe + Zahl + Sonderzeichen**
1	Sofort	Sofort	-	-
2	Sofort	Sofort	Sofort	-
3	Sofort	Sofort	Sofort	Sofort
4	Sofort	Sofort	Sofort	Sofort
5	Sofort	Sofort	Sofort	Sofort
6	Sofort	Sofort	Sofort	Sofort
7	Sofort	Sofort	1 Minute	6 Minuten
8	Sofort	22 Minuten	1 Stunde	8 Stunden
9	2 Minuten	19 Stunden	3 Tage	3 Wochen
10	1 Stunde	1 Monat	7 Monate	5 Jahre
11	1 Tag	5 Jahre	41 Jahre	400 Jahre
12	3 Wochen	300 Jahre	2.000 Jahre	34.000 Jahre
13	1 Jahr	16.000 Jahre	100.000 Jahre	2 Millionen Jahre
14	51 Jahre	800.000 Jahre	9 Millionen Jahre	200 Millionen Jahre
15	1.000 Jahre	43 Million Jahre	600 Millionen Jahre	15 Milliarden Jahre
16	34.000 Jahre	2 Milliarden Jahre	37 Milliarden Jahre	1 Billiarde Jahre

3.8. Sichere Passwörter

So machen Sie Ihr Passwort sicher:

- Mindestens 12 Zeichen
- Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen verwenden
- Keine Namen, Geburtstage oder einfache Wörter
- Idealerweise für jeden Dienst ein eigenes Passwort

3.9. Beispiel für ein sehr sicheres Passwort

Sehr gutes Passwort:

IJ1973fid1MnP!

Ein Trick für sichere **UND** merkbare Passwörter ist die **Eselsbrücke**:

Merksatz: **I**m **J**ahr **1973** **f**uhr **i**ch **d**as **e**rste **M**al **n**ach **P**aris**!**

Passwort: **I J 1 9 7 3 f i d 1 M n P !**

14 Zeichen

3.10. Passwort-Manager

Verwenden: Vor- und Nachteile

- **Sichere Passwortspeicherung**
  - Passwort-Manager bieten eine sichere Möglichkeit, Passwörter zu speichern und zu verwalten, sodass Benutzer sich keine Sorgen um Vergessen machen müssen.
- **Starke Passwortgenerierung**
  - Diese Tools generieren starke, komplexe Passwörter, die schwer zu knacken sind, und verbessern somit die Sicherheit der Benutzerkonten.
- **Vor- und Nachteile abwägen**
  - Benutzer sollten die Vor- und Nachteile eines Passwort-Managers abwägen, um sicherzustellen, dass es ihren Sicherheitsbedürfnissen entspricht.

Einfache Passwort-Manager

☑ **Bitwarden (https://bitwarden.com/)**

- Kostenlos & einfach
- Sehr übersichtlich, auch auf dem Smartphone.
- Deutsch verfügbar.
- Passwörter automatisch einfügen.
- Empfehlung: Ideal für Einsteiger

☑ **1Password (https://1password.com/)**

- Kostenpflichtig, aber sehr benutzerfreundlich
- Deutsch verfügbar.
- Klares, großes Design, leicht zu bedienen.
- Funktioniert auf PC und Handy.

☑ **NordPass (https://nordpass.com/)**

- Kostenlos & einfach
- Klar strukturiert
- Deutsch verfügbar.

- Einfache Oberfläche funktioniert auf allen Geräten.
- Ideal bei Nutzung von NordVPN

3.11. Zusammenfassung und wichtigste Punkte

Bedeutung sicherer Passwörter

Sichere Passwörter sind der erste Schritt zur Gewährleistung der Internet-Sicherheit und zum Schutz persönlicher Daten.

Starke und einzigartige Passwörter

Benutzer sollten Passwörter erstellen, die stark und einzigartig sind, um das Risiko von Hackerangriffen zu minimieren.

Nutzung von Passwort-Managern

Die Verwendung von Passwort-Managern kann die Passwortsicherheit erhöhen und das Verwalten verschiedener Passwörter erleichtern.

Verlassen Sie sich nicht auf Standard-Passwörter – Ihre Sicherheit liegt in Ihren Händen!

Quellen:

- *Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/DE/Service-Navi/Medien/Publikationen/Broschueren/Passwoerter*
- *Statista 2024: Durchschnittliche Knackdauer von Passwörtern https://de.statista.com/*
- *Verbraucherzentrale: Tipps für sichere Passwörter https://www.verbraucherzentrale.de*

4. Was ist Zwei-Faktor-Authentifizierung und warum schützt sie mich?

Die Zwei-Faktor-Authentifizierung (2FA) ist eine Sicherheitsmaßnahme, die sicherstellt, dass nur Sie auf ein Konto zugreifen können, auch wenn jemand Ihr Passwort kennt. Dabei werden zwei verschiedene Faktoren verwendet, um Ihre Identität zu verifizieren:

- Etwas, das nur Sie wissen (z.B. Ihr Passwort)
- Etwas, das nur Sie besitzen (z.B. ein Handy, ein Sicherheitstoken oder eine App zur Generierung eines Codes)

Durch diese doppelte Sicherheitsprüfung wird es für Angreifer deutlich schwieriger, in Ihr Konto einzudringen, selbst wenn sie Ihr Passwort kennen.

4.1. Wie funktioniert Zwei-Faktor-Authentifizierung (2FA)?

Beispiel 1: Login mit Passwort + SMS-Code

Stellen Sie sich vor, Sie möchten Sich in einem Online-Shop oder einem sozialen Netzwerk anmelden. Sie geben zuerst Ihr Passwort ein – das ist der erste Faktor: etwas, das nur Sie wissen.

Nun erhalten Sie auf Ihrem Mobiltelefon eine SMS mit einem einmaligen Code, den Sie eingeben müssen, um den Anmeldevorgang abzuschließen. Dieser Code ist der zweite Faktor: etwas, das nur Sie besitzen (Ihr Handy).

Erster Faktor: Passwort

Zweiter Faktor: Ein Code, der dir per SMS geschickt wird

Warum schützt Sie das? Wenn ein Angreifer Ihr Passwort gestohlen hat, kann er sich ohne den zweiten Faktor (den Code auf Ihrem Handy) nicht einloggen. Selbst mit Ihrem Passwort bleibt der Zugriff blockiert.

Hinweis 1 Zwei Faktor

Hinweis 2 SMS-Code

Beispiel 2: Login mit Passwort + Authentifizierungs-App

Ein weiteres Beispiel ist die Verwendung einer Authenticator-App wie Google Authenticator oder Authy. Sie geben wieder Ihr Passwort ein, aber anstatt eines Codes per SMS zu erhalten, öffnen Sie die Authentifizierungs-App auf Ihrem Handy. Diese App erzeugt alle 30 Sekunden einen neuen Code, den Sie eingeben müssen, um sich anzumelden.

- Erster Faktor: Passwort
- Zweiter Faktor: Ein Code aus der Authentifizierungs-App

Warum schützt Sie das? Ein Angreifer müsste nicht nur Ihr Passwort kennen, sondern auch Zugang zu Ihrem Handy **und** der Authentifizierungs-App haben, um den Code zu erhalten. Das macht den Zugriff viel schwieriger.

Hinweis 3 2FA-2Wege

4.2. Beispiele für gute Authenticator

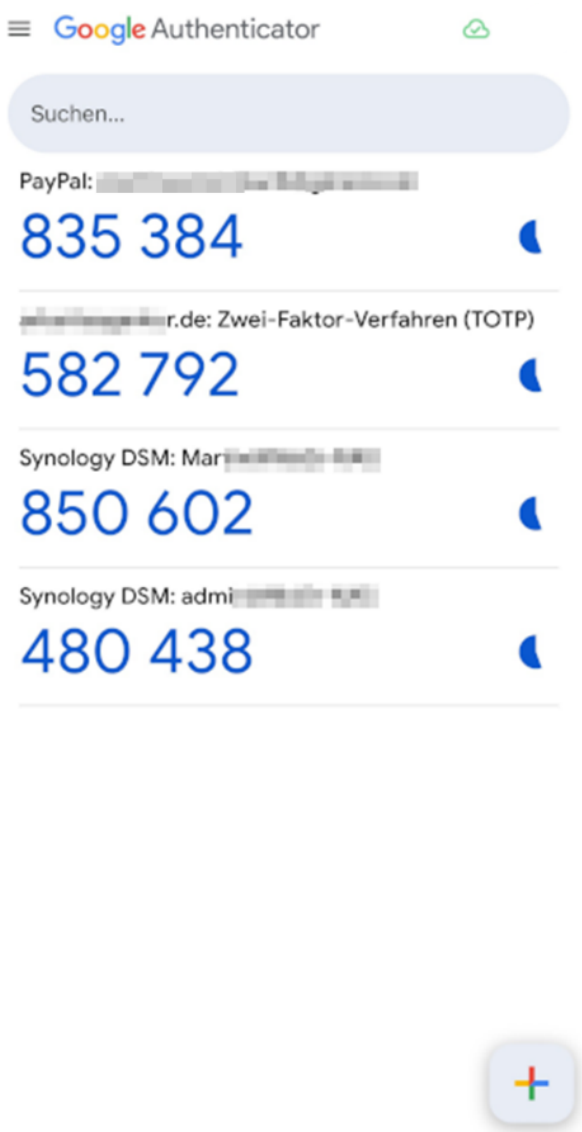
Beispiel 1: Google Authenticator

- **Funktion:** Generiert zeitbasierte Einmalpasswörter (TOTP), die alle 30 Sekunden wechseln.
- **Offline nutzbar**, keine Internetverbindung notwendig.
- **Plattformen**: Android, iOS
- **Einsatz:** Weit verbreitet bei Google-Diensten, AWS, Dropbox u. v. m.

Beispiel 2: Microsoft Authenticator

- **Funktion**: Unterstützt neben TOTP auch Push-Benachrichtigungen zur Freigabe per Klick.
- **Plattformen**: Android, iOS
- **Offline nutzbar**, keine Internetverbindung notwendig.
- **Einsatz**: Ideal in Office-365-/Microsoft-Umgebungen, auch mit Multi-Konto-Verwaltung.

Beispiel Google Authenticator:



Hinweis 4 Google Authenticator

Beispiel 3: Login mit Passwort + Biometrische Daten (Fingerabdruck oder Gesichtserkennung)

Ein weiteres Beispiel für die Zwei-Faktor-Authentifizierung ist die Verwendung von biometrischen Daten, wie einem Fingerabdruck oder der Gesichtserkennung auf einem Smartphone. Hierbei geben Sie zuerst Ihr Passwort ein (der erste Faktor) und müssen dann einen Fingerabdruck scannen oder Ihr Gesicht vor die Kamera halten (der zweite Faktor).

- Erster Faktor: Passwort
- Zweiter Faktor: Biometrische Daten (Fingerabdruck oder Gesichtserkennung)

Warum schützt Sie das? Ein Angreifer müsste nicht nur Ihr Passwort kennen, sondern auch in der Lage sein, Ihren Fingerabdruck zu scannen oder Sie zu „entblocken", was außerordentlich schwierig ist. Dies bietet eine zusätzliche Sicherheitsstufe.

Laut psychologischen und medienwissenschaftlichen Studien beginnt der durchschnittliche Mensch das **Fehlen des Smartphones nach etwa 10 bis 20 Minuten** bewusst wahrzunehmen – je nach Alter, Nutzungsmuster und Situation.

4.3. Warum ist Zwei-Faktor-Authentifizierung wichtig?

Schutz vor Passwortdiebstahl: Wenn ein Angreifer Ihr Passwort stiehlt (z.B. durch Phishing oder durch den Kauf von Daten aus einem Datenleck), benötigt er trotzdem den zweiten Faktor, um auf Ihr Konto zuzugreifen. Ohne diesen zweiten Faktor bleibt der Zugang verweigert.

Schutz bei unsicheren Passwörtern: Auch wenn Sie ein schwaches oder wiederverwendetes Passwort haben, schützt die Zwei-Faktor-Authentifizierung Ihr Konto. Ein Angreifer kann Ihr Passwort kennen, aber ohne den zweiten Faktor kommt er nicht weiter.

Verhinderung von unbefugtem Zugriff: Selbst, wenn jemand Zugriff auf Ihr Gerät hat oder Ihre Login-Daten kennt, sind sie ohne den zweiten Faktor nicht in der Lage, dein Konto zu benutzen. Das schützt Sie, falls Ihr Gerät gestohlen wird oder Sie Ihre Daten aus Versehen weitergeben.

Beispiele aus der Praxis:

E-Mail-Konten:

Ein Angreifer könnte Ihr E-Mail-Passwort durch Phishing oder andere Methoden stehlen. Wenn Sie aber die Zwei-Faktor-Authentifizierung aktiviert haben (z.B. per Authentifizierungs-App oder SMS), kann er sich trotzdem nicht in Ihr Konto einloggen, ohne Zugriff auf Ihr Handy oder Ihren Authentifikator zu haben.

Banking-Apps:

Viele Banken bieten inzwischen 2FA für den Online-Zugang oder mobile Banking-Apps an. Selbst wenn jemand Ihr Bankpasswort kennt, würde der Zugriff auf Ihr Konto blockiert, wenn er den zweiten Faktor (z.B. einen Code, den die Bank Ihnen per App oder SMS sendet) nicht kennt.

Soziale Medien:

Bei sozialen Netzwerken wie Facebook oder Instagram können Sie ebenfalls die Zwei-Faktor-Authentifizierung aktivieren. So wird ein Angreifer, selbst wenn er Ihr Passwort kennt, daran gehindert, Ihr Konto zu übernehmen.

4.4. Übersicht beliebter Konten mit TOTP

- ☑ **E-Mail & Kommunikation**
  - Google-Konto (Gmail, Drive etc.)
  - Microsoft-Konto (Outlook, Office 365, OneDrive)
  - Yahoo-Mail
  - GMX & Web.de (TOTP bei Premium-Zugängen)
- ☑ **Soziale Netzwerke & Plattformen**
  - Facebook
  - Instagram
  - Twitter / X
  - TikTok
  - LinkedIn
- ☑ **Online-Shopping & Bezahldienste**
  - Amazon (TOTP möglichversteckt)
  - PayPal (TOTP indirekt
  - eBay
  - Etsy
  - Shopify
- ☑ **Cloud & Speicher**
  - Dropbox

- Google Drive
- Microsoft OneDrive

- ☑ **Streaming & Medien**
  - **Netflix** (aktuell kein
  - **Spotify** (via E-Mail-Login absichern)
  - **YouTube** (über Google-Konto)

- 🔐 **Weitere nützliche Dienste**
- **1Password, Bitwarden, KeePassXC** → Passwort-Manager mit TOTP-Integration
- **Dropbox, Tresorit** → Cloud mit Sicherheitsoptionen
- **NordVPN, ProtonVPN, Mullvad** → unterstützen TOTP

Fazit:

Zwei-Faktor-Authentifizierung ist ein sehr effektiver Schutzmechanismus gegen die meisten Arten von Angriffen. Sie stellt sicher, dass auch im Falle eines kompromittierten Passworts eine zusätzliche Hürde für den Angreifer geschaffen wird. Sie schützen Ihre Daten und Konten erheblich, indem Sie diese zusätzliche Sicherheitsebene aktivieren.

5. Sicherheitsmaßnahmen für mobile Geräte

5.1. Warum ist Sicherheit auf dem Smartphone wichtig?

Smartphones und Tablets sind praktische Begleiter im Alltag. Man schreibt Nachrichten, macht Fotos, erledigt Bankgeschäfte oder kauft online ein. Doch viele Nutzer wissen nicht: **Mobile Geräte können genauso angegriffen werden wie Computer**.

Gefahren sind zum Beispiel:

- **Schadprogramme (Malware)**, die Daten ausspionieren
- **Unsichere Apps**, die heimlich auf Kontakte oder Fotos zugreifen
- **Datenklau** durch Betrugslinks oder gefälschte Webseiten

Darum ist es wichtig, das eigene Gerät zu **schützen**, um **Betrug, Datenmissbrauch und Ärger** zu vermeiden.

5.2. Sichere Apps – darauf sollten Sie achten

Viele Angriffe passieren über **gefährliche Apps**. So schützen Sie sich:

☑ **Apps nur aus offiziellen App-Stores herunterladen**

- Android: **Google Play Store**
- iPhone/iPad: **Apple App Store**

☑ **App-Berechtigungen prüfen**
Beispiel: Eine Taschenlampen-App braucht **keinen Zugriff auf Kontakte oder Kamera**.

☑ **Unbekannte Quellen vermeiden**
Keine Apps aus Links in E-Mails, WhatsApp oder fremden Webseiten installieren.

5.3. Wie erkenne ich vertrauenswürdige Apps

Und welche sollte ich lieber meiden?

Das Erkennen von vertrauenswürdigen Apps und das Vermeiden von unsicheren oder potenziell gefährlichen Apps ist besonders wichtig, um Ihre Daten und Privatsphäre zu schützen. Hier sind einige einfache Tipps, die Ihnen helfen, die richtigen Apps auszuwählen und problematische Apps zu meiden:

1. Apps nur aus offiziellen Quellen herunterladen

- **Warum ist das wichtig?** Offizielle App-Stores wie der **Google Play Store** oder der **Apple App Store** überprüfen die Apps, bevor sie zum Download angeboten werden. Das verringert das Risiko, dass Sie eine schadhafte oder betrügerische App herunterladen.
- **Beispiel:** Wenn Sie eine App auf Ihrem **Smartphone** installieren möchten, stellen Sie sicher, dass Sie sie nur aus dem Google Play Store (für Android) oder dem Apple App Store (für iPhone) herunterladen und vermeiden Sie das Herunterladen von Apps aus anderen, unbekannten Quellen.

2. Lesen Sie die Bewertungen und Rezensionen

- **Warum ist das wichtig?** Bewertungen von anderen Nutzern können Ihnen helfen, herauszufinden, ob eine App vertrauenswürdig ist. Wenn viele Nutzer von schlechten Erfahrungen berichten, ist es besser, die App zu meiden.
- **Beispiel:** Schauen Sie sich die Bewertungen und Rezensionen der App im Store an. Wenn Sie dort viele Beschwerden über Bugs, unerwünschte Werbung oder Probleme mit der App sehen, sollten Sie die App lieber nicht installieren.

3. Überprüfen der Berechtigungen der App

- **Warum ist das wichtig?** Apps fragen oft nach Berechtigungen, die sie möglicherweise nicht wirklich brauchen. Eine vertrauenswürdige App verlangt nur die Berechtigungen, die für ihre Funktion notwendig sind.
- **Beispiel:** Wenn eine Taschenlampen-App nach Zugriff auf Ihre **Kontakte** oder **Kamera** fragt, obwohl sie nur eine Taschenlampe-Funktion bieten sollte, könnte das ein Hinweis darauf sein, dass die App mehr Daten von Ihnen sammeln möchte, als sie eigentlich sollte.

4. Achten Sie auf die Entwicklerinformationen

- **Warum ist das wichtig?** Seriöse Entwickler geben oft klare Informationen zu ihrer App und stellen sicher, dass sie regelmäßig aktualisiert wird. Unbekannte oder unseriöse Entwickler können dazu neigen, Apps zu veröffentlichen, die unsicher sind.
- **Beispiel:** Wenn Sie auf den Entwickler-Namen in der App-Beschreibung klicken, sehen Sie sich an, ob der Entwickler bekannt und vertrauenswürdig ist. Wenn der Entwickler keine Informationen zu seiner App bereitstellt oder unklar ist, könnte das ein Warnsignal sein.

5. Regelmäßige Updates sind wichtig

- **Warum ist das wichtig?** Eine vertrauenswürdige App wird regelmäßig mit Sicherheitsupdates versorgt. Das zeigt, dass der Entwickler die App weiterhin pflegt und sicherstellt, dass sie keine neuen Sicherheitslücken aufweist.
- **Beispiel:** Überprüfen Sie, ob die App regelmäßig aktualisiert wird. Wenn eine App monatelang oder jahrelang nicht mehr aktualisiert wurde, könnte sie Sicherheitslücken aufweisen, die von Hackern ausgenutzt werden könnten.

6. Suche nach bekannten und beliebten Apps

- **Warum ist das wichtig?** Bekannte Apps, die von großen, vertrauenswürdigen Unternehmen entwickelt wurden, sind oft sicherer, weil diese Unternehmen ein Interesse daran haben, ihre Nutzer zu schützen.
- **Beispiel:** Apps wie **WhatsApp**, **Facebook**, **Google Maps** oder **Instagram** sind bekannt und haben Millionen von Nutzern. Diese Apps sind gut etabliert und bieten meist hohe Sicherheitsstandards.

7. Vorsicht bei zu guten Angeboten

- **Warum ist das wichtig?** Apps, die zu verlockende Versprechungen machen (z. B. „Kostenlose Premium-Dienste“ oder „Sofort Geld verdienen“), können betrügerisch sein oder schadhafte Software enthalten.

- **Beispiel:** Eine App, die Ihnen verspricht, viel Geld zu verdienen, ohne dass Sie viel dafür tun müssen, ist oft ein Hinweis auf einen Betrug oder eine unseriöse App. Solche Apps sammeln oft nur Ihre persönlichen Daten oder drängen Sie dazu, Geld auszugeben.

8. Apps mit hoher Werbung und unerwünschten Inhalten meiden

- **Warum ist das wichtig?** Wenn eine App ständig Werbung anzeigt oder Sie auffordert, zusätzliche Apps herunterzuladen, ist das ein Zeichen, dass sie möglicherweise nicht vertrauenswürdig ist. Diese Apps könnten Ihre Daten ausspähen oder Ihnen schadhafte Software unterjubeln.
- **Beispiel:** Eine einfache App, die ständig Pop-up-Werbung oder Anzeigen schaltet, könnte in Wirklichkeit nur darauf abzielen, Ihnen Werbung zu zeigen oder Sie auf unsichere Webseiten weiterzuleiten.

9. Falsche Apps erkennen (z. B. Fake-Apps)

- **Warum ist das wichtig?** Es gibt viele Apps, die so aussehen wie die beliebten und vertrauenswürdigen, aber in Wahrheit gefälscht sind und Ihnen schaden können.
- **Beispiel:** Achten Sie darauf, ob der Name der App korrekt geschrieben ist. Manchmal gibt es Apps, die fast genauso heißen wie die Originale, aber einen kleinen Rechtschreibfehler oder eine zusätzliche Zahl enthalten, um Sie in die Irre zu führen.

10. Apps auf Viren und Malware überprüfen

- **Warum ist das wichtig?** Einige Apps enthalten Viren oder schadhafte Software, die Ihr Gerät beschädigen oder Ihre Daten stehlen können.
- **Beispiel:** Wenn Sie eine App installieren, sollten Sie Ihr Gerät regelmäßig mit einer **Antiviren-App** oder einem **Malware-Scanner** überprüfen, um sicherzustellen, dass keine schädliche Software auf Ihrem Gerät ist.

Zusammenfassung:

- **Vertrauenswürdige Apps:** Sie kommen aus offiziellen App-Stores, haben gute Bewertungen, fragen nur nach den notwendigen Berechtigungen und werden regelmäßig aktualisiert.
- **Unsichere Apps:** Diese haben unklare Entwicklerinformationen, verlangen zu viele Berechtigungen, machen zu verlockende Versprechungen oder zeigen zu viel Werbung.

5.4. Entsperr-Methoden – Ihr Handy vor fremdem Zugriff schützen

Wenn Ihr Handy verloren geht oder gestohlen wird, schützt eine gute Entsperrung Ihre Daten.

1. PIN / Passwort / Muster

Vorteile	Nachteile	Sicherheit
Weit verbreitet und geräteunabhängig. Kann sehr sicher sein (je nach Komplexität). Keine biometrischen Daten nötig.	Nutzer muss sich etwas merken. Tippfehler möglich, vor allem bei langen Passwörtern. Anfällig für Schulter-Blick-Attacken.	**PIN** (4–6 Stellen): mittel → 6-stellig ≈ 1 Mio Kombinationen (erheblich besser) Muster: eher gering (meist nur 9 Punkte, typische Muster leicht erratbar) Alphanumerisches Passwort: sehr hoch (besonders bei >8 Zeichen mit Symbolen)

Hinweis 5 PIN-Passwort-Muster

5.5. Anzahl möglicher gültiger Muster

Viele Nutzer schützen Ihr Smartphone durch ein Punkte-Muster, welches aus 3x3 Punkten besteht. Dies limitiert die Anzahl der möglichen Muster mit der Sie Ihr Telefon schützen. Eine Übersicht über die möglichen Muster gibt Ihnen die nachstehende Tabelle. Dabei sind die Möglichkeiten sehr stark von der Anzahl der verwendeten Punkte abhängig.

Anzahl der Punkte	Anzahl gültiger Muster
4 Punkte	1.624
5 Punkte	7.152
6 Punkte	26.016
7 Punkte	72.912
8 Punkte	140.704
9 Punkte	140.704

Hinweis 6 Tabelle mögliche Muster

Hier erkennt man, dass die Anzahl der möglichen verschiedenen Kombinationen sehr stark eingeschränkt ist. Bitte beachten Sie, dass dies weltweit alle Nutzer von Smartphones mit Muster gültig ist.

Warum sieht die letzte Zeile merkwürdig aus?

Es wirkt seltsam, dass es **genauso viele 9-Punkte-Muster wie 8-Punkte-Muster** gibt. Das ist aber richtig. Der Grund liegt darin, dass man beim Zeichnen eines Musters nicht springen darf – jeder Punkt darf nur einmal verwendet werden. Dadurch ergibt sich bei 8 und 9 Punkten zufällig die gleiche Anzahl möglicher Muster.

2. Fingerabdruck (Fingerprint)

Vorteile	Nachteile	Sicherheit
Schnell und bequem. Keine Notwendigkeit, sich etwas zu merken. Guter Kompromiss aus Komfort und Sicherheit.	Kann durch hochauflösende Fotos oder Abdrücke (z. B. Glas) im Labor geklont werden. Funktioniert schlecht bei feuchten oder verschmutzten Fingern. Sensorqualität variiert stark.	Gut für alltägliche Nutzung. Nicht hochsicher (z. B. für besonders schützenswerte Daten ungeeignet). In Sicherheitskreisen eher als mittelmäßig sicher eingestuft.

Hinweis 7 Fingerabdruck

3. Gesichtserkennung (Face Unlock)

Vorteile	Nachteile	Sicherheit
Extrem schnell und benutzerfreundlich. Kann bei den meisten Lichtverhältnissen verwendet werden (bei 3D-Versionen). Keine Berührung nötig.	Funktioniert nicht gut mit Maske / Sonnenbrille (je nach System). 2D-Systeme können mit Foto oder Video überlistet werden. Datenschutzbedenken (Gesicht als biometrisches Datum).	2D-Face Unlock: niedrig (leicht überlistbar). Apple Face ID / andere 3D-Systeme: hoch, schwer zu fälschen – lt. Apple: 1:1.000.000 Fehlerrate.

Hinweis 8 Gesichtserkennung

5.6. Sicherheit von Entsperr-Codes

Ein sicheres alphanumerisches Passwort schlägt jede PIN um Längen, sowohl gegen Brute-Force als auch gegen Wörterbuchangriffe – sofern es zufällig ist.

Methode	Theoretische Möglichkeiten
6-stellige PIN	1.000.000
8-stellige PIN	100.000.000
8-stellig alphanumerisch	~218 Billionen
12-stellig alphanumerisch (62 Zeichen)	~3,2 Trillionen

Hinweis 9 Entsperr-Codes

Tipp: Ein **alphanumerisches Passwort** (z. B. *Haus!2024* oder *Rose&Garten55*) bietet die **beste Sicherheit**.

5.7. Wichtige Schutzmaßnahmen für Ihr Gerät

☑ **Regelmäßig Updates installieren**

- Updates schließen Sicherheitslücken.
- Alte Software ist leicht angreifbar.

☑ **Sicheres Gerät – sichere Daten**

- Sperrbildschirm aktivieren
- SIM-Karte mit PIN schützen

☑ **Sicherheits-App verwenden (optional)**

- Zum Beispiel: *Avast*, *AVG*, *Kaspersky* oder *Bitdefender*
- Achtung: Nur **eine** Sicherheits-App installieren, nicht mehrere

6. Wie kann ich sicher im Internet einkaufen?

Sicheres Einkaufen im Internet ist wichtig, um persönliche Daten und Zahlungsmethoden zu schützen.

6.1. Wie erkenne ich eine sichere Internetverbindung?

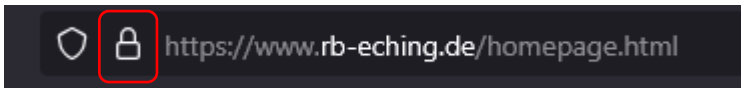
Wenn Sie eine Webseite besuchen – etwa Ihre Bank, eine Einkaufseite oder Ihr E-Mail-Konto – möchten Sie sicher sein, dass Ihre Daten **geschützt** sind. Eine sichere Internetverbindung sorgt dafür, dass niemand mitlesen kann, was Sie dort eingeben, z. B. Passwörter oder Kreditkartennummern.

Aber woran erkennt man, **ob eine Webseite sicher ist**?

Achten Sie auf das Schloss-Symbol 🔒

In der Adresszeile Ihres Browsers (also oben, wo die Internetadresse steht), sollte ein kleines Schloss-Symbol erscheinen. Es zeigt an, dass die Verbindung verschlüsselt, ist. Das bedeutet: Die Daten werden beim Versenden „verpackt", sodass niemand mitlesen kann.

Beispiel anhand der offiziellen Internet-Seite der Raiffeisenbank Buch-Eching eG im Browser **Firefox:**



Hinweis 10 Sichere Verbindung

⚠️ **Beispiel:** Gefälschte Adresse einer bekannten Bank

Stellen Sie sich vor, Sie möchten die Internetseite der **Sparkasse** besuchen. Die **echte** Adresse lautet:

☑ **https://www.sparkasse.de**

Nun erhalten Sie eine E-Mail, in der steht:

"Bitte melden Sie sich dringend über folgenden Link bei Ihrer Sparkasse an, um Ihr Konto zu schützen!"

Der Link in der Mail sieht so aus:

❌ **https://sparkasse-konto.sicher-login.info**

Oder auch:

❌ **https://sparkasse.de-kundensicherheit.net**

Beide Adressen **sehen auf den ersten Blick vertrauenswürdig aus**, sind aber **gefälscht**. Die Betrüger nutzen bekannte Namen und fügen z. B. „sicher", „login", „kundensupport" oder „konto" hinzu. Dadurch wirken die Seiten offiziell, sind aber **nicht von der echten Bank**.

🕵️ **So erkennen Sie den Unterschied:**

Die echte Adresse endet bei .de oder .com – und hat nichts Zusätzliches davor oder danach.

- → www.sparkasse.de ✅
- → www.sparkasse.de-login.net ❌

Gefälschte Seiten enthalten oft ungewöhnliche Wörter, viele Bindestriche oder fremde Domains (z. B. .info, .biz, .ru).

Prüfen Sie bei Unsicherheit immer direkt über die offizielle Startseite der Bank – geben Sie die Adresse von Hand ein oder speichern Sie sie als Lesezeichen.

Was ist ein Zertifikat auf einer Webseite?

Ein Zertifikat (genauer: ein SSL-/TLS-Zertifikat) ist ein digitales Dokument, das bestätigt, dass eine Webseite sicher ist und wirklich demjenigen gehört, der sie betreibt.

👉 Wichtig:

Wenn eine Webseite ein solches Zertifikat hat, wird die Verbindung zwischen deinem Gerät und der Webseite verschlüsselt. Das bedeutet: Niemand kann mitlesen – weder Passwörter noch persönliche Daten.

🔒 **Wie erkenne ich, ob eine Webseite ein gültiges Zertifikat hat?**

Du kannst das leicht in der **Adresszeile deines Internetbrowsers** erkennen (z. B. in Chrome, Firefox, Safari):

☑ **Zeichen für eine sichere Webseite:**

1. **Schloss-Symbol** links neben der Internetadresse
2. Die Adresse beginnt mit **https://** (das „s" steht für „secure" = sicher)

❌ **Zeichen für eine unsichere Webseite:**

- Kein Schloss
- Warnhinweis wie „Nicht sicher"
- Adresse beginnt nur mit **http://** (ohne „s")

🔍 **Wie prüfe ich das Zertifikat genauer?**

Wenn du wissen willst, **wer das Zertifikat ausgestellt hat** und ob es gültig ist:

So geht's in den gängigen Browsern:

🌐 **Google Chrome oder Microsoft Edge:**

1. Klicke auf das **Schloss-Symbol** links neben der Adresse.
2. Wähle „Zertifikat ist gültig" oder „Sicherheitsdetails".
3. Dort steht:
    - Für **welche Webseite** das Zertifikat gilt.
    - **Wer es ausgestellt hat** (z. B. DigiCert, Let's Encrypt).
    - **Bis wann es gültig ist**.

🦊 **Firefox:**

1. Klicke auf das **Schloss-Symbol**.
2. Dann auf „Verbindungsdetails" → „Weitere Informationen" → „Zertifikat anzeigen".

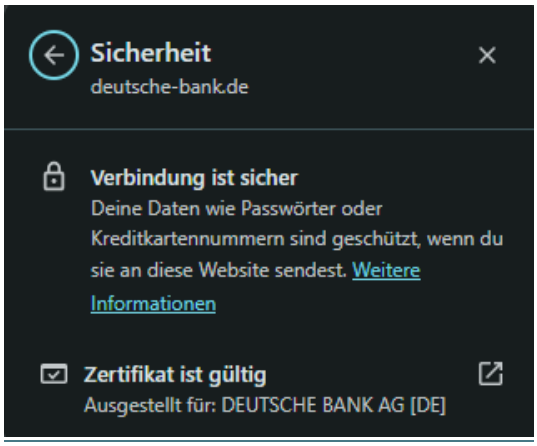
📱 **Auf dem Handy (z. B. im Chrome-Browser):**

- Auch hier kannst du auf das Schloss tippen – allerdings zeigen viele Smartphones nur eine einfache Sicherheitsinfo.

🕵 Beispiele

🔐 Sichere Webseite:

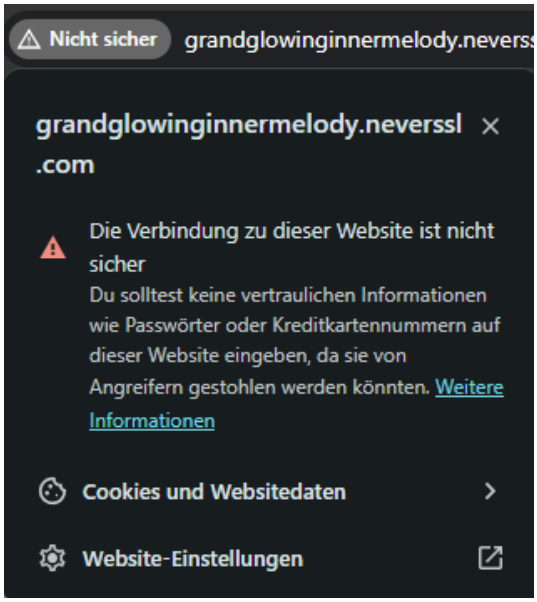
- https://www.deutsche-bank.de
  → Schloss-Symbol ✓
  → Adresse beginnt mit „https://" ✓
  → Zertifikat: gültig und von einer offiziellen Stelle ✓



Hinweis 11 Sichere Webseite

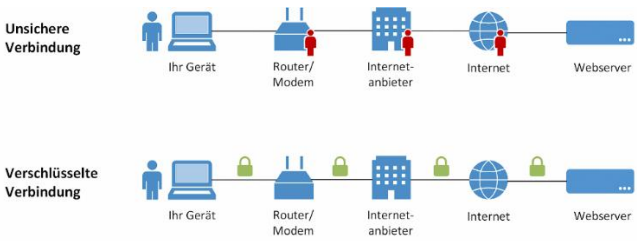
⚠ Unsichere Webseite (Beispiel):

- https://neverssl.com/
  → Kein Schloss ❌
  → „Nicht sicher"-Hinweis ❌
  → Daten sind nicht geschützt ❌



Hinweis 12 Unsichere Webseite

Unterschiede von unsichere und sicherer Verbindung:



Hinweis 13 Übersicht sichere Verbindungen

Tipps:

- **Nie persönliche Daten eingeben**, wenn kein Schloss zu sehen ist!
- Besonders bei **Online-Banking**, **Einkaufen** oder **E-Mails** immer auf das **https** und das **Schloss** achten.
- Bei Unsicherheiten lieber jemanden Fragen (Kinder, Enkel oder Nachbarn) oder die Seite meiden.

Merksatz:

"Wenn die Adresse komisch aussieht – nicht klicken!"

Achten Sie darauf, dass die Adresse mit https:// beginnt (nicht nur mit http://). Das „s" steht für „secure" – also „sicher".

Vorsicht bei Warnmeldungen

Moderne Browser wie Google Chrome, Firefox, Edge oder Safari warnen Sie oft, wenn eine Webseite unsicher oder sogar gefährlich ist. Dann sehen Sie z. B. eine rote Warnseite mit dem Hinweis „Diese Verbindung ist nicht sicher".

Tipp für Senioren:

Wenn Sie sich bei einer Seite nicht sicher sind, schließen Sie sie lieber und öffnen Sie sie später über eine vertrauenswürdige Quelle – z. B. die Startseite Ihrer Bank.

Nutzen Sie keine öffentlichen WLANs für sensible Dinge

Öffentliche WLAN-Netze (z. B. im Café oder Bahnhof) sind oft nicht ausreichend gesichert. Vermeiden Sie darin:

- Online-Banking
- Einkäufe mit Kreditkarte
- Eingabe von Passwörtern
- Wenn Sie solche Dinge erledigen möchten, nutzen Sie lieber Ihr Heim-WLAN oder das mobile Netz Ihres Smartphones.

Noch sicherer mit diesen Tipps:

- **Halten Sie Ihren Browser immer aktuell.**
- **Installieren Sie ein gutes Virenschutzprogramm.**
- **Geben Sie vertrauliche Daten nur auf bekannten Seiten ein.**

Quellen & Empfehlungen:

BSI – Sicher im Netz: www.bsi-fuer-buerger.de

Verbraucherzentrale – Sichere Webseiten erkennen: www.verbraucherzentrale.de

6.2. Häufige Bedrohungen und Betrugsarten

Gefälschte Online-Shops: Die Seite sieht super aus, aber die **Ware kommt nie** – und das Geld ist weg.

Phishing-E-Mails: E-Mails, die angeblich von der Bank, Post oder einem Online-Shop kommen – aber in Wirklichkeit nur eins wollen: Ihre **Zugangsdaten** oder Ihr Geld.

Fake-Rechnungen oder Mahnungen: Sie bekommen eine Rechnung für etwas, das Sie nie gekauft haben – und sollen **schnell** überweisen.

Telefonbetrug mit „Support" oder „Polizei": Da ruft jemand an und behauptet, der Computer sei **gehackt** worden – oder das Konto sei **gesperrt**.

Liebesbetrug („Love Scamming"): Jemand gibt sich online als Traumpartner aus – am Ende geht's um **Geld**, nicht um Gefühle.

Falsche Gewinnspiele: „Sie haben gewonnen!" – aber erst mal soll man **Gebühren** zahlen oder persönliche Daten rausrücken.

6.3. Unterschiedliche Arten von Bedrohungen

Betrug ohne Lieferung

- **Ziel:** Geld kassieren, ohne jemals Ware zu versenden.
- **Merkmale:**
  - Extrem günstige Preise, oft deutlich unter Marktwert.
  - Fehlendes oder gefälschtes Impressum.
  - Keine oder nur sehr eingeschränkte Zahlungsmethoden mit Käuferschutz (meist nur Vorkasse oder Kryptowährungen).
  - Keine echte Warenverfügbarkeit – Bilder und Texte oft kopiert von anderen Shops.
- **Risiko:** Reiner finanzieller Verlust, Ware kommt nie an.

Problematische, aber „echte" Händler

- **Ziel:** Verkauf findet statt, aber mit mangelhaften Bedingungen.
- **Merkmale:**
  - Lieferung zwar vorhanden, aber Ware defekt, falsch oder stark abweichend von der Beschreibung.
  - Schlechte oder unfaire Rückgabe- und Garantiebedingungen (z. B. Rücksendung nur auf eigene Kosten ins Ausland, keine Rückerstattung).
  - Überlange Lieferzeiten ohne klare Kommunikation.
  - Aggressive AGB, die Verbraucherrechte einschränken sollen.
- **Risiko:** Ärger, Qualitätsmängel, aufwendige Reklamation, möglicher Teil- oder Totalausfall des Geldes.

6.4. Achtung bei Shops außerhalb der EU

So prüfen Sie internationale Online-Anbieter auf Seriosität

- **Kein EU-Verbraucherschutz:** Bei Händlern außerhalb der EU gilt oft kein Widerrufsrecht oder Käuferschutz nach EU-Standard.

- **Impressum & Adresse prüfen:** Gibt es eine klare Firmenadresse? Prüfen Sie die Existenz über Google Maps.
- **AGB & Datenschutz vorhanden?** Seriöse Anbieter nennen klar ihre Rückgabe- und Datenschutzregeln – auch auf Englisch (**Terms & Conditions**).
- **Vorsicht bei Vorkasse:** Fehlt PayPal oder Kreditkarte mit 2FA, ist das Risiko bei Fake-Shops deutlich erhöht.

6.5. So erkennen Sie unseriöse oder gefälschte Internet-Shops

Fehlende Kontaktinformationen

Unseriöse Shops bieten oft keine oder unvollständige Kontaktinformationen, was Misstrauen wecken sollte.

Unrealistisch günstige Preise

Extrem niedrige Preise können auf gefälschte Shops hinweisen und sollten skeptisch betrachtet werden.

Schlechte Webseite und Design

Eine schlecht gestaltete Webseite deutet häufig auf einen unseriösen oder gefälschten Internet-Shop hin.

Fehlende Sicherheitszertifikate

Ohne SSL-Zertifikate oder Sicherheitskennzeichen sollten Sie keine Einkäufe tätigen.

6.6. So erkennen Sie einen Fake-Shop

Keine oder unvollständige Impressumsangaben

→ Ein seriöser Online-Shop hat ein vollständiges Impressum (mit Name, Adresse, Telefonnummer und E-Mail-Adresse).

Unglaubwürdig günstige Preise

→ Wenn Produkte deutlich unter dem Marktwert verkauft werden, ist das ein Warnzeichen.

Nur Vorkasse als Zahlungsmethode

→ Fehlen Optionen wie PayPal, Kreditkarte oder Kauf auf Rechnung, ist Vorsicht geboten.

Fehlende oder schlechte Kundenbewertungen

→ Prüfen Sie unabhängige Bewertungsseiten wie Trustpilot oder Google Reviews.

Fehlerhafte Sprache

→ Viele Fake-Shops haben schlecht übersetzte Texte oder ungewöhnliche Formulierungen.

Webadresse (URL)

→ Oft sind die Domains ungewöhnlich, z. B. mit exotischen Endungen oder Zahlencodes (z. B. shop12345.biz).

Webseiten zur Shop-Überprüfung

www.watchlist-internet.at

- Bietet aktuelle Warnungen vor Fake-Shops.
- Möglichkeit zur Meldung und Prüfung verdächtiger Seiten.

www.fakeshop-finder.de (vom Bayerischen Verbraucherschutzministerium)

- Einfach URL eingeben → automatische Prüfung.
- Ampelsystem: grün = sicher, rot = gefährlich.

www.verbraucherzentrale.de

- Dort findest du eine Fake-Shop-Liste und weitere Ratgeber.
- Möglichkeit zur Meldung von Betrugsfällen.

◐ Zusätzlicher Tipp

Nutze beim Online-Shopping Browser-Add-ons, wie:

- Web of Trust (WOT) https://www.mywot.com/de/→ bewertet Websites anhand von Nutzerfeedback.
- Trusted Shops Badge → Shops mit Gütesiegel sind meist geprüft.

6.7. Verwendung von vertrauenswürdige Websites

Achten Sie auf die URL: Stelle sicher, dass die Webseite eine sichere Verbindung hat, indem die URL mit "https" beginnt (das "s" steht für Sicherheit).

Reputation prüfen: Kaufen Sie nur bei bekannten und vertrauenswürdigen Online-Shops oder großen Plattformen (z.B. Amazon, Zalando, eBay). Nutzen Sie Bewertungen und Rezensionen, um die Seriosität der Seite zu überprüfen.

Datenschutzerklärung lesen: Informieren Sie sich über die Datenschutzrichtlinien der Webseite, um sicherzustellen, dass Ihre persönlichen Daten geschützt sind.

6.8. Verwenden von sichere Zahlungsmethoden

Kreditkarte oder PayPal: Diese Zahlungsmethoden bieten in der Regel einen zusätzlichen Schutz. Besonders PayPal bietet Käuferschutz, falls etwas schief geht.

Keine Überweisungen an unbekannte Verkäufer: Vermeiden Sie direkte Banküberweisungen an unbekannte Händler, da dies bei Problemen schwer rückgängig gemacht werden kann.

Zwei-Faktor-Authentifizierung: Nutzen Sie, wenn möglich, eine zusätzliche Authentifizierungsmethode, wie eine TAN oder ein Fingerabdruck, um die Sicherheit deiner Zahlungen zu erhöhen. (Siehe auch nachfolgendes Kapitel: „Was ist Zwei-Faktor-Authentifizierung – und warum schützt sie mich?"

6.9. Sichere Online-Shops und vertrauenswürdiges Einkaufen

Bekannte Anbieter sind meist sicherer

Viele große und etablierte Online-Shops arbeiten zuverlässig und seriös. Sie bieten klare Kontaktmöglichkeiten, liefern pünktlich und nehmen Ware bei Problemen wieder zurück. Wenn Sie sich unsicher sind, kaufen Sie lieber bei bekannten Anbietern oder bei Shops, die Ihnen von Freunden empfohlen wurden.

Vorsicht bei:

- Shops, die außergewöhnlich billig wirken

- Angeboten auf unbekannten Webseiten
- Online-Shops ohne Impressum oder Kontaktadresse

Prüfsiegel – ein Zeichen für geprüfte Sicherheit

Seriöse Händler lassen sich regelmäßig prüfen. Sie erhalten dafür Prüfsiegel, die man auf ihrer Internetseite findet. Zu den bekanntesten gehören:

Prüfsiegel	Bedeutung
Trusted Shops	Käuferschutz und Datenschutz geprüft
EHI-Gütesiegel	Händlerrecht, Transparenz und Sicherheit geprüft
TÜV geprüft	Technische Sicherheit des Shops geprüft

Hinweis 14 Prüfsiegel

Wichtig zu wissen: Prüfsiegel können gefälscht sein! Ein echtes Siegel ist **anklickbar** und führt zu einer offiziellen Zertifikatsseite. Funktioniert der Klick nicht – Finger weg!

Achten Sie auf sichere Internetverbindungen

Eine sichere Verbindung erkennen Sie am **Schloss-Symbol** im Browser und am **„https://“** vor der Internetadresse. Das „s“ steht für „sicher“.

☑ Beispiel einer sicheren Adresse:
https://www.bekannter-shop.de
❌ Unsichere Adresse:
http://billig-shop-online.de

Warnzeichen:

- Kein Schloss-Symbol im Browser
- Adresse enthält Rechtschreibfehler (z. B. **www.adidass.de**)
- Die Adresse wirkt „komisch“ – dann ist sie das meist auch!

So erkennen Sie gefälschte Online-Shops

Betrüger machen sich viel Mühe, gefälschte Shops echt aussehen zu lassen. Doch es gibt typische Warnsignale:

- **Keine Kontaktmöglichkeit** – nur E-Mail, kein Telefon
- **Kein Impressum** – keine Firma, keine Adresse
- **Nur Vorkasse oder Bitcoin** – keine sicheren Zahlungsmethoden
- **Sensationelle Preise** – zu gut, um wahr zu sein
- **Druck** – „Nur noch heute!“, „Letzte Chance!“

Beispiel für eine fragwürdige Adresse:
🚫 **www.nike-deutschland-schnäppchen.store**

Das klingt zwar seriös, ist aber eine Falle. Marken wie Nike verkaufen nicht über solche Fantasie-Webseiten.

Tipp zum Merken

Im Internet gibt es viele echte Schnäppchen – aber auch viele Schwindler.
Wer zweimal hinschaut, kauft sicherer.

6.10. Achten auf Sicherheitszeichen

SSL-Zertifikate: Seiten mit einem SSL-Zertifikat (erkennbar an "https" und einem Schloss-Symbol in der URL-Leiste) bieten verschlüsselte Kommunikation, die Daten schützt.

Vertrauenssiegel: Achten Sie auf bekannte Vertrauenssiegel, wie z.B. "Trusted Shops" oder "EHI-Siegel". Diese zeigen, dass die Seite bestimmte Sicherheitsstandards erfüllt.

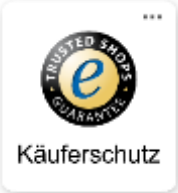
Was sind Trusted Shops?

Trusted Shops (Vertrauenswürdige Geschäfte) ist ein bekanntes Siegel, das Online-Shops in Europa erhalten können, um Vertrauen und Sicherheit zu vermitteln. Es stellt sicher, dass der Online-Shop bestimmte Sicherheits- und Qualitätskriterien erfüllt.

Wie funktioniert ein Trusted Shop?

Überprüfung des Shops: Trusted Shops prüft regelmäßig, ob ein Online-Shop sicher ist. Dazu gehören die Überprüfung von Datenschutzrichtlinien, allgemeinen Geschäftsbedingungen (AGB), Lieferbedingungen, Rückgaberechten und den Zahlungsmethoden. Ein Shop muss auch ein kundenfreundliches und faires Verhalten zeigen.

Das Trusted Shop Siegel sieht so aus:



Hinweis 15 Trusted Shop Siegel

Käuferschutz: Das Trusted Shops-Siegel bietet den Käufern zusätzlichen Schutz. Wenn Sie etwas bei einem zertifizierten Shop kaufen, sind Sie durch den Trusted Shops Käuferschutz abgesichert. Dies bedeutet, dass Sie Ihr Geld zurückerhalten können, wenn der Shop nicht liefert oder die Ware beschädigt ist. Der Käuferschutz greift auch bei Problemen mit der Rückerstattung von Rücksendungen.

Bewertungen: Trusted Shops ermöglicht es Käufern, Bewertungen abzugeben. Diese Bewertungen sind ein wichtiger Teil des Vertrauenssystems und helfen anderen Käufern, sich eine Meinung über den Shop zu bilden.

Zertifizierungskosten: Online-Shops müssen für die Zertifizierung durch Trusted Shops zahlen. Es gibt jedoch strenge Anforderungen, die erfüllt werden müssen, um das Siegel zu erhalten, was bedeutet, dass dieser Shop als vertrauenswürdig gilt.

Vorteile für den Verbraucher:

- **Käuferschutz**: Im Falle von Problemen bekommen Sie Ihr Geld zurück.
- **Vertrauen**: Das Trusted Shops-Siegel signalisiert, dass der Shop hohe Sicherheits- und Qualitätsstandards erfüllt.
- **Transparenz**: Trusted Shops bietet eine transparente Bewertung von Shops und Produkten.

EHI-Siegel

Was ist das EHI-Siegel? Das EHI-Siegel wird vom EHI Retail Institute, einer renommierten deutschen Forschungseinrichtung, vergeben. Es ist ein weiteres Sicherheitszeichen, das Online-Shops erhalten können, wenn sie hohe Anforderungen in Bezug auf Sicherheit, Service und Qualität erfüllen.

Das EHI-Siegel sieht so aus:

Hinweis 16 EHI Siegel

Wie funktioniert das EHI-Siegel?

Überprüfung und Zertifizierung: Das EHI-Siegel wird an Online-Shops vergeben, die sich einer umfassenden Prüfung unterziehen müssen. Diese Prüfung umfasst sowohl rechtliche als auch sicherheitstechnische Aspekte des Online-Shops. Dazu gehören Datenschutz, Versandbedingungen, Rückgaberechte, Zahlungsmethoden und die IT-Sicherheit.

Regelmäßige Audits: Ein EHI-zertifizierter Shop wird regelmäßig überprüft, um sicherzustellen, dass er weiterhin den hohen Standards entspricht.

Verbraucherschutz: Das EHI-Siegel steht für hohe Verbraucherfreundlichkeit. Shops, die dieses Siegel tragen, bieten transparente Geschäftsbedingungen und fairen Kundenservice. Dazu gehört auch ein klarer Prozess für Rücksendungen und Rückerstattungen.

Vorteile für den Verbraucher:

Rechtliche Sicherheit: Shops mit dem EHI-Siegel erfüllen die deutschen Verbraucherrechte, was dir als Käufer zusätzliche Sicherheit gibt.

Verbraucherschutz: Das Siegel stellt sicher, dass der Shop alle gesetzlichen Anforderungen im Hinblick auf Datenschutz, Preisangaben und Zahlungsbedingungen erfüllt.

Verlässlichkeit: EHI-zertifizierte Shops müssen regelmäßig Audits bestehen, was das Vertrauen in den Shop erhöht.

Unterschiede zwischen Trusted Shops und EHI-Siegel

Trusted Shops bietet in erster Linie Käuferschutz und ermöglicht die Abgabe von Bewertungen durch Kunden. Es ist stärker auf den Kundenschutz fokussiert und umfasst zusätzliche Dienste wie eine Geld-zurück-Garantie.

Das EHI-Siegel legt mehr Wert auf die Einhaltung von rechtlichen Anforderungen und den Verbraucherschutz. Es stellt sicher, dass der Shop die notwendigen gesetzlichen Vorschriften einhält und regelmäßig überprüft wird, bietet jedoch keinen expliziten Käuferschutz wie Trusted Shops.

Wie Sie das Siegel erkennen:

Trusted Shops: Sie finden das Trusted Shops-Siegel oft im Fußbereich der Seite oder auf Produktseiten. Es ist auch häufig als Logo mit der Aufschrift "Trusted Shops" sichtbar. Wenn Sie auf das Siegel klicken, bekommen Sie Informationen zur Zertifizierung des Shops. **Wichtiger Hinweis:** Das Siegel muss man anklicken können und dort auf die entsprechende Seite weitergeleitet werden, es darf **kein Bild** sein!

EHI-Siegel: Das EHI-Siegel ist ein rundes Logo mit dem Schriftzug "EHI geprüfter Online-Shop". Auch dieses Siegel ist meist am Ende der Seite oder auf der „Über uns"-Seite des Shops zu finden.

Wichtiger Hinweis: Das Siegel muss man anklicken können und dort auf die entsprechende Seite weitergeleitet werden, es darf **kein Bild** sein!

Fazit

Beide Siegel bieten zusätzliche Sicherheit beim Online-Einkauf. Trusted Shops eignet sich besonders, wenn Sie zusätzlichen Schutz für Ihren Einkauf suchen, während das EHI-Siegel Vertrauen in die Einhaltung rechtlicher und sicherheitsrelevanter Standards des Shops gibt. Beide Siegel tragen dazu bei, dass Sie mit einem sicheren Gefühl einkaufen können.

Wenn Sie beim Online-Shopping auf eines dieser Siegel stoßen, können Sie sicherer sein, dass der Shop überprüft wurde und hohe Standards in Bezug auf Service, Sicherheit und Verbraucherschutz einhält.

7. Wie bezahle ich sicher mit PayPal oder anderen Online-Diensten?

Das Bezahlen mit PayPal und anderen Online-Zahlungsdiensten ist eine bequeme und sichere Möglichkeit, um Einkäufe im Internet zu tätigen. Allerdings gibt es bestimmte Maßnahmen, die Sie ergreifen können, um sicherzustellen, dass Ihre Zahlungen geschützt sind. Hier sind einige bewährte Schritte, die Sie befolgen können:

7.1. Verwendung vertrauenswürdiger Online-Zahlungsdienste

PayPal ist eine der beliebtesten und sichersten Zahlungsmethoden, da sie Ihren Zahlungsverkehr schützen und keine sensiblen Finanzdaten direkt an den Händler weitergibt. Auch andere Dienste wie Stripe oder Apple Pay bieten hohe Sicherheitsstandards.

Achten Sie auf die Qualität des Anbieters: Nutzen Sie nur bekannte Zahlungsdienste, die hohe Sicherheitsstandards haben und von großen Online-Shops oder etablierten Plattformen verwendet werden.

7.2. Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA)

Schützen Sie Ihr PayPal-Konto mit 2FA: Aktivieren Sie die Zwei-Faktor-Authentifizierung für Ihr PayPal-Konto, um zusätzliche Sicherheit zu bieten. So benötigen Sie neben Ihrem Passwort einen zusätzlichen Code (z.B. aus einer Authentifizierungs-App oder per SMS), um sich einzuloggen.

Schutz vor unbefugtem Zugriff: Wenn jemand Ihr Passwort stiehlt, ist der Zugriff auf Ihr Konto trotzdem durch den zweiten Faktor gesichert.

7.3. Nutzen Sie eine sichere Internetverbindung

WLAN und öffentliche Netzwerke: Vermeiden Sie es, Zahlungen über öffentliche WLAN-Netzwerke oder unsichere Verbindungen zu tätigen. Öffentliche Netzwerke sind anfällig für Angriffe, und ein Angreifer könnte versuchen, Ihre Zahlungsdaten abzufangen.

VPN verwenden: Wenn Sie von öffentlichen Netzwerken aus einkaufen, können Sie ein VPN (Virtual Private Network) verwenden, um Ihre Internetverbindung zu verschlüsseln und Ihre Daten zu schützen. Nützliche benutzerfreundliche VPN-Anbieter aus Deutschland oder mit deutscher Oberfläche:

- **CyberGhost** (https://www.cyberghostvpn.com/de/)– deutschsprachig, sehr einsteigerfreundlich, viele Server.
- **ZenMate** (https://zenmate.com/)– deutscher Anbieter, einfache Bedienung, gut für Alltagssurfer.
- **NordVPN** (https://nordvpn.com/de/) international, aber komplett auf Deutsch verfügbar, viele Sicherheitsfunktionen.
- **Avira Phantom VPN** (https://www.avira.com/de/free-vpn-windows) vom deutschen Antivirus-Hersteller Avira, schlicht und leicht zu nutzen.

7.4. Achten Sie auf die Adresse der Webseite (URL)

HTTPS: Stellen Sie sicher, dass die Webseite, auf der Sie einkaufen, „https" in der URL verwendet und ein kleines Schloss-Symbol in der Adressleiste Ihres Browsers angezeigt wird. Dies bedeutet, dass die Verbindung verschlüsselt und sicher ist.

Kein **„http" ohne „s":** Webseiten, die kein „https" haben, sind nicht sicher, und deine Zahlungsdaten könnten abgefangen werden.

7.5. Zahlen Sie nur bei vertrauenswürdigen Händlern

Vertrauenssiegel und Bewertungen: Kaufen Sie nur bei Händlern, die gut bewertet sind und vertrauenswürdige Siegel wie Trusted Shops oder EHI-Siegel haben. Diese Siegel garantieren, dass der Händler geprüft wurde und Sie geschützt sind.

Überprüfen Sie den Händler: Wenn Sie bei einem unbekannten Online-Shop einkaufen, schauen Sie sich Kundenbewertungen an und prüfen, ob der Händler eine gültige Rückgabe- und Datenschutzrichtlinie hat.

7.6. Achten Sie auf die Sicherheit Ihrer PayPal- oder Kontoinformationen

Phishing vermeiden: Betrüger könnten versuchen, Sie mit gefälschten E-Mails oder Nachrichten dazu zu bringen, Ihre Login-Daten preiszugeben. PayPal und andere seriöse Zahlungsdienste werden Sie niemals per E-Mail auffordern, auf Links zu klicken oder sensible Informationen einzugeben.

Direkt einloggen: Gehen Sie immer direkt auf die Webseite von PayPal (oder dem Zahlungsdienst Ihrer Wahl), anstatt Links aus E-Mails zu folgen. Idealerweise haben Sie sich in dem Browser Ihre eigenen Favoritenliste gespeichert. So vermeiden Sie Phishing-Angriffe.

7.7. Nutzen Sie die Käuferschutzfunktionen

PayPal Käuferschutz: Einer der größten Vorteile von PayPal ist der Käuferschutz. Wenn etwas mit Ihrer Bestellung nicht stimmt (z.B. der Artikel kommt nicht an oder entspricht nicht der Beschreibung), können Sie eine Rückerstattung über PayPal beantragen.

Rückerstattung sicherstellen: Überprüfen, ob der Händler ebenfalls ein Rückgaberecht anbietet, um Sie abzusichern, falls der Artikel defekt ist oder nicht wie beschrieben.

7.8. Behalten Sie Ihre Kontobewegungen im Auge

Regelmäßige Kontrolle: Überprüfen Sie regelmäßig Ihr PayPal-Konto oder das Konto Ihres Online-Zahlungsdienstes auf ungewöhnliche Aktivitäten. Wenn Sie eine unbekannte Zahlung sehen, sollten Sie sofort reagieren und den Anbieter kontaktieren.

Benachrichtigungen aktivieren: Stellen Sie sicher, dass Sie Benachrichtigungen für alle Zahlungen und Transaktionen erhalten, sodass Sie sofort informiert werden, wenn es zu einer nicht autorisierten Zahlung kommt.

7.9. Vermeiden Sie das Speichern von Zahlungsinformationen

Nicht speichern lassen: Viele Online-Shops bieten an, Ihre Zahlungsinformationen für zukünftige Einkäufe zu speichern. Dies ist zwar bequem, aber es kann zu Sicherheitsrisiken führen, wenn ein Hacker Zugang zu Ihren Konto erhält. Geben Sie Ihre Zahlungsinformationen lieber jedes Mal manuell ein.

Alternativen wie virtuelle Kreditkarten: Sie können auch eine virtuelle Kreditkarte verwenden, die nur für einmalige Zahlungen verwendet wird und keine direkten Bankdaten speichert.

Beispiele zur sicheren Zahlung mit PayPal oder anderen Online-Diensten:

Beispiel 1: Einkauf bei einem bekannten Online-Shop (z.B. Amazon)

Sie möchten ein Produkt auf Amazon kaufen. Sie wählen PayPal als Zahlungsmethode und geben Ihre PayPal-Anmeldedaten ein.

Nachdem Sie Ihr Passwort eingegeben haben, erhalten Sie einen einmaligen Code auf Ihr Handy, den Sie eingeben (Zwei-Faktor-Authentifizierung).

Sie überprüfen die HTTPS-Verbindung der Amazon-Webseite (die URL beginnt mit „https://" und es erscheint ein Schlosssymbol in der Browserleiste).

Ihre PayPal-Transaktion wird durch den Käuferschutz gesichert, falls etwas mit der Lieferung schiefgeht.

Beispiel 2: Bezahlung bei einem weniger bekannten Online-Shop

Sie sind auf einem Online-Shop, der PayPal als Zahlungsmethode anbietet. Sie überprüfen, ob die Webseite mit einem sicheren HTTPS-Protokoll verschlüsselt ist.

Nachdem Sie Ihre Bestellung abgeschlossen haben, werden Sie zur PayPal-Seite weitergeleitet. Sie geben Ihre PayPal-Anmeldedaten ein und bestätigen die Zahlung.

Falls der Artikel nie ankommt oder nicht wie beschrieben ist, können Sie den Käuferschutz von PayPal aktivieren, um Ihr Geld zurückzuerhalten.

Fazit:

Die Zahlung mit PayPal und anderen Online-Zahlungsdiensten ist eine sehr sichere Methode, um Einkäufe im Internet zu tätigen, wenn Sie einige grundlegende Sicherheitsvorkehrungen beachten. Durch die Zwei-Faktor-Authentifizierung, die Auswahl eines vertrauenswürdigen Händlers, und die Vermeidung von Phishing-Angriffen können Sie Ihre Zahlungen effektiv absichern. Die Käuferschutzfunktionen sorgen dafür, dass Sie im Fall von Problemen mit der Bestellung Ihr Geld zurückbekommen.

8. Bekannte Betrugsmethoden und Maßnahmen

8.1. Woran erkenne ich eine Phishing-E-Mail?

Phishing-E-Mails sind betrügerische Nachrichten, mit denen Kriminelle versuchen, sensible Informationen wie **Passwörter**, **Bankdaten** oder **Zugangsdaten** zu erlangen. Sie tarnen sich oft als offizielle E-Mails von Banken, Online-Shops oder bekannten Diensten wie PayPal oder Amazon. Wenn Sie solche E-Mails erkennen, können Sie sich und Ihre Daten effektiv schützen.

✅ **Merkmale einer Phishing-E-Mail**

8.2. Dringender Handlungsbedarf oder Drohungen

- **Typisch**: „Ihr Konto wurde gesperrt" oder „Letzte Mahnung".
- **Ziel**: Druck aufbauen, damit Sie schnell (und unüberlegt) reagieren.

🔍 **Beispiel**:

"*Sehr geehrter Kunde, Ihr PayPal-Konto wurde aus Sicherheitsgründen gesperrt. Bitte bestätigen Sie Ihre Identität über folgenden Link, um den Zugriff wiederherzustellen.*"

8.3. Ungewöhnliche Absenderadresse

- Die Adresse sieht oft ähnlich aus, hat aber kleine Abweichungen:
    - Statt **service@paypal.com** → **serviice@pay-pal.com**

🔍 **Beispiel**:

Absender: paypal-support@security-check.io (Achtung: Das „**l**" in „paypal" ist ein großes **i**, kein kleines **L**!)

8.4. Links, die zu gefälschten Webseiten führen

- Sie werden aufgefordert, auf einen Button oder Link zu klicken.
- **Ziel** ist eine gefälschte Webseite, die aussieht wie das Original, um Ihre Daten zu stehlen.

🔍 **Tipp**: Fahren Sie mit der Maus über den Link (**ohne zu klicken!**) – erscheint eine verdächtige oder unbekannte URL, ist das ein Warnsignal.

8.5. Grammatik- und Rechtschreibfehler

- Viele Phishing-E-Mails enthalten manchmal schlechte Übersetzungen, fehlende Umlaute oder unübliche Formulierungen.

🔍 **Beispiel**:

"*Wir benötigen Ihre Aktualizirung der Daten, sonst wird ihr Zugrif begrenzt!*"

8.6. Unpersönliche Anrede

- Echte Unternehmen sprechen Sie mit deinem Namen an. Phishing-Mails oft nur mit:
    - „Sehr geehrter Kunde", „Lieber Nutzer", „Hallo", „Guten Tag".

🔍 **Beispiel**:

"*Hallo Nutzer, Ihre Amazon-Bestellung konnte nicht verarbeitet werden.*"

8.7. Aufforderung zur Eingabe sensibler Daten

Kein **seriöser** Anbieter wird Sie per E-Mail auffordern, Ihre

- **Passwörter**
- **Bankdaten**
- **TANs oder PINs**
- **Personalausweisdaten**

einzugeben – schon gar nicht über einen Link in der Mail.

🔍 **Beispiel**:

"*Bitte geben Sie Ihre Kreditkartennummer und das Ablaufdatum ein, um die Sperrung zu verhindern.*"

🚨 **Was tun bei Verdacht auf Phishing?**

☑ **NICHT klicken – weder auf Links noch auf Dateianhänge**
☑ **E-Mail nicht beantworten**
☑ **Absenderadresse prüfen**
☑ **Webseite direkt im Browser eingeben (z. B. www.paypal.com statt auf den Link in der Mail klicken)**
☑ **E-Mail weiterleiten an z. B. phishing@paypal.com, phishing@amazon.de**

📌 **Echtes Beispiel: Gefälschte Sparkassen-Mail**

Betreff: "*Ihr Online-Banking wurde eingeschränkt – jetzt freischalten!*"
Text:
"*Sehr geehrter Kunde, aufgrund einer neuen EU-Richtlinie müssen Sie Ihre Daten aktualisieren. Bitte melden Sie sich über folgenden Link an und bestätigen Sie Ihre Angaben.*"
Link: www.sparkasse-login-sicher.de (gefälschte Adresse)
→ **Ziel**: Zugangsdaten abgreifen

🔒 Sparkassen-Mitarbeiter warnen: *„Wir versenden solche E-Mails nie."*

🧠 **Merksatz:**

„Im Zweifel: Nicht klicken, nicht tippen, nicht trauen!"

8.8. Wie reagiere ich richtig auf verdächtige E-Mails und Nachrichten?

Verdächtige E-Mails, SMS oder Messenger-Nachrichten können gefährlich sein – besonders wenn sie versuchen, Sie zu täuschen (Phishing), Malware zu verbreiten oder Ihre persönlichen Daten zu stehlen. Aber keine Sorge: Mit der richtigen Reaktion bleiben Sie sicher.

✅ **So reagieren Sie richtig – Schritt für Schritt**

1. Nicht klicken, nicht antworten, nicht öffnen

🔒 Das Wichtigste zuerst:

- **Klicken Sie niemals auf Links oder Anhänge**, wenn Sie unsicher sind.
- **Antworten Sie nicht** – selbst eine harmlose Antwort kann zeigen, dass Ihre Adresse aktiv ist.
- **Öffnen Sie keine Anhänge** – sie könnten Schadsoftware enthalten.

📌 **Merksatz**: *„Im Zweifel: Finger weg!"*

2. Absender und Inhalte genau prüfen

👀 Achten Sie auf:

- **Ungewöhnliche E-Mail-Adressen**
- **Fehlerhafte Sprache oder schlechte Grammatik**
- **Unpersönliche Anrede** (z. B. „Sehr geehrter Kunde")
- **Druckvolle Sprache** („Sperrung droht", „Letzte Warnung")

🔍 Beispiel:

Absender: service@amazzon-support.org
Inhalt: „Klicken Sie hier, um Ihre Bestellung zu bestätigen"

→ **Verdächtig!** Kein echter Absender, kein echter Link.

3. Auf keinen Fall persönliche Daten eingeben

🚫 Seriöse Unternehmen fordern Sie **niemals per E-Mail oder Nachricht** dazu auf, Passwörter, TANs, PINs oder Bankdaten anzugeben – auch nicht „zur Sicherheit" oder „zur Verifizierung".

4. Keine Angst – einfach ignorieren oder löschen

🗑️ Wenn Sie sich unsicher sind, aber keine wichtigen Daten eingegeben haben:

- **Löschen Sie die Nachricht**
- **Markieren Sie sie ggf. als Spam oder Junk**
- Das war's – keine weiteren Schritte notwendig.

5. E-Mail als Phishing melden

📧 Weiterleiten an:

- **phishing@amazon.de**
- **spoof@paypal.com**

- Oder an Ihr eigenes IT-Team (z. B. bei Firmen-E-Mails)

📌 Tipp: Viele E-Mail-Programme (z. B. Gmail, Outlook) bieten eine Funktion **„Phishing melden"** – nutzen Sie sie!

6. Haben Sie versehentlich geklickt oder Daten eingegeben? Dann sofort:

Eine rasche Reaktion kann Schäden verhindern:

- **Passwort ändern** (bei dem betroffenen Dienst – und überall dort, wo Sie dasselbe Passwort nutzen)
- **Zugang sperren lassen** (z. B. beim Online-Banking)
- **Kontoaktivitäten prüfen**
- **Antivirus-Scan starten** auf Ihrem Gerät
- **Kontakt zum Anbieter aufnehmen**, wenn Sie sich unsicher sind.

🔐 **Beispiel: Sie bekommen eine verdächtige PayPal-Mail**

📩 Inhalt: „Ihr Konto wurde aus Sicherheitsgründen eingeschränkt. Melden Sie sich hier an, um es zu reaktivieren."
🔗 Link: paypal-kundenservice.net
📧 Absender: support@paypal-account-check.info

Richtiges Vorgehen:

- Link **nicht** anklicken
- Mail an **spoof@paypal.com** weiterleiten
- Mail löschen

☑ Fertig – Sie haben alles richtig gemacht!

Fazit:

🛡 Der beste Schutz gegen Betrugsversuche ist **gesunder Menschenverstand**, **Vorsicht** und **richtiges Verhalten im Ernstfall**. Mit ein paar Klicks zu viel kann man schnell viel Schaden anrichten – mit ein paar richtigen Klicks auch viel vermeiden.

8.9. Was steckt hinter betrügerischen Anrufen?

Zum Beispiel von angeblichen Banken oder der Polizei?

Betrügerische Anrufe – auch **Telefon-Phishing** oder **„Vishing"** genannt (von „Voice Phishing") – sind gezielte Versuche, Sie telefonisch zu täuschen. Die Täter geben sich als **Bank**, **Polizei**, **Microsoft-Support** oder andere seriöse Organisationen aus, um an Ihre **Daten**, **Zugangsinformationen** oder **Ihr Geld** zu gelangen.

🎭 **Wie funktionieren diese Anrufe?**

Die Täter setzen Sie unter Druck, um Sie zu einer **schnellen Reaktion** zu bewegen. Dabei nutzen sie verschiedene **Tricks** und **Szenarien**:

☑ **Typische Maschen – und was dahintersteckt**

Falsche Polizei („Ihr Konto ist in Gefahr")

👮 Der Anrufer gibt sich als Polizist aus und sagt:

„Wir haben Hinweise auf einen Betrug mit Ihrem Bankkonto. Sie müssen Ihr Geld sichern!"

🎯 Ziel: Sie sollen Ihr Geld auf ein „sicheres Konto" überweisen – das in Wirklichkeit den Betrügern gehört.

🔍 **Achtung**: Die Polizei ruft Sie **niemals an**, um Geld zu sichern oder Sie zu Überweisungen zu drängen!

Falsche Bankmitarbeiter

🏦 Ein vermeintlicher Bankangestellter warnt Sie:

„Auf Ihrem Konto gab es einen verdächtigen Zugriff. Wir benötigen Ihre TANs oder Ihre PIN."

🎯 Ziel: Zugang zu Ihrem Online-Banking oder Ihrer Kreditkarte erlangen.

🔍 **Echte Banken fragen Sie NIE telefonisch nach PINs, TANs oder Passwörtern!**

Microsoft-Support oder Tech-Firma

💻 Der Anrufer behauptet:

„Ihr Computer ist von Viren befallen. Wir helfen Ihnen bei der Reparatur. Bitte installieren Sie jetzt dieses Programm."

🎯 Ziel: Schadsoftware einschleusen oder Zugriff auf Ihren PC erhalten.

🔍 **Microsoft ruft niemanden von sich aus an – schon gar nicht auf Deutsch!**

Enkeltrick / Schockanrufe

👵 Betrüger geben sich als Enkel, Sohn oder Tochter aus – oft mit verstellter Stimme und unter Tränen:

„Oma, ich hatte einen schweren Unfall und brauche dringend Geld – bitte hilf mir!"

🎯 Ziel: Angst und Panik erzeugen, um zu einer Überweisung zu bewegen.

Gewinnspiel-Betrug

🎁 Sie sollen einen „großen Gewinn" gemacht haben – müssen aber vorab Gebühren zahlen.

🎯 Ziel: Geld kassieren, obwohl es nie einen Gewinn gibt.

🧠 Woran erkennen Sie betrügerische Anrufe?

Merkmal	Achtung bei…
Unbekannte Rufnummer	Besonders bei ausländischen oder unterdrückten Nummern
Zeitdruck oder Drohungen	„Handeln Sie jetzt, sonst wird gesperrt/verhaftet“
Ungewöhnliche Anforderungen	Geld überweisen, Software installieren, PIN am Telefon
Kein Rückruf möglich	Nummer ist später nicht erreichbar oder gibt es nicht
Viele persönliche Fragen	Nach Adresse, Geburtsdatum, Bankdaten, Zugangsdaten

☑ So reagieren Sie richtig bei einem verdächtigen Anruf

1. **Ruhe bewahren** – lassen Sie sich nicht unter Druck setzen.
2. **Keine persönlichen Daten preisgeben** – keine Passwörter, Kontodaten, TANs.
3. **Niemals Überweisungen tätigen** auf Anweisung eines Anrufers.
4. **Auflegen!** – höflich oder einfach kommentarlos.
5. **Nummer notieren** (falls sichtbar) und bei der **echten Polizei** oder **Bank** rückfragen.
6. **Melden** – z. B. bei der Polizei (110) oder über Portale wie **verbraucherzentrale.de**.

📌 Beispiel: Betrügerischer Anruf von „Bankmitarbeiter“

Anrufer: „Hier ist Herr Meier von Ihrer Sparkasse. Wir haben einen Sicherheitsvorfall auf Ihrem Konto festgestellt. Bitte lesen Sie mir Ihre TAN vor, damit ich die Transaktion blockieren kann.“

Richtiges Verhalten:

- Keine TAN nennen
- Sofort auflegen
- Offizielle Banknummer selbst raussuchen und zurückrufen

🧠 Merksatz:

Echte Behörden und Banken fordern am Telefon nie Ihre Zugangsdaten oder Geldtransfers!

Hinweis 17 Telefonbetrug

8.10. Wie funktioniert der Enkeltrick – am Telefon und über WhatsApp?

Der **Enkeltrick** ist eine besonders hinterhältige Betrugsmasche, bei der Betrüger gezielt ältere Menschen ansprechen, um ihnen unter einem Vorwand Geld zu entlocken. Ursprünglich fand der Enkeltrick fast ausschließlich **am Telefon** statt – heute nutzen Betrüger auch **Messenger-Dienste wie WhatsApp**.

🎭 **Wie läuft der klassische Enkeltrick am Telefon ab?**

1. **Anruf**:
   - Betrüger melden sich mit einer unsicheren oder undeutlichen Stimme.
   - Sie sagen nicht direkt ihren Namen, sondern warten, bis das Opfer rät:

„Rate mal, wer hier spricht!"
Opfer: „Bist du es, Peter?"
Täter: „Ja genau, Peter!"

2. **Notlüge**:
   - Der angebliche Enkel oder ein anderer Verwandter behauptet, dringend Geld zu benötigen:
     - Wegen eines **Unfalls**,
     - einer **Autoreparatur**,
     - oder **rechtlicher Probleme**.
3. **Druck und Geheimhaltung**:
   - Das Opfer wird gedrängt, schnell zu handeln („Sonst wird es schlimmer!") und niemandem etwas zu erzählen („Es soll eine Überraschung bleiben.").
4. **Geldübergabe**:
   - Ein Bote wird geschickt, um das Geld persönlich abzuholen – oft unter dem Vorwand: „Ich kann leider nicht selbst kommen."

📱 **Wie funktioniert der Enkeltrick über WhatsApp?**

Seit einigen Jahren wird der Enkeltrick auch über Messenger-Dienste wie **WhatsApp** durchgeführt.

🔔 **Typischer Ablauf:**

1. **Nachricht von einer unbekannten Nummer**:

„Hallo Oma, mein Handy ist kaputt, das ist meine neue Nummer!"

2. **Vortäuschen einer Notlage**:

„Ich muss dringend eine Rechnung überweisen, aber mein Online-Banking geht nicht."

3. **Aufforderung zur Überweisung**:
   - Betrüger bitten um **schnelle Hilfe** und senden eine **IBAN** (meist auf den Namen eines Dritten).
4. **Druck erzeugen**:

- „Bitte überweise noch heute, sonst gibt es große Probleme!“

🗣 Wie erkennen Sie den Enkeltrick?

Anzeichen	Erklärung
Unbekannte Nummer	Angeblicher Enkel schreibt oder ruft von fremder Nummer an.
Dringende Geldforderungen	Oft wird behauptet, sofort Geld zu brauchen.
Keine Rückrufmöglichkeit	„Kann gerade nicht telefonieren“ – ein beliebter Trick.
Geheimhaltung verlangt	„Bitte erzähl es niemandem!“ – Alarmstufe **Rot**!
Zeitdruck	„Muss noch heute überwiesen werden!“

☑ So schützen Sie sich und Ihre Familie

- **Immer nachfragen!**
  → Rückruf auf die alte, bekannte Nummer starten, nicht auf die neue Nummer antworten.
- **Misstrauisch bei neuen Handynummern sein!**
  → Immer persönlich verifizieren lassen.
- **Keine Geldübergabe an unbekannte Personen!**
- **Im Zweifel eine Vertrauensperson einschalten**
  → Kinder, Enkel oder Freunde fragen: „Ist da wirklich was dran?“
- **Die Polizei informieren**, wenn ein Betrugsversuch vorliegt. (Notruf 110)

Tipp: Vereinbaren Sie mit den Enkeln oder Kindern eine Sicherheitsfrage. Nur wenn der Anrufer oder angebliche Kontakt über WhatsApp oder andere Messenger Dienste die richtige Antwort weiß, können Sie sicher sein, dass es tatsächlich Ihr Enkel oder Kind ist.

Dabei sollten Sie darauf achten, dass die Antwort nicht leicht zu erraten ist, denn viele Angreifer nutzen die Sozialen Medien oder auch Künstliche-Intelligenz, um so an mögliche Informationen zu kommen. Besser ist es, wenn Frage und Antwort so gar nichts miteinander zu tun haben.

Beispiele:

Frage: Was ist Dein Lieblingsessen?

Antwort: New York

Frage: Was ist dein Spitzname

Antwort: Apfelstrudel

📌 Beispiel: Enkeltrick via WhatsApp

Nachricht:
"*Hallo Oma, ich hab mein Handy verloren. Hier ist meine neue Nummer. Kannst du mir schnell 1.800€ überweisen? Ich erkläre später alles. Hier die IBAN: DE89 3704 0044 0532 0130 00.*"

→ **Richtiges Verhalten**:

- Nicht überweisen.

- Die alte Nummer anrufen.
- Polizei informieren.

🧠 **Merksatz:**

„Bei Geldforderungen immer skeptisch bleiben – egal ob am Telefon oder per WhatsApp."

Hinweis 18 Enkeltrick

8.11. Fallbeispiel: Ein betrügerischer Anruf

Was ist passiert und wie hätte man sich schützen können?

Telefonbetrug ist eine der ältesten Maschen – doch sie ist heute raffinierter denn je. Gerade Senioren werden gezielt angerufen, weil Betrüger hoffen, auf Vertrauen oder Unsicherheit zu stoßen.

Hier ein echtes Beispiel:

🗂️ **Fallbeispiel: Der angebliche Bankmitarbeiter**

Herr Schmitt, 78 Jahre alt, wurde eines morgens angerufen. Am Telefon meldete sich ein **freundlicher Mann**, der sich als Mitarbeiter seiner Sparkasse vorstellte.

Er sagte:

"Guten Tag Herr Schmitt, wir haben ungewöhnliche Aktivitäten auf Ihrem Konto bemerkt. Zu Ihrer Sicherheit müssen wir Ihr Konto jetzt sofort schützen. Bitte nennen Sie mir Ihre Kontonummer und Ihr Online-Banking-Passwort."

Herr Schmitt erschrak. Er wollte nicht, dass sein Geld verloren geht, und gab – gutgläubig – seine Daten preis.

Was dann passierte:
Innerhalb weniger Minuten buchten die Betrüger mehrere tausend Euro von seinem Konto ab.
Als Herr Schmitt bei seiner echten Bank anrief, war es bereits zu spät.

🚨 **Wie arbeiten Telefonbetrüger?**

- Sie **geben sich als Polizisten, Bankmitarbeiter oder Verwandte** aus.
- Sie **bauen gezielt Stress und Druck auf** ("Sofort handeln!").

- Sie **fordern persönliche Daten oder Geldüberweisungen**.
- Oftmals wird sogar die **offizielle Telefonnummer der Bank oder Polizei gefälscht** („Call ID Spoofing"), sodass im Display scheinbar eine echte Nummer erscheint.

☑ **Wie hätte Herr Schmitt sich schützen können?**

1. Ruhe bewahren:

Echte Bankmitarbeiter oder Polizisten verlangen **niemals** am Telefon Ihre Zugangsdaten oder PIN-Nummern.

2. Auflegen und selbst anrufen:

Herr Schmitt hätte einfach auflegen und die **offizielle Nummer seiner Sparkasse** anrufen sollen – die Telefonnummer finden Sie immer auf Ihrer Bankkarte oder im Internet.

3. Niemals Daten am Telefon preisgeben:

Banken und Behörden klären Probleme **immer schriftlich** oder direkt vor Ort – niemals am Telefon.

4. Vertrauensperson einbeziehen:

Bei Unsicherheit: mit Kindern, Enkelkindern oder guten Freunden sprechen, bevor man handelt.

Hinweis 19 Betrügerische Anrufe

8.12. Welche Warnzeichen deuten auf Betrug oder Datendiebstahl hin?

Es ist wichtig, auf bestimmte Warnzeichen zu achten, die auf Betrug oder Datendiebstahl hinweisen könnten. Hier sind einige der häufigsten Anzeichen, die Ihnen helfen können, sich vor solchen Gefahren zu schützen:

Ungewöhnliche E-Mails oder Nachrichten

- **Warum ist das wichtig?** Betrüger nutzen oft E-Mails oder Nachrichten, um Sie zu täuschen und an Ihre persönlichen Daten zu kommen.
- **Warnzeichen:**

  - Die **E-Mail-Adresse** oder der **Absendername** sieht verdächtig aus (z. B. „support@facebook-security.com“ anstelle von „support@facebook.com“).
  - Die Nachricht enthält **dringende Aufforderungen**, z. B. „Dein Konto wird in Kürze gesperrt, klicke hier, um es zu sichern!“
  - Die Nachricht fordert Sie auf, **persönliche Informationen** wie Passwörter, Bankdaten oder Sozialversicherungsnummern preiszugeben.
  - **Rechtschreibfehler** oder **ungewöhnliche Formulierungen** im Text.
- **Beispiel:** Sie bekommen eine E-Mail, die behauptet, von Ihrer Bank zu sein und Sie auffordert, auf einen Link zu klicken, um Ihr Konto zu verifizieren. Dies könnte ein Phishing-Versuch sein.

Verdächtige Links oder Anhänge

- **Warum ist das wichtig?** Phishing-Angriffe oder Malware werden häufig über schadhafte Links und Anhänge verbreitet.
- **Warnzeichen:**
  - Ein Link, der Sie zu einer **falschen Webseite** führt, die ähnlich aussieht wie eine vertrauenswürdige Seite (z. B. eine gefälschte Bankseite).
  - Anhänge, die Sie nicht erwartet haben, insbesondere wenn sie eine Datei mit einer ungewöhnlichen Erweiterung (z. B. .exe, .zip) haben.
  - Der Link scheint **unlogisch** oder **komisch** zu sein, zum Beispiel eine URL mit vielen Zahlen und zufälligen Buchstaben.
- **Beispiel:** Sie bekommen eine SMS von „Deinem Mobilfunkanbieter“, die einen Link enthält, der Sie auffordert, ein Software-Update herunterzuladen. Der Link führt jedoch zu einer gefährlichen Seite, die Schadsoftware installiert.

Ungewöhnliche Aktivitäten auf Ihren Konten

- **Warum ist das wichtig?** Wenn jemand Zugriff auf Ihre Konten hat, könnte er unbefugte Aktivitäten durchführen.
- **Warnzeichen:**
  - Sie sehen **Käufe oder Zahlungen**, die Sie nicht getätigt haben, auf Ihrem **Bankkonto** oder Ihrer **Kreditkartenabrechnung**.
  - **Passwortänderungen** oder **Login-Versuche** aus ungewohnten Ländern oder Städten.
  - Sie bekommen plötzlich **Benachrichtigungen** über Aktivitäten, die Sie nicht selbst durchgeführt haben (z. B. ein Login auf deinem **Google-Konto** von einem anderen Gerät).
- **Beispiel:** Sie sehen auf Ihrem Kontoauszug eine Abbuchung von einem Online-Shop, bei dem Sie nie eingekauft haben. Das könnte ein Hinweis darauf sein, dass jemand Ihre Kreditkartendaten gestohlen hat.

Angebote, die zu gut sind, um wahr zu sein

- **Warum ist das wichtig?** Betrüger locken Sie häufig mit unrealistisch guten Angeboten, um Sie in eine Falle zu locken.
- **Warnzeichen:**
    - Sie bekommen **Werbeanrufe** oder **Nachrichten**, die Ihnen etwas **kostenlos** oder zu einem ausgesprochen niedrigen Preis anbieten, z. B. ein teures Produkt für nur einen Bruchteil des Preises.
    - **„Gewinnspiele"** oder **„Preisausschreiben"**, bei denen Sie etwas gewinnen sollen, aber Ihre **Kontodaten** oder eine **Zahlung** verlangen.
- **Beispiel:** Sie erhalten eine Nachricht, die Ihnen mitteilt, dass Sie ein teures Smartphone gewonnen haben, aber um den Gewinn zu bestätigen, müssen Sie zuerst eine kleine Gebühr bezahlen. Dies ist ein typisches Zeichen für einen Betrug.

Ungewöhnliche Anrufe oder Nachrichten von „Bekannten"

- **Warum ist das wichtig?** Betrüger geben sich oft als Bekannte oder vertrauenswürdige Personen aus, um Sie zu täuschen.
- **Warnzeichen:**
    - Sie erhalten einen Anruf oder eine Nachricht von jemandem, der vorgibt, ein Freund, ein Familienmitglied oder ein Kollege zu sein, aber etwas merkwürdig wirkt (z. B. sie bitten Sie um Geld oder eine schnelle Handlung).
    - Es wird nach **persönlichen Informationen** gefragt, z. B. nach Ihren **Geburtsdatum**, **Bankdaten** oder **Passwörtern**.
- **Beispiel:** Sie bekommen einen Anruf von einem „Freund", der angeblich in Schwierigkeiten ist und schnell Geld von Ihnen braucht. Es könnte sein, dass die Nummer Ihres Freundes gehackt wurde und ein Betrüger Sie in eine Falle locken möchte.

Forderungen nach sofortiger Zahlung oder persönlicher Information

- **Warum ist das wichtig?** Betrüger setzen Sie oft unter Druck, schnell zu handeln, damit Sie nicht genug Zeit haben, um zu prüfen, ob die Anfrage echt ist.
- **Warnzeichen:**
    - Sie werden aufgefordert, **sofort zu zahlen**, zum Beispiel für eine **Steuerrechnung**, **Strafzettel** oder ein **gewonnenes Preisgeld**, dass Sie nicht erwartet haben.
    - Die Nachricht oder der Anruf sagt, dass Ihre **Kreditkarteninformationen** oder **Bankverbindung** angeben müssen, um „Probleme zu vermeiden".
- **Beispiel:** Sie bekommen eine E-Mail, die vorgibt, vom **Finanzamt** zu kommen und Ihnen mitteilt, dass Sie eine Strafe zahlen müssen, weil Sie „Steuern hinterzogen haben", mit der Aufforderung, sofort zu bezahlen, sonst gäbe es „ernste Konsequenzen". Dies ist höchstwahrscheinlich ein Betrug.

Mangel an Kontaktmöglichkeiten oder schlechten Support

- **Warum ist das wichtig?** Seriöse Unternehmen bieten klare Kontaktmöglichkeiten und guten Kundenservice. Wenn Sie bei einem Anbieter keine Möglichkeit finden, jemanden zu erreichen, ist das ein Warnsignal.
- **Warnzeichen:**
  - Es gibt keine **Telefonnummer**, **E-Mail-Adresse** oder **Adresse** auf der Website oder in der Nachricht.
  - **Kundenbewertungen** oder **Foren** berichten über **schlechten oder keinen Support**.
- **Beispiel:** Sie bestellen etwas von einer Website, aber die Webseite enthält keine gültigen Kontaktinformationen, und Sie können den Kundenservice nicht erreichen, um nach Ihrer Bestellung zu fragen.

Fazit:

- **Betrug und Datendiebstahl** beginnen oft mit merkwürdigen Nachrichten, verdächtigen Links oder auffälligen Angeboten. Bleiben Sie immer wachsam und hinterfragen ungewöhnliche Aufforderungen oder Anfragen.
- **Reagieren Sie schnell:** Wenn Sie ein Warnzeichen entdecken, ändern Sie sofort Ihre Passwörter und kontaktieren den Kundenservice oder die Bank, wenn nötig.

Achten Sie auf diese Anzeichen und seien Sie vorsichtig, um sich vor Betrug und Datendiebstahl zu schützen!

8.13. Was sollte ich beim Umgang mit sozialen Netzwerken beachten?

Der Umgang mit sozialen Netzwerken wie **Facebook**, **WhatsApp** und anderen sollte sorgfältig und sicher erfolgen, besonders wenn es um den Schutz Ihrer persönlichen Daten und Ihre Privatsphäre geht. Hier sind einige wichtige Punkte, die Sie beachten sollten:

1. Datenschutz-Einstellungen regelmäßig überprüfen

- **Warum ist das wichtig?** Viele soziale Netzwerke sammeln eine Menge Daten über Sie. Sie können in den Einstellungen festlegen, welche Informationen Sie mit anderen teilen möchten und welche nicht.
- **Beispiel:** Auf **Facebook** können Sie in den **Privatsphäre-Einstellungen** festlegen, wer Ihre Beiträge sehen darf, wer Ihnen Nachrichten schicken kann und ob Suchmaschinen Ihr Profil finden können. Überprüfen Sie diese Einstellungen regelmäßig, um sicherzustellen, dass nur die Personen Zugang zu Ihren Informationen haben, die Sie möchten.

2. Persönliche Informationen sparsam teilen

- **Warum ist das wichtig?** Je weniger persönliche Informationen Sie online teilen, desto sicherer sind Sie vor potenziellen Gefahren wie Betrug oder Identitätsdiebstahl.
- **Beispiel:** Achten Sie darauf, dass Sie auf **WhatsApp** keine vertraulichen Informationen wie deine Bankdaten, Passwörter oder anderen persönlichen Daten teilen, auch nicht in privaten Nachrichten. Denken Sie daran, dass die Daten, die Sie teilen, auch von anderen Personen weitergegeben werden könnten.
- **Anmerkung:** Geben Sie Ihren vollen Namen, gegebenenfalls den Wohnort, in eine Suchmaschine ein, und kontrollieren Sie die Ergebnisse.

3. Alternative Suchmaschinen

Ist Ihnen schon aufgefallen, dass Ihre Suchanfragen mit Google Ihnen eine vermehrte Werbung in den sozialen beschert? Dies liegt daran, dass Google diese Informationen an andere Betreiber im Internet verkauft. Doch dies können Sie ganz einfach abstellen. Verwenden Sie eine dieser Alternativen Suchmaschinen:

Startpage: Server in den Niederlanden, nutzt anonymisierte Google-Suchergebnisse, speichert keine IP-Adressen. [https://www.startpage.com/de/]

DuckDuckGo: US-Anbieter mit klarer Datenschutzpolitik, keine Nutzerverfolgung oder personalisierte Werbung. [https://duckduckgo.com/]

MetaGer: Aus Deutschland, betreibt eigene Crawler, kombiniert mehrere Quellen, komplett anonym nutzbar. [https://metager.de/]

Qwant: Aus Frankreich, verfolgt keine Nutzeraktivitäten, eigene Suchtechnologie. [https://www.qwant.com/]

Mojeek: britischer Anbieter mit eigenem Index, ohne Tracking oder Profilbildung. [https://www.mojeek.com/]

Swisscows: Aus der Schweiz, sicherheitsorientiert, speichert keine personenbezogenen Daten, familienfreundliche Filter. [https://www.mojeek.com/]

Suchmaschine	Herkunft	Datenschutz	Besonderheiten
Google	USA	Speichert Daten, personalisierte Werbung	Sehr schnell, liefert personalisierte Ergebnisse
Startpage	Niederlande	Sehr hoch – anonymisierte Google-Suche	Keine Speicherung von IP-Adressen, vertraut, EU-basiert
Duck-DuckGo	USA	Hoch – keine Nachverfolgung	Klar verständliche Datenschutzrichtlinie, keine Nutzerprofile
MetaGer	Deutschland	Sehr hoch – gemeinnützig, anonym	Eigene Server in Deutschland, Open Source
Qwant	Frankreich	Hoch – keine Nutzerverfolgung	Kindersuchfunktion, modern gestaltete Oberfläche
Mojeek	Großbritannien	Hoch – eigener Index, kein Tracking	Keine Werbung, konsequent unabhängig
Swisscows	Schweiz	Sehr hoch – keine Datenspeicherung	Familienfreundlich, Server in der Schweiz

Hinweis 20 Suchmaschinen Alternative

Anleitungen zum Einstellen der Suchmaschine finden Sie für Ihren Browser unter den nachfolgenden Links:

Microsoft Edge:

- Öffnen Sie Microsoft Edge.
- Klicken Sie oben rechts auf das Drei-Punkt-Menü (⋯) und wählen **Einstellungen**.
- Navigieren Sie zu **Datenschutz, Suche und Dienste**.

- Scrollen Sie nach unten zu **Adressleiste und Suche**.
- Wählen Sie unter **In Adressleiste verwendete Suchmaschine** Ihre bevorzugte Suchmaschine aus.

Mozilla Firefox

- Öffnen Sie Firefox.
- Klicken Sie oben rechts auf das Drei-Strich-Menü (≡) und wählen Sie **Einstellungen**.
- Gehen Sie zum Abschnitt **Suche**.
- Unter **Standardsuchmaschine** können Sie Ihre bevorzugte Suchmaschine auswählen.

Google Chrome

- Öffnen Sie Google Chrome.
- Klicken Sie oben rechts auf das Drei-Punkt-Menü (⋮) und wählen Sie **Einstellungen**.
- Im Abschnitt **Suchmaschine** können Sie eine andere Suchmaschine auswählen oder eine neue hinzufügen.

Safari (iPhone, iPad oder Mac)

- Öffnen Sie Safari.
- Klicken Sie in der Menüleiste auf **Safari** und wählen Sie **Einstellungen**.
- Gehen Sie zum Tab **Suchen**.
- Wählen Sie im Dropdown-Menü neben **Suchmaschine** Ihre bevorzugte Option aus.

4. Achten Sie auf Phishing-Nachrichten

- **Warum ist das wichtig?** Phishing ist eine Methode, mit der Betrüger versuchen, Ihre persönlichen Daten oder Passwörter zu stehlen, indem sie sich als vertrauenswürdige Quelle ausgeben.

- **Beispiel:** Seien Sie vorsichtig bei Nachrichten, die Sie auffordern, auf einen Link zu klicken oder persönliche Informationen einzugeben, selbst wenn sie von einem Freund oder einer bekannten Person zu kommen scheinen. Oft wird der Absender gehackt und sendet betrügerische Nachrichten.

4. Vermeiden Sie das Akzeptieren von Freundschaftsanfragen oder Nachrichten von Unbekannten

- **Warum ist das wichtig?** Manchmal versuchen Betrüger oder unseriöse Personen, über soziale Netzwerke Kontakt zu Ihnen aufzunehmen, um Ihnen schadhafte Links zu senden oder Sie zu betrügen.

- **Beispiel:** Wenn Ihnen jemand auf **Facebook** eine Freundschaftsanfrage schickt, den Sie nicht kennen, seien Sie vorsichtig. Akzeptieren Sie keine Anfragen von unbekannten Personen und öffnen keine Links oder Anhänge in Nachrichten, die Sie nicht erwarten.

5. Gruppen- und Chat-Einstellungen anpassen

- **Warum ist das wichtig?** In vielen sozialen Netzwerken können Sie einstellen, wer in Ihre Gruppen oder Chats hineinschauen kann. So verhindern Sie, dass Fremde Zugriff auf private Inhalte haben.

- **Beispiel:** Auf **WhatsApp** können Sie Ihre Gruppen so einstellen, dass nur bestimmte Personen Sie zu einer Gruppe hinzufügen können. Auf **Facebook** können Sie entscheiden, wer in privaten Gruppen Beiträge sehen kann, und Sie können auch die Mitglieder einer Gruppe kontrollieren.

6. Seien Sie vorsichtig mit dem Teilen von Bildern und Videos

- **Warum ist das wichtig?** Bilder und Videos können oft mehr über Sie preisgeben, als Sie denken. Überlegen Sie immer, ob Sie möchten, dass andere Personen diese Inhalte sehen.
- **Beispiel:** Wenn Sie ein Bild von Ihnen im Urlaub postest, achten Sie darauf, dass keine persönlichen Informationen (z. B. Ihre Adresse oder genaue Aufenthaltsorte) darauf sichtbar sind. Vermeiden Sie auch, Bilder von anderen Personen, ohne deren Zustimmung zu posten.

7. Vermeiden Sie das Teilen von zu vielen Details

- **Warum ist das wichtig?** Zu viele Details über Ihren Alltag oder Ihren Standort können von unbefugten Personen für betrügerische Zwecke genutzt werden.
- **Beispiel:** Wenn Sie in den sozialen Netzwerken schreiben, dass Sie gerade im Urlaub sind, können Kriminelle dies ausnutzen, um Ihr Zuhause auszurauben. Es ist besser, diese Informationen erst zu teilen, wenn Sie wieder zu Hause sind.

8. Vorsicht bei App-Berechtigungen

- **Warum ist das wichtig?** Viele soziale Netzwerke und Apps fragen nach Berechtigungen, um auf Daten auf Ihrem Gerät zuzugreifen (z. B. Kontakte, Fotos, Standort). Sie sollten genau überlegen, ob eine App wirklich diese Berechtigungen benötigt.
- **Beispiel:** Wenn Sie eine neue **WhatsApp**-Version installieren, fragt die App möglicherweise nach Berechtigungen für den Zugriff auf Ihren Standort oder Ihre Kontakte. Stellen Sie sicher, dass Sie nur die Berechtigungen gewähren, die notwendig sind.

9. Sicherheitsfunktionen wie Zwei-Faktor-Authentifizierung (2FA) aktivieren

- **Warum ist das wichtig?** Zwei-Faktor-Authentifizierung fügt eine zusätzliche Sicherheitsebene hinzu, sodass niemand Ihr Konto ohne Ihr Einverständnis aufrufen kann, selbst wenn er Ihr Passwort kennt.
- **Beispiel: Facebook** und **WhatsApp** bieten beide die Möglichkeit, 2FA zu aktivieren. Das bedeutet, dass Sie zusätzlich zu Ihrem Passwort einen Code eingeben müssen, der Ihnen auf Ihr Handy gesendet wird.

10. Seien Sie vorsichtig bei Gewinnspielen und zu guten Angeboten

- **Warum ist das wichtig?** Viele Betrüger bieten in sozialen Netzwerken „Gewinnspiele" oder „Angebote" an, um an Ihre persönlichen Informationen zu kommen.
- **Beispiel:** Wenn Sie ein Gewinnspiel auf **Facebook** sehen, bei dem Sie persönliche Daten eingeben müssen, seien Sie vorsichtig. Seriöse Gewinnspiele verlangen oft keine sensiblen Informationen wie deine Bankdaten.

11. Überlege, was du über andere teilst

- **Warum ist das wichtig?** Es ist nicht nur wichtig, auf Ihre eigene Privatsphäre zu achten, sondern auch darauf, wie Sie Informationen über andere teilen.

- **Beispiel:** Posten Sie keine privaten Informationen über andere Menschen (z. B. Telefonnummern oder private Gespräche), ohne deren Erlaubnis. Achten Sie auch darauf, dass Sie keine Fotos von anderen teilen, wenn sie nicht einverstanden sind.

12. Regelmäßig überprüfen, wer Ihnen folgt oder wer auf Ihre Inhalte zugreift

- **Warum ist das wichtig?** Indem Sie überprüfen, wer Ihre Inhalte sehen kann, behalten Sie die Kontrolle über Ihre Online-Präsenz.
- **Beispiel:** Überprüfen Sie regelmäßig die **Freundesliste** auf **Facebook** und die **Kontakte** auf **WhatsApp**, um sicherzustellen, dass Sie nur mit vertrauenswürdigen Personen verbunden sind.

Zusammenfassung:

- **Schützen Sie Ihre Privatsphäre**: Überprüfen Sie die Datenschutz-Einstellungen regelmäßig und teilen Sie nicht zu viele persönliche Informationen.
- **Seien Sie vorsichtig mit unbekannten Personen**: Akzeptieren Sie keine Freundschaftsanfragen von Fremden und öffnen keine verdächtigen Links.
- **Schützen Sie Ihre Daten**: Verwenden Sie Sicherheitsfunktionen wie Zwei-Faktor-Authentifizierung und achten auf die Berechtigungen von Apps.
- **Vermeiden Sie Betrug**: Seien Sie vorsichtig bei zu guten Angeboten oder Gewinnspielen.

Mit diesen einfachen Tipps können Sie sicher und geschützt in sozialen Netzwerken unterwegs sein.

9. Einstellungen auf den Geräten

9.1. Welche Einstellungen auf den Geräten erhöhen die Sicherheit

Automatische Updates aktivieren

- **Warum ist das wichtig?** Updates helfen, das Gerät sicher zu halten, weil sie Schwachstellen schließen, die von Hackern ausgenutzt werden könnten.
- **Beispiel:** Wenn Sie ein **Smartphone** oder **Tablet** haben, stellen Sie sicher, dass Sie die **automatischen Updates** für Ihr Betriebssystem und Ihre Apps aktiviert haben. So müssen Sie sich nicht selbst darum kümmern und bekommen immer die neuesten Sicherheitsfunktionen.

Starke Passwörter benutzen

- **Warum ist das wichtig?** Ein sicheres Passwort schützt Ihr Gerät und Ihre Konten vor unbefugtem Zugriff.
- **Beispiel:** Anstatt einfache Passwörter wie „1234“ oder „password“ zu verwenden, wählen Sie ein Passwort, das aus Buchstaben, Zahlen und Sonderzeichen besteht, z. B. „Sonnenschein2025!“.
- **Tipp:** Sie können sich ein Passwort merken, das für Sie persönlich wichtig ist, aber schwer zu erraten ist. Oder nutzen eine **Passwort-App**, die Ihnen hilft, sichere Passwörter zu erstellen.

Zwei-Faktor-Authentifizierung (2FA) aktivieren

- **Warum ist das wichtig?** Zwei-Faktor-Authentifizierung bedeutet, dass Sie sich zusätzlich zu Ihrem Passwort noch mit einem zweiten Code anmelden müssen. Dieser Code wird oft per SMS oder über eine App an Sie geschickt.
- **Beispiel:** Bei **Google** oder **Facebook** können Sie 2FA aktivieren. Wenn Sie sich dann das nächste Mal anmelden, geben Sie Ihr Passwort ein und bekommen noch einen Code auf Ihr Handy, das Sie eingeben.

Gerät verschlüsseln

- **Warum ist das wichtig?** Wenn Ihr Gerät gestohlen wird, kann niemand Ihre Daten lesen, wenn die Verschlüsselung aktiviert ist.
- **Beispiel:** Auf **iPhones** ist die Verschlüsselung standardmäßig aktiviert. Bei **Android-Geräten** können Sie die Verschlüsselung unter den Einstellungen aktivieren, damit Ihre Daten sicher sind.

Automatische Sperre des Geräts aktivieren

- **Warum ist das wichtig?** So wird Ihr Gerät gesperrt, wenn du es eine Zeit lang nicht benutzt. Das schützt Ihre Daten, falls Sie das Gerät aus Versehen unbeaufsichtigt lassen.
- **Beispiel:** Sie können einstellen, dass sich Ihr **Handy** nach 1 oder 2 Minuten ohne Benutzung automatisch sperrt. Um es wieder zu benutzen, müssen Sie ein Passwort oder deinen Fingerabdruck eingeben.

Verwendung von Antiviren-Software

- **Warum ist das wichtig?** Diese Software hilft dabei, gefährliche Apps oder Programme zu finden, die Ihr Gerät schädigen könnten.
- **Beispiel:** Auf Android-Geräten gibt es kostenlose Antiviren-Apps wie „Avast" oder „Kaspersky", die Sie einfach herunterladen und regelmäßig laufen lassen können, um sicher zu bleiben.

Bluetooth und WLAN sicher nutzen

- **Warum ist das wichtig?** Öffentliche WLAN-Netze oder Bluetooth können leicht von anderen Personen genutzt werden, wenn sie nicht richtig gesichert sind.
- **Beispiel:** Wenn Sie in einem Café sind und das WLAN nutzen, sollten Sie lieber ein **VPN** (virtuelles privates Netzwerk) verwenden, um Ihre Verbindung sicherer zu machen.
- **Tipp:** Stellen Sie sicher, dass **Bluetooth** nur aktiviert ist, wenn Sie es tatsächlich brauchen, und dass Sie Ihr Gerät nicht einfach mit anderen Geräten verbinden, ohne sie zu überprüfen.

Berechtigungen für Apps kontrollieren

- **Warum ist das wichtig?** Manche Apps fragen nach Zugriff auf Ihre Kamera, Mikrofon oder Ihren Standort, obwohl sie das nicht wirklich brauchen.
- **Beispiel:** Wenn Sie eine neue App herunterladen, prüfen Sie, ob sie wirklich Zugriff auf Ihre Kamera oder Ihren Standort brauchen. Wenn nicht, lehnen Sie den Zugriff ab.

Regelmäßige Backups machen

- **Warum ist das wichtig?** So können Sie Ihre Fotos, Kontakte und andere Daten wiederherstellen, wenn etwas mit Ihrem Gerät passiert.
- **Beispiel:** Wenn Sie ein iPhone haben, können Sie Ihre Daten ganz einfach über **iCloud** sichern. Auf Android können Sie die **Google Drive**-Sicherung aktivieren, damit Ihre Daten immer sicher sind.

WLAN richtig einrichten

- **Warum ist das wichtig?** Ihr WLAN-Router ist wie eine Tür zu Ihrem Zuhause im Internet. Wenn er nicht sicher ist, können Unbefugte auf Ihr Internet zugreifen.
- **Beispiel:** Achten Sie darauf, dass Ihr WLAN-Passwort lang und sicher ist. Nutzen Sie die WPA3-Verschlüsselung, wenn Ihr Router dies unterstützt. Das schützt Sie vor Fremdzugriff.

Diese einfachen Schritte helfen Ihnen dabei, Ihr Gerät sicherer zu machen und Sie vor möglichen Gefahren zu schützen. Sicherheit muss nicht kompliziert sein, und ein paar einfache Anpassungen machen schon einen großen Unterschied!

9.2. Wie schütze ich…?

…meinen PC, mein Smartphone oder Tablet vor Viren und Betrug?

Unsere Geräte – egal ob Computer, Smartphone oder Tablet – enthalten viele persönliche Daten. Deshalb sind sie beliebte Angriffsziele für Kriminelle. Ein guter Schutz ist einfach umzusetzen und schützt vor großem Schaden.

🚨 **Typische Bedrohungen:**

- **Viren und Trojaner**: Schadprogramme, die Daten stehlen oder Geräte sperren.
- **Phishing-Apps und gefälschte Webseiten**: Sie locken zur Eingabe von Passwörtern oder Kontodaten.
- **Betrügerische Nachrichten (SMS, E-Mail, WhatsApp)**: Sie enthalten schädliche Links oder Anhänge.

☑ **Wichtige Schutzmaßnahmen:**

1. Aktuelle Software verwenden:

Regelmäßige Updates für Betriebssysteme und Apps schließen Sicherheitslücken.

2. Virenschutzprogramme installieren:

Sowohl für PCs als auch für Smartphones gibt es wirksame Schutzprogramme, z. B. von Avira, Kaspersky oder Bitdefender.

3. Nur vertrauenswürdige Apps installieren:

Apps nur aus offiziellen Stores wie dem **Google Play Store** oder **Apple App Store** herunterladen.

4. Keine unbekannten Anhänge öffnen:

E-Mails oder Nachrichten von unbekannten Absendern sollten ignoriert werden – auch wenn sie seriös wirken!

5. Geräte mit Passwort, PIN oder Fingerabdruck sichern:

Eine Bildschirmsperre schützt, falls das Gerät verloren geht.

6. Regelmäßig Backups machen:

Sichern Sie Ihre wichtigen Daten auf einer externen Festplatte oder in einer sicheren Cloud.

🗂 **Fallbeispiel: Schadsoftware auf dem Smartphone**

Frau Müller, 74 Jahre alt, erhielt eine SMS:

"Ihr Paket wurde nicht zugestellt. Bitte klicken Sie hier zur Nachverfolgung."

Sie klickte auf den Link und installierte eine App. Ergebnis: Ihr Smartphone wurde mit einer Schadsoftware infiziert, die ihre Bankdaten ausspähte. Glücklicherweise bemerkte ihre Bank die ungewöhnlichen Überweisungen frühzeitig.

Wie hätte sie sich schützen können?

- Keine Links aus unbekannten Nachrichten anklicken.
- Im Zweifelsfall die Paketdienste selbst über deren offizielle Website kontaktieren.
- Ein aktuelles Virenschutzprogramm hätte die App erkannt und blockiert.

📦 **Merk Tipp: 5 goldene Regeln für Ihre Gerätesicherheit**

- Immer Updates durchführen 🔄

- Virenschutz aktivieren 🛡️
- Nur Apps aus offiziellen Quellen laden 📱
- Keine unbekannten Links anklicken 🚫
- Geräte mit Passwort oder Fingerabdruck sichern 🔐

📚 **Quellen:**

- Bundesamt für Sicherheit in der Informationstechnik (BSI): bsi-fuer-buerger.de
- Polizei-Beratung: polizei-beratung.de

9.3. Sicherheits-Checkliste: Bin ich gut geschützt?

Mit dieser Checkliste können Sie selbst schnell überprüfen, wie sicher Sie im Internet und auf Ihrem Gerät unterwegs sind. Haken Sie einfach die Punkte ab, Sie auf dich zutreffen!

Habe ich sichere Passwörter?

- Meine Passwörter sind **lang** (mindestens 8 Zeichen).
- Ich verwende **Groß- und Kleinbuchstaben**, **Zahlen** und **Sonderzeichen** (z.B. *, !, #).
- Für **jedes Konto** (E-Mail, Bank, Online-Shops) nutze ich **ein anderes Passwort**.

Nutze ich eine Zwei-Faktor-Authentifizierung?

- Bei wichtigen Konten (z.B. Bank, E-Mail) habe ich eine zusätzliche **Sicherheitsabfrage** eingerichtet: (Zum Beispiel einen Code, der per SMS geschickt wird.)

Sind meine Geräte aktuell?

- Mein Smartphone, Tablet oder Computer installiert **regelmäßig Updates**.
- Ich habe **automatische Updates** eingeschaltet.

Habe ich einen Virenschutz?

- Auf meinem Gerät läuft ein **Antivirenprogramm** oder eine **Sicherheits-App**.
- Ich lasse ab und zu einen **Sicherheits-Scan** laufen.

Klicke ich vorsichtig auf Links?

- Ich öffne **nur Links** aus vertrauenswürdigen Nachrichten oder Webseiten.
- Ich klicke nicht auf **unbekannte Anhänge** oder **merkwürdige Angebote**.

Prüfe ich unbekannte Kontakte?

- Ich überprüfe Freundschaftsanfragen oder Nachrichten von Fremden in sozialen Netzwerken.
- Ich gebe **keine persönlichen Daten** (Adresse, Kontonummer) an Unbekannte weiter.

Nutze ich sichere WLAN-Verbindungen?

- Zuhause ist mein WLAN mit einem **eigenen Passwort** geschützt (nicht das Standardpasswort).
- In Cafés oder Hotels benutze ich möglichst **keine sensiblen Dienste** (z.B. Online-Banking).

Habe ich wichtige Daten gesichert?

- Ich habe eine **Sicherungskopie** (Backup) meiner wichtigsten Dateien auf einem USB-Stick oder in der Cloud.

Achte ich auf verdächtige Aktivitäten?

- Ich kontrolliere regelmäßig meine **Bankabrechnungen** und **E-Mails** auf Unregelmäßigkeiten.
- Ich reagiere schnell, wenn ich ungewöhnliche Bewegungen feststelle.

Habe ich eine Notfall-Checkliste griffbereit?

- Ich weiß, was ich tun muss, falls ich Opfer eines Betrugs werde (z. B. Passwörter ändern, Bank kontaktieren, Polizei informieren).

→ Wenn Sie alle oder fast alle Punkte abhaken können, sind Sie schon sehr gut geschützt!

9.4. Was tun im Notfall? – Erste Hilfe bei Betrugsverdacht

Wenn Sie den Verdacht haben, Opfer eines Betrugs geworden zu sein oder dass jemand Ihre Daten gestohlen hat, ist schnelles Handeln besonders wichtig. Hier finden Sie eine einfache Schritt-für-Schritt-Anleitung für den Notfall – klar und verständlich erklärt.

1. Ruhe bewahren

- **Warum das wichtig ist:** In einem Notfall ist es leicht, panisch zu werden. Aber: Mit einem kühlen Kopf können Sie am besten reagieren.
- **Tipp:** Atmen Sie tief durch und arbeiten die folgenden Schritte in Ruhe durch – Sie sind nicht allein!

2. Passwörter sofort ändern

- **Warum das wichtig ist:** Wenn jemand Ihre Daten gestohlen hat, kann er sich mit Ihrem Passwort in Ihre Konten einloggen. Ein neues Passwort blockiert den Zugriff.
- **Was tun:**
  - Ändern Sie zuerst Ihr Passwort bei der betroffenen Seite (z. B. Facebook, E-Mail oder Online-Banking).
  - Verwenden Sie ein **sicheres Passwort**: mindestens 8 Zeichen, am besten mit Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
- **Beispiel:** Statt „Geburtstag123“ lieber: „Gebi!2024Haus*“

3. Bank oder Sparkasse informieren

- **Warum das wichtig ist:** Wenn Sie befürchten, dass Ihre **Konto- oder Kartendaten** gestohlen wurden, kann Ihre Bank sofort Maßnahmen ergreifen.

- **Was tun:**
  - Rufen Sie die **Notfallnummer deiner Bank** an (auf der Rückseite deiner Bankkarte).
  - Bitten Sie darum, Ihr Konto **vorübergehend zu sperren**, um Schaden zu vermeiden.
  - Lassen Sie **unberechtigte Abbuchungen prüfen** oder rückgängig machen.

4. Gerät überprüfen oder Hilfe holen

- **Warum das wichtig ist:** Wenn Sie auf einen verdächtigen Link geklickt oder eine gefährliche Datei geöffnet haben, könnte Ihr Gerät (Smartphone, Tablet oder PC) infiziert sein.
- **Was tun:**
  - Starten Sie einen **Virenscan**, wenn Sie ein Antivirenprogramm haben.
  - Oder: Lassen Sie Ihr **Gerät** von jemandem **überprüfen**, dem Sie vertrauen (z. B. Enkel, Nachbarn, Fachgeschäft).
  - In schweren Fällen kann eine **Neuinstallation** des Geräts notwendig sein – lieber auf Nummer sicher gehen.

5. Polizei oder Verbraucherzentrale informieren

- **Warum das wichtig ist:** Bei Betrug oder Betrugsversuch sollten Sie den Vorfall melden – damit Sie rechtlich abgesichert sind und andere gewarnt werden können.
- **Was tun:**
  - Wenden Sie sich an die **Polizei vor Ort** oder rufe die **110**, wenn Sie sich dich bedroht fühlen.
  - Sie können den Betrug auch online bei der Polizei melden: z. B. über die Webseite der **Online-Wache** in Ihrem Bundesland.
  - Alternativ hilft auch die **Verbraucherzentrale** bei der Einschätzung und weiteren Schritten.

6. Zugang sperren lassen (z. B. SIM-Karte oder Online-Konto)

- **Warum das wichtig ist:** Wenn Ihr **Smartphone** oder Ihr **Online-Konto** betroffen ist, sollten Sie es vorübergehend sperren lassen.
- **Was tun:**
  - Bei **WhatsApp oder Facebook**: Melden Sie Ihr Konto als gehackt und lassen es sperren.
  - Bei **Mobilfunkanbietern**: SIM-Karte sperren lassen, falls Sie verdächtige SMS bekommen oder Ihr Handy verloren haben.

7. Angehörige informieren

- **Warum das wichtig ist:** Betrüger versuchen manchmal, auch Ihr Umfeld zu täuschen – zum Beispiel über gehackte Konten.
- **Was tun:**

- Informieren Sie Ihre **Kinder, Enkel oder Freunde**, dass dein Konto oder Gerät betroffen sein könnte.
- Bitten Sie sie, **keine verdächtigen Nachrichten oder Geldanfragen** von Ihnen zu öffnen.

8. Anzeige bei Betrugsplattformen melden

- **Warum das wichtig ist:** Plattformen wie Facebook, eBay oder Amazon haben eigene Möglichkeiten, Betrug zu melden.
- **Was tun:**
  - Suchen Sie auf der Webseite nach dem Bereich **„Hilfe" oder „Sicherheit"**.
  - Dort finden Sie meist einen Button „Problem melden" oder „Betrug melden".
  - Melden Sie dort den Vorfall – so kann die Plattform den Betrüger sperren.

Zusätzlicher Tipp: Eine Checkliste auf Papier

Viele Seniorinnen und Senioren fühlen sich sicherer, wenn sie im Notfall eine

Checkliste zum Abhaken zu Hause haben.

Hier ein Beispiel:

☑ **1. Ruhig bleiben und tief durchatmen**

→ Keine hektischen Entscheidungen treffen.

☑ **2. Passwörter sofort ändern**

→ Wichtig: Besonders für E-Mail, Bankkonto und soziale Netzwerke.

☑ **3. Bank oder Sparkasse informieren**

→ Karte oder Konto sperren lassen, unberechtigte Abbuchungen melden.

☑ **4. Gerät auf Viren überprüfen oder Hilfe holen**

→ Antiviren-Programm nutzen oder Fachmann/-frau um Hilfe bitten.

☑ **5. Polizei oder Verbraucherzentrale benachrichtigen**

→ Vorfall melden, Anzeige erstatten, falls nötig.

☑ **6. Online-Konten sperren oder sichern**

→ Beispielsweise WhatsApp, Facebook oder E-Mail-Konto.

☑ **7. Familie und Freunde informieren**

→ Warnen, dass keine verdächtigen Nachrichten geöffnet werden sollen.

☑ **8. Betrugsversuch bei der jeweiligen Plattform melden**

→ Etwa bei Facebook, Amazon, eBay oder anderen.

☑ 9. Wichtige Unterlagen sichern

→ Nachrichten, E-Mails oder Screenshots aufbewahren – sie helfen bei der Anzeige.

☑ 10. Zukünftig besonders vorsichtig sein

→ Nie auf unbekannte Links klicken oder persönliche Daten leichtfertig herausgeben.

💡 Tipp:

Diese Liste können Sie ausdrucken und in der Nähe Ihres Computers oder Telefons aufbewahren. Im Ernstfall haben Sie sofort einen klaren Plan!

10. Nützliche Links, Telefonnummern und weitere Hilfsangebote

Manchmal braucht man bei Problemen oder Fragen schnelle Unterstützung. Hier finden Sie eine Übersicht mit wichtigen Telefonnummern, Webseiten und Anlaufstellen, die Ihnen im Notfall oder bei Unsicherheiten helfen können.

☎ Wichtige Telefonnummern

Polizei – Notruf:

- 📞 110 → Bei akuten Betrugsfällen oder Bedrohung immer die Polizei rufen!

Sperr-Notruf für Bankkarten und Kreditkarten:

- 📞 116 116 (kostenfrei, rund um die Uhr) → Wenn Sie Ihre Bankkarte, Kreditkarte oder dein Online-Banking sperren lassen musst.

Verbraucherzentrale:

- 📞 Beratungstelefon Verbraucherschutz (regional unterschiedlich) → Hier bekommen Sie Rat bei Betrug, Abzocke oder unseriösen Angeboten. → Zentrale Info-Seite: www.verbraucherzentrale.de

🌐 Wichtige Webseiten

Verbraucherzentrale – Phishing-Radar:

- 🔗 www.verbraucherzentrale.de/phishingradar → Hier findest du aktuelle Warnungen vor Betrugs-E-Mails und gefälschten Webseiten.

Polizei – Internetkriminalität melden:

- 🔗 www.polizei.de → Unter „Internetkriminalität" kannst du Online-Betrugsfälle melden und Infos erhalten.

Sicher im Netz – Deutschland sicher im Netz e.V. (DsiN):

- 🔗 www.sicher-im-netz.de → Tipps und Ratgeber, wie Sie Ihr Smartphone, Tablet oder PC sicher nutzen.

Bundesamt für Sicherheit in der Informationstechnik (BSI):

- 🔗 www.bsi-fuer-buerger.de → Offizielle Tipps für mehr Sicherheit im Internet, speziell auch für private Nutzer.

🛠 **Weitere Hilfsangebote speziell für Senioren**

Silver Tipps – Sicher online im Alter:

- 🔗 www.silver-tipps.de → Extra für ältere Internetnutzer: Anleitungen, Videos und Sicherheitstipps in einfacher Sprache.

Telefonseelsorge:

- 📞 0800 111 0 111 oder 0800 111 0 222 (kostenfrei, rund um die Uhr) → Wenn Sie über einen Betrug sprechen möchten oder Sie sich einfach unsicher fühlen.

Initiative "Klicksafe":

- 🔗 www.klicksafe.de → Hilfreiche Informationen über sicheres Surfen, soziale Netzwerke und Datenschutz.

💡 **Mein Tipp:**

Speichern Sie sich diese wichtigen Nummern und Links an einem Ort, wo Sie sie im Notfall schnell finden – zum Beispiel auf einem kleinen Zettel neben Ihrem Telefon oder Computer.

11. Sichern und Wiederherstellen mit Smartphones

Viele Menschen spüren, wie sehr das eigene Smartphone im Alltag an Bedeutung gewonnen hat, es ist Fotoalbum, Adressbuch, Kalender, Notizblock und manchmal sogar Erinnerungsstütze zugleich. Gerade deshalb lohnt es sich, sich einen Moment Zeit zu nehmen, um all diese wertvollen Inhalte zuverlässig zu schützen. Wer weiß, dass seine Daten sicher aufgehoben sind, fühlt sich sofort entspannter und geht gelassener mit dem Gerät um.

Zudem passieren Missgeschicke schneller, als man denkt: Ein Gerät fällt herunter, der Akku gibt plötzlich den Geist auf, ein Update läuft schief oder das Telefon verschwindet unterwegs. Ohne vorherige Sicherung führt so etwas oft zu ärgerlichem Datenverlust. Mit einem funktionierenden Backup dagegen lässt sich selbst ein neues Gerät ohne großen Aufwand wieder so herstellen, wie man es gewohnt war; Kontakte, Fotos und Einstellungen erscheinen fast wie von selbst wieder.

Gerade Seniorinnen und Senioren profitieren sehr von klaren, verständlichen Sicherungswegen. Die Technik wirkt zu Beginn manchmal verwirrend, doch schon wenige einfache Schritte reichen aus, um ein gutes Gefühl zu entwickeln. Wer einmal erlebt hat, wie hilfreich eine Wiederherstellung im Notfall sein kann, möchte den Komfort nicht mehr missen. Diese Einführung zeigt anschaulich, wie man Smartphone-Daten zuverlässig schützt – und wie man sie bei Bedarf ebenso zuverlässig zurückholt. So entsteht ein beruhigendes Maß an Unabhängigkeit und persönlicher Sicherheit.

11.1. Was bedeutet Datensicherung (Backup) und warum ist sie wichtig

Datensicherung bedeutet schlicht, wichtige Inhalte wie Fotos, Kontakte, Nachrichten oder Dokumente an einem zweiten, sicheren Ort aufzubewahren. Man erstellt also eine Art „Kopie" seiner digitalen Erinnerungen. Dadurch bleiben diese Informationen erhalten, selbst wenn das Smartphone einmal kaputtgeht, verlorengeht oder versehentlich gelöscht wird.

Die Bedeutung solcher Sicherungen wird oft erst klar, wenn ein Gerät plötzlich streikt. Ohne Backup lassen sich viele Inhalte dann nicht mehr wiederherstellen. Mit einer vorher erstellten Sicherung gelingt es jedoch, das eigene Smartphone oder ein Ersatzgerät schnell wieder so einzurichten, wie man es gewohnt war.

Regelmäßige Datensicherungen geben älteren Nutzerinnen und Nutzern ein beruhigendes Gefühl: Nichts Wichtiges hängt allein an einem Gerät. Selbst bei kleinen Pannen oder größeren Problemen bleiben persönliche Erinnerungen und wichtige Informationen geschützt. Datensicherung ist deshalb ein grundlegender Baustein für einen sicheren, sorgenfreien Umgang mit moderner Technik.

Definition der Datensicherung

Datensicherung umfasst das Erstellen von 1:1 Kopien wichtiger Daten oder des kompletten Smartphones zum Schutz vor Verlust oder Beschädigung.

Warum ist das wichtig?

Wenn das Smartphone verloren geht, gestohlen wird oder kaputtgeht, können alle Fotos, Kontakte, Nachrichten und Dokumente verloren sein.

Mit einer Datensicherung lassen sich diese Inhalte leicht wiederherstellen – auf demselben oder einem neuen Gerät.

Einfach gesagt:

„Datensicherung ist wie ein Sicherheitsgurt für Ihre Daten, man hofft, ihn nie zu brauchen, aber ist froh, wenn man ihn hat."

Typische Risiken: Verlust, Diebstahl, Defekt des Geräts

Neues Telefon
Wenn man ein neues Smartphone bekommt, z.B.: durch Vertragsumstellung, hilft eine vorherige Datensicherung dabei, alle wichtigen Inhalte mühelos wiederherzustellen. So bleiben Fotos, Kontakte und Einstellungen erhalten und das neue Gerät fühlt sich sofort vertraut an.
Verlust des Smartphones, Diebstahl des Geräts
Smartphones können leicht verloren gehen, was zum Verlust wichtiger Daten und Informationen führt. Gestohlene Smartphones führen zum Verlust sensibler persönlicher Daten und privaten Informationen.
Defekt des Geräts
Ein defektes Smartphone kann alle gespeicherten Fotos, Kontakte und Nachrichten unzugänglich machen. Meistens dadurch, dass das Telefon nicht mehr bedient werden kann.

Welche Daten sollten gesichert werden: Fotos, Kontakte, Nachrichten

Viele Inhalte auf dem Smartphone sind wertvoller, als man im Alltag bemerkt. Besonders Fotos verdienen Schutz, denn sie halten Erinnerungen fest, Familienfeiern, Reisen, alltägliche Augenblicke. Gehen diese Bilder verloren, lässt sich das oft nicht mehr nachholen. Eine Sicherung bewahrt diese Momente zuverlässig. Ebenso wichtig sind Kontakte. Sie enthalten Telefonnummern, E-Mail-Adressen und oft kleine Hinweise, die man sich sonst nirgends notiert hat. Ein Backup sorgt dafür, dass man im Fall eines Gerätewechsels oder einer Reparatur weiterhin jede vertraute Person erreicht. Auch Nachrichten sollten gesichert werden. Viele Unterhaltungen enthalten wichtige Informationen, gemeinsame Absprachen oder herzliche Worte, die man gern aufbewahren möchte. Durch eine regelmäßige Sicherung bleiben solche Texte geschützt und können bei Bedarf wiederhergestellt werden.

Wer diese drei Bereiche, Fotos, Kontakte und Nachrichten, im Blick behält, legt die wichtigste Grundlage dafür, dass nichts Wertvolles verloren geht und das Smartphone jederzeit verlässlich bleibt.

Bitte beachten Sie aufmerksam, dass einige Apps nach einer Wiederherstellung oder beim Wechsel auf ein neues Smartphone eine erneute Anmeldung verlangen können. Besonders sensible Anwendungen wie Krankenkassen Apps, die Ausweis App oder verschiedene Banking Apps schützen Ihre Daten durch zusätzliche Sicherheitsabfragen.

Es ist daher sinnvoll, Zugangsdaten und Anmeldeunterlagen gut erreichbar aufzubewahren, damit die erneute Anmeldung ohne Stress gelingt. Wer diese Informationen parat hat, richtet solche Apps meist in wenigen Schritten wieder ein und kann sie zuverlässig weiter nutzen.

11.2. Fotos und Videos sicher speichern und wiederherstellen

Fotos und Videos gehören für viele Menschen zu den persönlichsten Inhalten auf ihrem Smartphone, sie bewahren Erinnerungen an Familienfeste, Reisen, besondere Augenblicke und kleine Alltagsszenen. Deshalb verdienen sie besonders sorgfältige Aufmerksamkeit, denn ein unerwarteter Geräteausfall oder ein Verlust kann ohne vorherige Sicherung schmerzliche Lücken hinterlassen.

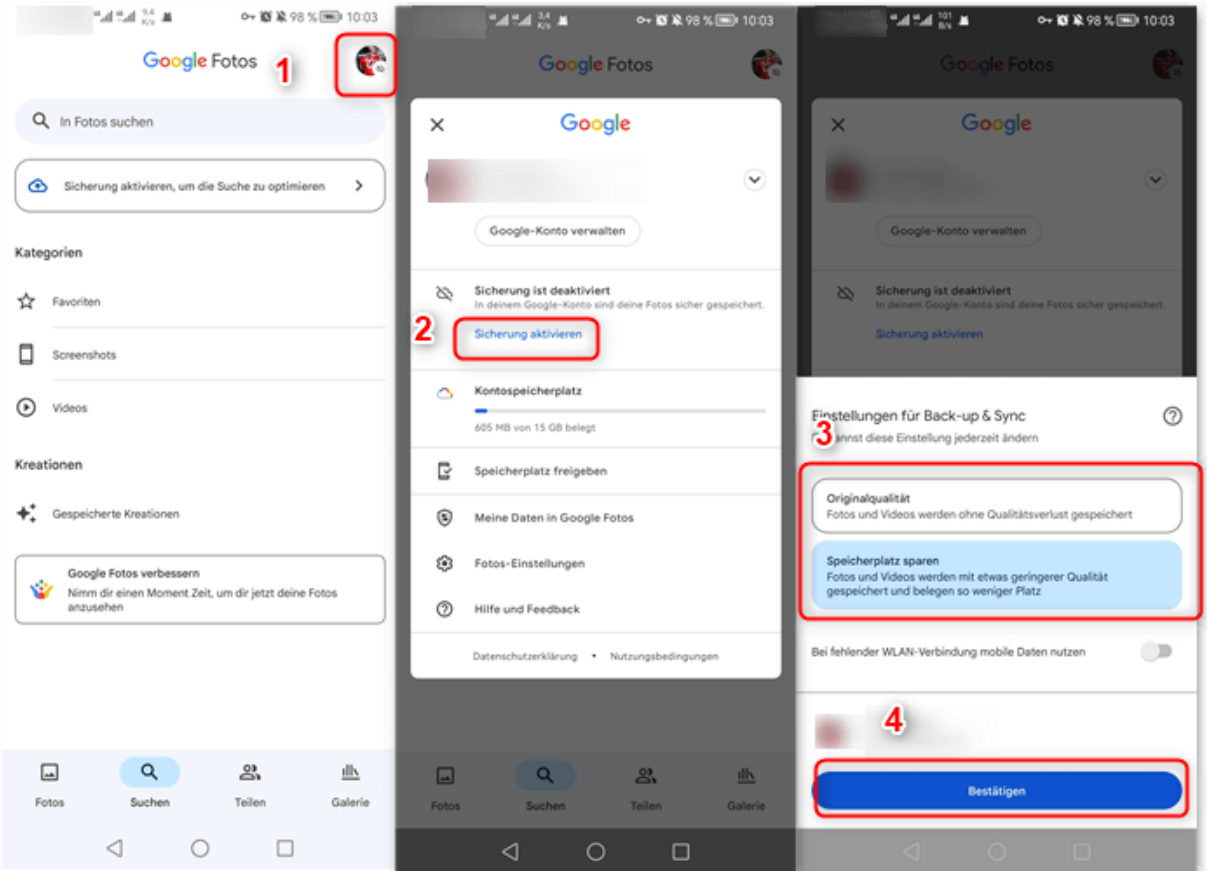
Wir erläutern verständlich, wie sowohl Android Geräte als auch iPhones diese Erinnerungen automatisch bewahren können. Moderne Smartphones bieten praktische Funktionen, mit denen neue Aufnahmen im Hintergrund gesichert werden, sodass man sich selbst um nichts kümmern muss. Gleichzeitig zeigen wir, wie Sie zusätzlich eigene Kopien auf anderem Speicher anlegen können, etwa auf einem Computer oder einem externen Medium.

Wer beide Wege nutzt, also die automatische Sicherung im Gerät und eine zusätzliche Archivierung, schützt seine wertvollsten Aufnahmen besonders zuverlässig. So bleiben schöne Momente erhalten und lassen sich jederzeit wieder anschauen, unabhängig davon, was mit dem Smartphone geschieht.

Fotosicherung bei Android: Google Fotos aktivieren und prüfen

- Installieren und öffnen Sie Google Fotos (normalerweise vorinstalliert).
- Melde dich mit deinem Google-Account an.
- Zugang zu Einstellungen > Sichern und Synchronisieren und aktivieren Sie die Option.
- Wählen Sie, ob Sie Ihre Bilder und Videos in Originalqualität (benötigt Speicherplatz) oder komprimierter Qualität (längere Speicherzeit) speichern möchten (Speicher im Standard 15 GB). *Zusätzliche 100 GB 0,49 monatlich (Stand 11/2025)
- Konfigurieren Sie, welche Geräteordner synchronisiert werden sollen: Standardmäßig lädt die Kamera hoch, Sie können jedoch Ordner für WhatsApp, Telegram, Screenshots usw. hinzufügen.

Bei Android-Geräten können Sie Google Fotos nutzen, um Fotos automatisch in der Cloud zu sichern. Wir erklären, wie Sie Google Fotos aktivieren, prüfen ob die Sicherung funktioniert und wie Sie Fotos bei Bedarf wiederherstellen.



Hinweis 21 Google Konto Foto sichern

Fotosicherung beim iPhone: iCloud-Fotos einschalten und Speicher prüfen

- Öffne die Einstellungen (Zahnrad-Symbol).
- Tippe ganz oben auf deinen Namen / Apple-ID.

- Wähle „iCloud“ → dann „Fotos“.
- Schiebe den Regler bei „iCloud-Fotos“ nach rechts (grün).
- → Jetzt werden alle neuen Fotos automatisch in der Cloud gesichert.
- Apple gibt 5 GB für jeden, aber weitere 50 GB für ~ 12,- € pro Jahr sinnvoll. *Stand 11/2025

Tipp: Wenn Sie „iPhone-Speicher optimieren“ aktivieren, werden große Fotos in der Cloud gespeichert, und auf dem Gerät bleibt nur eine platzsparende Version.

iPhone-Nutzer sichern ihre Fotos über die iCloud. Wir zeigen Schritt für Schritt, wie Sie iCloud-Fotos aktivieren, den Speicherstatus kontrollieren und Fotos von der Cloud auf das iPhone zurückholen können.

Hinweis 22 iPhone Fotos sichern

Zusätzliche Sicherheit: Bilder auf Computer oder USB-Stick kopieren

Android:

- Verbinde das Smartphone mit dem USB-Kabel am Computer.

- Auf dem Handy erscheint die Meldung „Dateien übertragen“ – antippen und bestätigen.
- Auf dem Computer öffnet sich das Gerät wie ein Wechseldatenträger (z. B. Kamera oder USB-Stick).
- Öffne den Ordner DCIM → darin findest du deine Fotos und Videos.
- Kopiere die gewünschten Dateien auf den Computer (z. B. in den Ordner „Handy-Backup“).

Tipp: Es gibt auch kostenlose Programme wie Samsung Smart Switch oder Huawei HiSuite, der kompletten Backups (auch Kontakte, SMS usw.) erstellen.

iPhone:

- Verbinde das iPhone per Kabel mit dem Computer.
- Öffne iTunes (auf Windows) oder den Finder (auf Mac).
- Wähle dein iPhone aus → klicke auf „Backup jetzt erstellen“.
- Aktiviere optional „Backup verschlüsseln“, um Passwörter mitzusichern.
- Tipp: Fotos lassen sich zusätzlich einfach sichern, indem du im Windows-Explorer oder Mac-Finder den Ordner DCIM öffnest und die Bilder auf den Computer oder eine Festplatte kopierst.

Neben der Cloud-Sicherung ist es ratsam, Fotos auch auf einem Computer oder USB-Stick zu speichern. So haben Sie eine weitere Sicherheitskopie und sind auch ohne Internetzugang geschützt.

Kontakte, Kalender und Nachrichten zuverlässig sichern

11.3. Kontakte, Kalender und Nachrichten zuverlässig sichern

Neben Fotos sind auch Kontakte, Kalender und Nachrichten wichtige Daten. Wir erläutern, wie Sie diese Daten sicher synchronisieren und speichern, damit sie bei einem Gerätewechsel oder Datenverlust erhalten bleiben.

Kontakte synchronisieren und sichern mit Google-Konto oder iCloud

Automatische Sicherung: Kontakte werden in der Regel automatisch in Ihr Google-Konto oder iCloud gesichert, um Datenverlust zu vermeiden

(Empfehlung **Android**: Speicherkarte verwenden und dort speichern)

Einfache Wiederherstellung: Gesicherte Kontakte können problemlos auf neuen Geräten wiederhergestellt werden.

Geräteübergreifende Synchronisation: Synchronisation ermöglicht Zugriff auf Kontakte auf mehreren Geräten gleichzeitig.

11.4. Kalenderdaten sichern: Automatische Synchronisierung und Wiederherstellung

Automatische Synchronisierung: Kalenderdaten werden automatisch über Google-Konto oder iCloud synchronisiert, um Termine aktuell zu halten.

Sicherung aktivieren: Die automatische Sicherung kann einfach aktiviert werden, damit alle Kalenderdaten sicher gespeichert sind.

Wiederherstellung von Terminen: Kalenderdaten lassen sich bei Bedarf wiederherstellen, um keine wichtigen Termine zu

Kontakte sichern: Automatische Synchronisierung und Wiederherstellung

Für Android-Smartphones (Google-Konto):

Öffne die Einstellungen.

Tippe auf Google → Konto.

Aktiviere unter „Kontakte synchronisieren" den Schalter (meist automatisch an).

Kontakte werden regelmäßig in der Google Cloud gespeichert.

Tipp: Auf www.contacts.google.com kann man die Kontakte auch am Computer sehen und verwalten.

Für iPhones (iCloud):

Öffne die Einstellungen.

Tippe oben auf deinen Namen / Apple-ID → iCloud.

Aktiviere den Schalter bei „Kontakte".

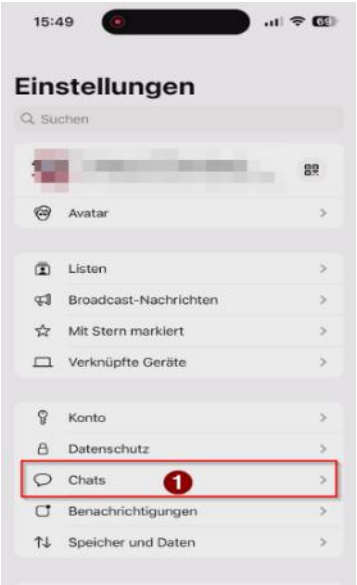
iPhone speichert die Kontakte automatisch in der iCloud.

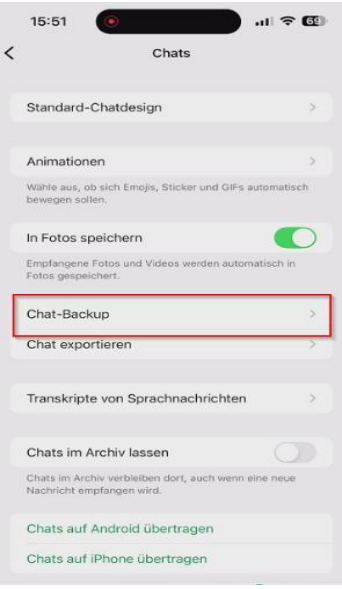
Tipp: Unter www.icloud.com können Kontakte ebenfalls online angesehen und bearbeitet werden.

11.5. Chats sichern WhatsApp &Co

Viele Unterhaltungen in WhatsApp oder anderen Chat Apps enthalten wichtige Informationen, kleine Erinnerungen oder liebevolle Nachrichten, die man nicht verlieren möchte. Deshalb lohnt es sich, auch diese Chats regelmäßig zu sichern. Sowohl WhatsApp als auch vergleichbare Dienste bieten dafür einfache Funktionen, mit denen die Unterhaltung automatisch im Hintergrund gespeichert wird.

Wer eine solche Sicherung eingerichtet hat, kann seine Chats problemlos auf ein neues Smartphone übertragen und behält alle Gespräche in vertrauter Form. Selbst beim Verlust oder Defekt des Geräts bleiben die Nachrichten geschützt und lassen sich später bequem wiederherstellen. Dadurch bleibt die persönliche Kommunikation zuverlässig erhalten, ganz gleich, was mit dem Smartphone geschieht.





Hinweis 23WhatsApp sichern

11.6. Datensicherung bei Telegram

Wichtiger Unterschied zu WhatsApp

Telegram speichert fast alles automatisch in der Cloud, also nicht direkt auf dem Handy, sondern auf den Telegram-Servern.
Das bedeutet: Ihre Nachrichten, Fotos, Videos, Dateien und Kontakte werden automatisch gesichert, sobald Sie sie verschicken oder empfangen.

Sie können sich auf einem neuen Gerät anmelden, und alle Chats erscheinen sofort wieder. Es ist keine manuelle Sicherung nötig.

11.7. Das gesamte Smartphone sichern und wiederherstellen

Komplettsicherung über Google-Konto: Android-Geräte sichern automatisch Apps, Einstellungen und Daten über das verknüpfte Google-Konto.

Aktivierung der Sicherungsfunktion: Die Sicherungsfunktion kann einfach in den Geräteeinstellungen aktiviert und konfiguriert werden.

Datenschutz und Wiederherstellung: Die gesicherten Daten können bei Gerätewechsel oder Wiederherstellung sicher übertragen werden.

Android-Komplettsicherung: Google-Konto nutzen für Apps, Einstellungen und Daten

- Öffnen Sie die Einstellungen, wählen Sie Google, anschließend Sicherung. Bei einigen Geräten finden Sie den Punkt unter Einstellungen, System, Sicherung.
- Aktivieren Sie „Mit Google One sichern", bei älteren Android Versionen eventuell „In Google Drive sichern".
- Prüfen Sie sorgfältig, welche Daten erfasst werden, dazu zählen App Daten, Anrufverlauf, Kontakte, Geräteeinstellungen, SMS-Nachrichten, Fotos sowie Videos, sofern Google Fotos verwendet wird.
- Tippen Sie auf „Jetzt sichern", um sofort eine manuelle Sicherung anzustoßen.
- Kontrollieren Sie Ihre Sicherungen über drive.google.com, dort sehen Sie die zuletzt gespeicherten Inhalte.

Google-Backup verwenden (eingebaute Sicherung)

Schritte

- Öffnen Sie die Einstellungen, wählen Sie Google, anschließend Sicherung. Auf einigen Geräten finden Sie diesen Punkt unter Einstellungen, System, Sicherung.
- • Aktivieren Sie „Mit Google One sichern", bei manchen Android Versionen eventuell „In Google Drive sichern".
- • Prüfen Sie aufmerksam, welche Inhalte erfasst werden, dazu gehören:
    - App Daten,
    - Anrufverlauf,
    - Kontakte
    - Geräteeinstellungen
    - SMS

    - Nachrichten
    - Fotos und Videos über Google Fotos.
- Tippen Sie auf „Jetzt sichern“, damit eine manuelle Sicherung sofort startet.
- Überprüfen Sie Ihre gespeicherten Sicherungen unter drive.google.com, Bereich Sicherungen.

Herstellerspezifische Sicherungstools nutzen

Viele Smartphone Hersteller bieten eigene Sicherungsprogramme an, die speziell auf ihre Geräte abgestimmt sind. Diese Lösungen arbeiten oft sehr zuverlässig und speichern zusätzlich Einstellungen, Layouts oder App Anordnungen, die andere Dienste nicht immer vollständig erfassen. Wer ein Samsung, Xiaomi, Huawei oder ein ähnliches Gerät besitzt, profitiert daher davon, das herstellereigene Werkzeug zu nutzen.

Solche Programme führen Schritt für Schritt durch den Sicherungsprozess und ermöglichen eine besonders genaue Wiederherstellung, falls ein neues Gerät eingerichtet wird oder ein altes ausfällt. Die Bedienung ist meist übersichtlich gestaltet, sodass Sie ohne großen Aufwand eine vollständige Kopie Ihres Smartphones anlegen können.

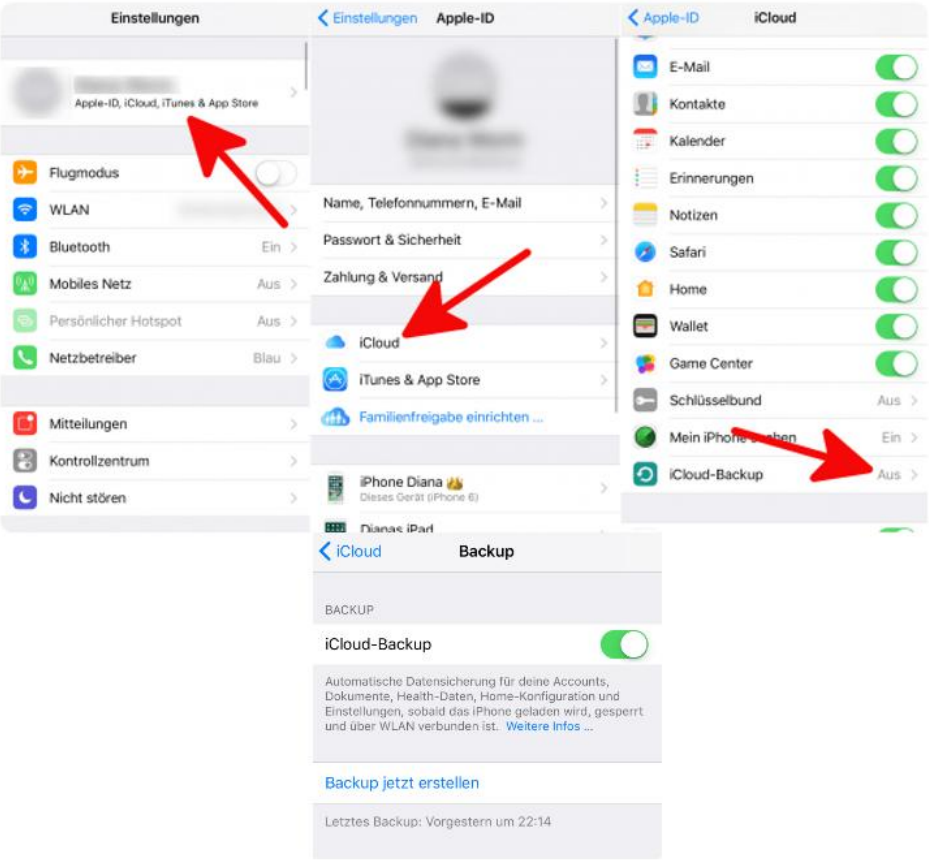
iPhone-Komplettsicherung: iCloud-Backup aktivieren und regelmäßig ausführen

So richten Sie das iCloud-Backup auf Ihrem iPhone einfach und schnell ein, um Ihre Daten zu schützen.

- Automatische Sicherung aktivieren: Aktivieren Sie automatische Backups, damit Ihre Daten regelmäßig und ohne Aufwand gesichert werden.
- Wichtige Hinweise: Beachten Sie Speicherplatz und WLAN-Verbindung für ein erfolgreiches und unterbrechungsfreies Backup.
- Beim iPhone ist das iCloud-Backup die Möglichkeit, das gesamte Gerät in der Cloud zu sichern. Wir erklären, wie Sie das Backup einrichten, automatisch ausführen lassen und worauf zu achten ist.

Cloud-Backup Einrichtung

- Öffnen Sie die Einstellungen (Zahnrad-Symbol).
- Tippen Sie ganz oben auf Ihren Namen / Apple-ID.
- Wählen Sie „iCloud“ → dann „iCloud-Backup“.
- Wählen Sie "Backup jetzt erstellen".



Hinweis 24 iCloud Backup

Wichtige Hinweise zur **Wiederherstellung**: WLAN und Stromversorgung beachten:

WLAN-Verbindung sicherstellen

Eine stabile WLAN-Verbindung ist entscheidend für eine sichere und schnelle Wiederherstellung von Backups ohne Unterbrechungen.

Ausreichende Stromversorgung

Das Smartphone sollte während der Wiederherstellung ausreichend geladen oder an eine Stromquelle angeschlossen sein, um Unterbrechungen zu vermeiden.

- **Einstellungen für die Sicherung auf Android-Geräten:**
  Hier sieht man, wie man in den Einstellungen den Bereich „Google" und dann „Sicherung" auswählt. Dort kann man festlegen, welche Daten automatisch gesichert werden sollen, wie etwa App-Daten, Kontakte, Geräteeinstellungen und SMS-Nachrichten. Die Ansicht hilft, die richtigen Menüpunkte zu finden und die Sicherungsfunktion zu aktivieren.
- **Google One oder Google Drive Sicherung:**
  Ein Screenshot zeigt, wie die Option „Mit Google One sichern" oder „In Google Drive sichern" aussieht. Man erkennt, welche Daten aktuell gesichert werden und wie man eine manuelle Sicherung startet. Dies ist besonders hilfreich, um den Überblick über die eigenen Backups zu behalten.

- **Sicherung von Fotos und Videos über Google Fotos:**
  Es wird gezeigt, wie man in der Google Fotos App die Sicherungs- und Synchronisierungsfunktion aktiviert. Man sieht, wie man auswählen kann, ob Fotos in Originalqualität oder komprimiert gespeichert werden und wie man zusätzliche Ordner (z. B. WhatsApp, Screenshots) zur Sicherung hinzufügt.
- **Herstellerspezifische Backup-Tools:**
  Die Folie enthält Screenshots von Programmen wie Samsung Smart Switch, Huawei HiSuite oder Xiaomi Mi Cloud. Diese Tools bieten oft eine komfortable Möglichkeit, das gesamte Smartphone inklusive Apps, Einstellungen und persönlicher Daten zu sichern. Die Bilder zeigen die Benutzeroberfläche und die wichtigsten Funktionen dieser Programme.
- **iCloud-Backup auf dem iPhone:**
  Es wird dargestellt, wie man auf dem iPhone die iCloud-Backup-Funktion aktiviert. Die Screenshots zeigen die Einstellungen, den Bereich „iCloud" und die Option „Backup jetzt erstellen". Man erkennt, wie einfach es ist, regelmäßige Backups zu starten und zu überprüfen, ob die Sicherung erfolgreich war.
- **Backup-Status und Wiederherstellung:**
  Weitere Screenshots zeigen, wie man den Status der Sicherungen überprüft, z. B. in Google Drive oder iCloud. Man sieht, wie viele Backups vorhanden sind, wann das letzte Backup erstellt wurde und wie man im Fall eines Gerätewechsels oder Datenverlusts die Wiederherstellung startet.

Zusammengefasst:
Die Screenshots auf dieser Folie bieten eine praktische Orientierungshilfe für alle, die ihre Daten auf dem Smartphone sichern möchten. Sie zeigen Schritt für Schritt, wie die Sicherung auf Android- und iOS-Geräten funktioniert, welche Menüpunkte und Optionen wichtig sind und wie man im Ernstfall auf die gesicherten Daten zugreifen kann. So wird deutlich, dass Datensicherung kein komplizierter Prozess ist, sondern mit wenigen Klicks erledigt werden kann – und dass regelmäßige Backups der beste Schutz vor Datenverlust sind.

12. Digitaler Daten-Nachlass

Viele Menschen kümmern sich zu Lebzeiten um Testamente, Versicherungen oder Bankangelegenheiten. Was jedoch häufig vergessen wird, sind digitale Konten und Online-Zugänge. Dabei gehören heute auch E-Mail-Konten, Online-Shops, soziale Netzwerke oder Bezahldienste zum persönlichen Vermögen. Man spricht hier vom sogenannten digitalen Nachlass.

Warum ist das wichtig?

Nach einem Todesfall bleiben viele Konten zunächst aktiv:

- Abonnements laufen weiter
- Zahlungen werden weiterhin abgebucht
- Profile in sozialen Netzwerken bleiben sichtbar
- Fotos, Dokumente und Nachrichten sind weiterhin gespeichert

Angehörige wissen oft nicht:

- Welche Konten existieren
- Wo Zugangsdaten hinterlegt sind
- Ob laufende Verträge bestehen
- Wie Guthaben gesichert werden kann

Das kann zu unnötigen Kosten und organisatorischen Problemen führen.

Welche digitalen Konten sind besonders relevant?

Besonders wichtig sind:

- E-Mail-Konten
- Online-Banking und Bezahldienste
- Amazon, eBay oder andere Online-Shops
- Soziale Netzwerke wie Facebook oder Instagram
- Cloud-Speicher mit Fotos und Dokumenten
- Streaming-Abonnements

Gerade E-Mail-Konten spielen eine zentrale Rolle, da über sie häufig andere Konten zurückgesetzt werden können.

Was passiert ohne Vorsorge?

Ohne klare Regelung dürfen Angehörige sich nicht einfach in ein Konto einloggen – selbst wenn das Passwort bekannt ist. Viele Plattformen verbieten die Nutzung durch Dritte.

In der Regel müssen Erben:

- Sterbeurkunde vorlegen
- Erbnachweis einreichen
- offizielle Anträge stellen

Manche Inhalte, zum Beispiel gekaufte E-Books oder Filme, sind rechtlich nicht übertragbar, da lediglich eine Nutzungslizenz besteht.

Gute Vorsorge – das können Sie tun

Sie können selbst bestimmen, was später mit Ihren digitalen Konten geschehen soll. Sinnvolle Maßnahmen:

- Eine schriftliche Liste aller wichtigen Online-Konten erstellen
- Zugangsdaten sicher hinterlegen, zum Beispiel in einem Passwort-Manager
- Eine Vertrauensperson benennen
- Im Testament eine Regelung zum digitalen Nachlass aufnehmen
- Bei wichtigen Diensten vorhandene Nachlassfunktionen nutzen

Einige Anbieter ermöglichen es, schon zu Lebzeiten festzulegen, wer im Ernstfall informiert wird oder Zugriff erhält.

Sinnvolle Maßnahmen:

- Eine schriftliche Liste aller wichtigen Online-Konten erstellen
- Zugangsdaten sicher hinterlegen, zum Beispiel in einem Passwort-Manager
- Eine Vertrauensperson benennen
- Im Testament eine Regelung zum digitalen Nachlass aufnehmen
- Bei wichtigen Diensten vorhandene Nachlassfunktionen nutzen

Einige Anbieter ermöglichen es, schon zu Lebzeiten festzulegen, wer im Ernstfall informiert wird oder Zugriff erhält.

Tipp für die Praxis

Erstellen Sie einmal im Jahr eine kleine „digitale Bestandsaufnahme“:

- Welche Konten nutze ich regelmäßig?
- Gibt es kostenpflichtige Abonnements?
- Sind meine Zugangsdaten aktuell dokumentiert?

Schon wenige Minuten im Jahr können später viel Aufwand ersparen.

Fazit:

Der digitale Nachlass gehört heute genauso zur persönlichen Vorsorge wie Versicherungen oder Bankunterlagen.

Wer frühzeitig klare Regelungen trifft, entlastet Angehörige und verhindert unnötige Kosten.

Digitale Sicherheit endet nicht beim Passwort – sie umfasst auch die Frage, was eines Tages mit unseren Daten geschieht.

12.1. Online Bezahldienste

Viele Menschen nutzen heute selbstverständlich digitale Bezahl- und Kundenkonten. Dazu gehören unter anderem PayPal, das Amazon-Kundenkonto, eBay oder Kleinanzeigen, Käufe im App-Store oder bei Google Play sowie verschiedene Streaming- und Abonnement-Dienste.

Diese Konten erleichtern den Alltag erheblich. Einkäufe sind schnell erledigt, Rechnungen werden automatisch beglichen, Abonnements verlängern sich bequem im Hintergrund. Doch gerade diese Bequemlichkeit kann im Ernstfall zum Problem werden.

Digitale Bezahlkonten sind häufig direkt mit dem Bankkonto oder der Kreditkarte verbunden. Dadurch entstehen laufende Verpflichtungen, die nicht sofort sichtbar sind.

- Abonnements laufen weiter und verursachen Kosten.
- Rechnungen werden weiterhin automatisch abgebucht.
- Mitunter ist sogar Guthaben auf einem Konto vorhanden.

Hinzu kommt: Angehörige wissen oft gar nicht, welche Online-Konten existieren. Digitale Verträge liegen nicht mehr in einem Ordner, sondern sind nur im jeweiligen Benutzerkonto gespeichert. Viele kleine monatliche Beträge fallen zunächst kaum auf – summieren sich jedoch über die Zeit.

Ohne Vorbereitung ist der Zugriff schwierig. Zugangsdaten fehlen häufig, und eine eigenständige Anmeldung ist rechtlich nicht immer zulässig.

Bezahldienste und Online-Konten werden deshalb häufig unterschätzt. Dabei können sie sowohl finanzielle Werte als auch laufende Verpflichtungen enthalten.

Wer sich frühzeitig einen Überblick verschafft und wichtige Konten dokumentiert, schafft Klarheit – und erspart Angehörigen später unnötigen Aufwand.

12.1.1. PayPal Konten

PayPal ist kein gewöhnliches Online-Konto, sondern ein Zahlungsdienst mit direktem Geldbezug. Häufig ist es mit einem Bankkonto oder einer Kreditkarte verbunden, kann eigenes Guthaben enthalten und führt automatische Abbuchungen für Abonnements oder Einkäufe aus. Deshalb gehört ein PayPal-Konto rechtlich zum Vermögen des Nachlasses.

Was passiert nach einem Todesfall?

Ein PayPal-Konto bleibt zunächst technisch aktiv. Das bedeutet:

- Laufende Abonnements können weiter abbuchen
- Zahlungen können weiterhin ausgelöst werden
- Eventuelles Guthaben bleibt auf dem Konto

PayPal wird nicht automatisch über einen Todesfall informiert. Ohne Meldung bleibt das Konto bestehen.

Dürfen Angehörige sich einfach einloggen? → Nein.

Auch wenn Zugangsdaten bekannt sind, ist eine eigenständige Anmeldung rechtlich problematisch. PayPal-Konten sind personenbezogen, und die Nutzungsbedingungen verbieten eine Weitergabe oder Übernahme.

Der korrekte Weg führt immer über eine offizielle Mitteilung an PayPal.

Wie erfolgt die Abwicklung?

In der Regel verlangt PayPal folgende Unterlagen:

- Sterbeurkunde
- Identitätsnachweis der antragstellenden Person
- Nachweis der Erbenstellung, zum Beispiel durch Erbschein oder Testamentsvollstrecker

Nach Prüfung durch PayPal wird das Konto eingeschränkt, laufende Zahlungen werden gestoppt und vorhandenes Guthaben an den Nachlass ausgezahlt.

Eine dauerhafte Übernahme oder Weiterführung des Kontos ist nicht möglich. PayPal-Konten sind nicht übertragbar.

Warum ist Vorsorge sinnvoll?

Viele Angehörige wissen nicht, ob ein PayPal-Konto existiert oder ob laufende Zahlungen eingerichtet sind. Dadurch können unnötige Kosten entstehen.

Es ist daher empfehlenswert:

- PayPal in einer persönlichen Kontenübersicht zu dokumentieren
- Hinterlegte Bankverbindungen festzuhalten
- Zugangsdaten sicher, aber nachvollziehbar zu verwahren

Eine klare Dokumentation erleichtert die Abwicklung erheblich und verhindert finanzielle Überraschungen.

Fazit

Ein PayPal-Konto kann Teil des finanziellen Nachlasses sein. Ohne rechtzeitige Information bleiben Zahlungen aktiv. Eine frühzeitige Dokumentation und transparente Regelung schützen Angehörige vor unnötigem Aufwand und zusätzlichen Belastungen.

12.1.2. Amazon Konten

Ein Amazon-Konto gehört heute für viele Menschen selbstverständlich zum Alltag. Darüber werden nicht nur Waren bestellt, sondern auch digitale Inhalte genutzt, Abonnements verwaltet und Zahlungsdaten hinterlegt. Gerade deshalb ist ein Amazon-Konto im digitalen Nachlass von besonderer Bedeutung.

Gibt es eine automatische Nachlassregelung?

Amazon bietet keine klassische „Kontovererbung" und keinen festen Nachlasskontakt, der bereits zu Lebzeiten eingerichtet werden kann. Im Todesfall erfolgt die Abwicklung ausschließlich über den Kundendienst. Das bedeutet: Angehörige müssen aktiv auf Amazon zugehen und den Todesfall melden. Eine automatische Übertragung oder Weiterführung des Kontos ist nicht vorgesehen.

Was können Angehörige veranlassen?

Nach Vorlage entsprechender Nachweise können Angehörige:

- das Konto schließen lassen
- laufende Abonnements beenden
- offene Bestellungen klären
- Zahlungsarten entfernen

Amazon prüft jeden Fall einzeln. In der Regel werden folgende Unterlagen verlangt:

- Sterbeurkunde
- Nachweis der Berechtigung, beispielsweise Erbschein
- Identitätsnachweis der antragstellenden Person

Erst nach erfolgreicher Prüfung wird das Konto deaktiviert.

Besonderheit: Digitale Inhalte sind meist nicht übertragbar Ein wichtiger Punkt betrifft digitale Käufe. Viele Nutzer erwerben über Amazon:

- Kindle-E-Books
- Prime-Video-Inhalte
- Audible-Hörbücher
- App-Käufe

Rechtlich handelt es sich hierbei häufig nicht um Eigentum, sondern um eine persönliche Nutzungslizenz. Das bedeutet: Die Inhalte dürfen genutzt, aber nicht vererbt oder übertragen werden. Selbst wenn Angehörige Zugriff auf das Konto hätten, wäre eine dauerhafte rechtliche Übernahme dieser digitalen Inhalte in der Regel nicht möglich.

Dürfen Angehörige sich einfach einloggen?

Auch hier gilt: **Nein**.

Selbst wenn Benutzername und Passwort bekannt sind, verstößt eine eigenständige Anmeldung gegen die Nutzungsbedingungen von Amazon. Das Konto ist personenbezogen. Eine unautorisierte Nutzung kann zur Sperrung führen. Der korrekte Weg führt immer über die offizielle Kontaktaufnahme mit dem Kundenservice.

Warum ist Vorsorge sinnvoll?

Amazon-Konten enthalten häufig:

- gespeicherte Zahlungsarten
- aktive Prime-Mitgliedschaften
- laufende Spar-Abonnements
- digitale Inhalte
- Bestellhistorien

Viele dieser Punkte sind für Angehörige zunächst unsichtbar. Besonders kleine, regelmäßige Zahlungen werden oft erst spät bemerkt. Eine Dokumentation wichtiger Online-Konten erleichtert im Ernstfall die Abwicklung erheblich.

Fazit

Ein Amazon-Konto ist mehr als nur ein Einkaufsprofil. Es kann laufende Kosten verursachen, digitale Inhalte enthalten und sensible Zahlungsinformationen speichern. Wer frühzeitig Klarheit schafft und seine Online-Konten strukturiert dokumentiert, verhindert unnötige Belastungen für Angehörige und sorgt für einen geordneten digitalen Nachlass.

12.1.3. eBay und Kleinanzeigen

Schauen wir uns als nächstes eBay und Kleinanzeigen im digitalen Nachlass an.

Plattformen wie eBay oder Kleinanzeigen werden häufig genutzt, um Gegenstände zu verkaufen, Auktionen durchzuführen oder gebrauchte Artikel zu erwerben. Oft sind dort persönliche Daten, gespeicherte Zahlungsinformationen und laufende Verkaufsangebote hinterlegt. Im digitalen Nachlass spielen diese Konten daher eine wichtige Rolle.

Gibt es eine Nachlassfunktion?

Sowohl bei eBay als auch bei Kleinanzeigen gibt es keine spezielle, vorab einrichtbare Nachlassfunktion. Eine automatische Kontoübertragung ist nicht vorgesehen. Im Todesfall müssen Angehörige aktiv werden und den jeweiligen Kundenservice kontaktieren.

eBay

Bei eBay können über ein Benutzerkonto unter anderem folgende Inhalte bestehen:

- laufende Auktionen
- aktive Verkaufsangebote
- offene Käufe
- gespeichertes Guthaben
- Bewertungen und Nachrichten

Nach Meldung des Todesfalls verlangt eBay in der Regel:

- Sterbeurkunde
- Nachweis der Erbenstellung
- Identitätsnachweis

Nach Prüfung werden:

- laufende Angebote beendet
- offene Transaktionen geklärt
- vorhandenes Guthaben ausgezahlt
- das Konto geschlossen

Eine dauerhafte Weiterführung oder Übernahme des Accounts ist nicht vorgesehen.

Kleinanzeigen

Auch bei Kleinanzeigen können verschiedene Aktivitäten bestehen:

- aktive Verkaufsanzeigen
- laufende Preisverhandlungen
- gespeicherte Nachrichten
- eventuell angebundene Zahlungsabwicklungen

Nach entsprechender Mitteilung und Prüfung werden Anzeigen deaktiviert und das Konto geschlossen. Ein direkter Zugriff durch Angehörige ist ebenfalls nicht vorgesehen. Warum ist das relevant?

Gerade bei Verkaufsplattformen können noch:

- unbeendete Auktionen
- laufende Kaufverträge
- Zahlungsansprüche
- offene Verpflichtungen

bestehen. Ohne offizielle Klärung kann dies zu Missverständnissen oder finanziellen Nachteilen führen.

Hinzu kommt, dass Nachrichtenverläufe oder Bewertungen personenbezogen sind und rechtlich nicht einfach übernommen werden dürfen.

Wichtiger Hinweis

Auch wenn Zugangsdaten bekannt sind, ist eine eigenständige Anmeldung rechtlich problematisch. Die Nutzung verstößt in der Regel gegen die Plattformbedingungen. Der korrekte Weg führt immer über die offizielle Kontaktaufnahme mit dem Anbieter.

Fazit

Konten bei eBay und Kleinanzeigen werden häufig unterschätzt. Sie enthalten jedoch persönliche Daten, laufende Verträge und gegebenenfalls finanzielle Werte. Eine frühzeitige Dokumentation wichtiger Online-Konten erleichtert Angehörigen die Abwicklung erheblich und verhindert unnötige Komplikationen.

12.1.4. Netflix-Konto im digitalen Nachlass

Streaming-Dienste wie Netflix gehören für viele Menschen selbstverständlich zum Alltag. Filme, Serien und Dokumentationen stehen jederzeit zur Verfügung. Bezahlt wird in der Regel bequem per monatlichem Abonnement. Gerade diese automatische Verlängerung macht Netflix im digitalen Nachlass relevant.

Gibt es eine Nachlassfunktion?

Netflix bietet keine spezielle Nachlassregelung an. Es gibt:

- keinen Nachlasskontakt
- keine Kontoübertragung
- keinen Gedenkstatus
- keine automatische Information im Todesfall

Das bedeutet: Ohne aktive Kündigung läuft das Abonnement weiter.

Was passiert ohne Kündigung?

Bleibt das Konto unberührt,

- erfolgt weiterhin die monatliche Abbuchung,
- bleibt das Profil aktiv,
- bleiben gespeicherte Zahlungsmethoden hinterlegt.

Netflix wird nicht automatisch über einen Todesfall informiert. Besonders problematisch ist, dass die Beträge vergleichsweise gering erscheinen. Dadurch fallen sie im Kontoauszug oft nicht sofort auf.

Dürfen Angehörige sich einfach einloggen?

Auch hier gilt: Eine eigenständige Anmeldung ist rechtlich nicht eindeutig zulässig, selbst wenn Zugangsdaten bekannt sind. Konten sind personenbezogen und an die Nutzungsbedingungen des Anbieters gebunden. Der korrekte Weg ist die offizielle Kündigung über den Kundenservice oder – sofern Zugang rechtmäßig besteht – über die reguläre Kontoverwaltung.

Was sollten Angehörige prüfen?

Im Zusammenhang mit Streaming-Diensten empfiehlt es sich zu kontrollieren:

- Besteht ein aktives Abonnement?
- Welche Zahlungsart ist hinterlegt?
- Gibt es weitere gekoppelte Streaming-Dienste?

Oft bestehen neben Netflix noch weitere Abos, die in Vergessenheit geraten sind.

Fazit

Netflix-Konten enthalten in der Regel kein übertragbares Vermögen. Dennoch können sie laufende Kosten verursachen. Streaming-Abonnements werden häufig unterschätzt, da es sich um kleine monatliche Beträge handelt. Über längere Zeit summieren sich diese jedoch. Eine vollständige Übersicht über bestehende Abonnements schafft Klarheit und verhindert unnötige Belastungen für Angehörige.

12.2. Sozialer Netzwerke im digitalen Nachlass

Sicherstellung der Privatsphäre und Zugangskontrolle

Soziale Netzwerke enthalten eine Vielzahl persönlicher Informationen: Fotos, Nachrichten, Kontakte, Kommentare und oft sehr private Inhalte. Im digitalen Nachlass spielt deshalb der Schutz der Privatsphäre eine zentrale Rolle. Ohne klare Regelungen besteht das Risiko, dass persönliche Daten ungewollt offengelegt oder missbräuchlich verwendet werden. Der Schutz der Privatsphäre ist im digitalen Nachlass unverzichtbar. Ziel muss es sein, sensible Informationen auch nach dem eigenen Tod vor unbefugtem Zugriff zu bewahren.

Hilfreich sind technische und organisatorische Maßnahmen. Dazu gehören beispielsweise Passwortmanager, digitale Nachlassverfügungen sowie eine sichere Verwaltung von Zugangsdaten. Solche Werkzeuge erleichtern eine kontrollierte und nachvollziehbare Zugriffsregelung für berechtigte Personen. Viele Menschen fühlen sich bei diesem Thema unsicher. Studien zeigen, dass rund 68 Prozent der Nutzer keine klare Regelung für ihren digitalen Nachlass getroffen haben und Fragen zum Datenschutz offenbleiben. Diese Unsicherheit führt häufig dazu, dass notwendige Entscheidungen aufgeschoben werden.

Umso wichtiger sind klare und verbindliche Regelungen. Eindeutige Zugriffskontrollen und durchdachte Datenschutzmaßnahmen verhindern Missbrauch und schützen vor ungewollter Offenlegung persönlicher Daten. Wer rechtzeitig vorsorgt, sorgt nicht nur für Ordnung, sondern auch für Sicherheit und Würde im digitalen Raum.

12.2.1. Digitaler Nachlass bei Google-Konten

Ein Google-Konto ist für viele Menschen weit mehr als nur eine E-Mail-Adresse. Oft sind darüber zahlreiche Dienste miteinander verknüpft. Dazu gehört unter anderem Gmail, Google Fotos, Google Drive, Kontakte, Kalender, YouTube, Android-Backups sowie gespeicherte Passwörter. Gerade weil ein Google-Konto so viele persönliche Daten bündelt, ist es im digitalen Nachlass von besonderer Bedeutung. Häufig handelt es sich dabei um den zentralen Zugang zu weiteren Online-Diensten.

Welche Daten können betroffen sein?

In einem Google-Konto können unter anderem gespeichert sein:

- E-Mails und persönliche Korrespondenz
- Fotos und Videos aus vielen Jahren
- wichtige Dokumente in Google Drive
- Kontakte und Kalenderdaten
- Sicherungen von Smartphones
- gespeicherte Zugangsdaten

Für Angehörige ist dieses Konto daher oft der wichtigste digitale Datenbestand.

Der Kontoinaktivitätsmanager – Vorsorge zu Lebzeiten

Google bietet eine besondere Funktion an: den sogenannten Kontoinaktivitätsmanager. Mit dieser Einstellung kann bereits zu Lebzeiten festgelegt werden:

- Nach welchem Zeitraum der Inaktivität das Konto als „inaktiv" gilt
- Welche Personen informiert werden sollen
- Ob bestimmte Daten freigegeben werden
- Oder ob das gesamte Konto gelöscht werden soll

Diese Regelung tritt nur dann in Kraft, wenn das Konto über einen längeren Zeitraum nicht mehr genutzt wird. Google versucht zuvor mehrfach, Kontakt aufzunehmen, beispielsweise per E-Mail oder SMS. Erfolgt keine Reaktion, greift die zuvor festgelegte Regelung automatisch.

Einstellbare Zeiträume

Der Zeitraum bis zur Einstufung als inaktiv kann individuell gewählt werden. Möglich sind in der Regel drei bis achtzehn Monate. Für ältere Nutzer kann ein Zeitraum von sechs oder zwölf Monaten sinnvoll sein, um ausreichend Sicherheit zu bieten und dennoch klare Verhältnisse zu schaffen.

Was können benannte Personen erhalten?

Der Kontoinhaber entscheidet selbst, welche Daten weitergegeben werden dürfen. Möglich ist beispielsweise:

- Zugriff nur auf Google Fotos
- Zugriff nur auf Gmail
- Zugriff auf das gesamte Konto

Die benannten Personen erhalten nach Identitätsprüfung einen sicheren Download-Link. Der Zugriff ist zeitlich begrenzt. Warum ist diese Funktion sinnvoll?

Ohne eine solche Regelung müssen Angehörige nach einem Todesfall gesondert Anträge stellen und umfangreiche Nachweise erbringen. Der Prozess kann zeitaufwendig sein. Durch die Nutzung des Kontoinaktivitätsmanagers wird bereits zu Lebzeiten klar festgelegt, was mit dem Konto geschehen soll. Das schafft Transparenz, schützt persönliche Daten und entlastet Hinterbliebene. **Wichtig** ist: Mit dieser Einstellung wird das Konto nicht sofort gelöscht. Es wird lediglich bestimmt, was im Falle längerer Inaktivität automatisch geschehen soll.

Fazit

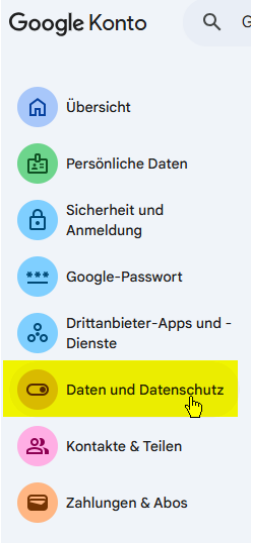
Ein Google-Konto enthält häufig einen großen Teil des digitalen Lebens. Wer hier frühzeitig vorsorgt, sorgt für Klarheit und verhindert Unsicherheiten. Die bewusste Nutzung des Kontoinaktivitätsmanagers ist ein wichtiger Schritt, um Privatsphäre und Daten auch über das eigene Leben hinaus verantwortungsvoll zu regeln.

Wie geht man vor?

Einloggen in das Google Konto:

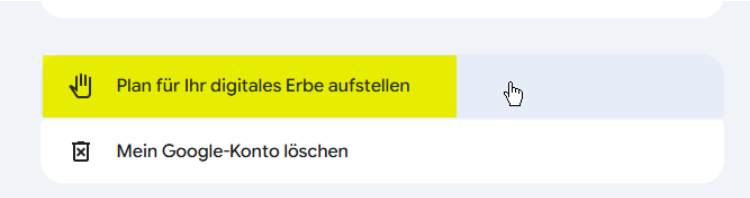
Hinweis 25 Einloggen In Google Konto

Navigieren Sie zu „Daten und Datenschutz:



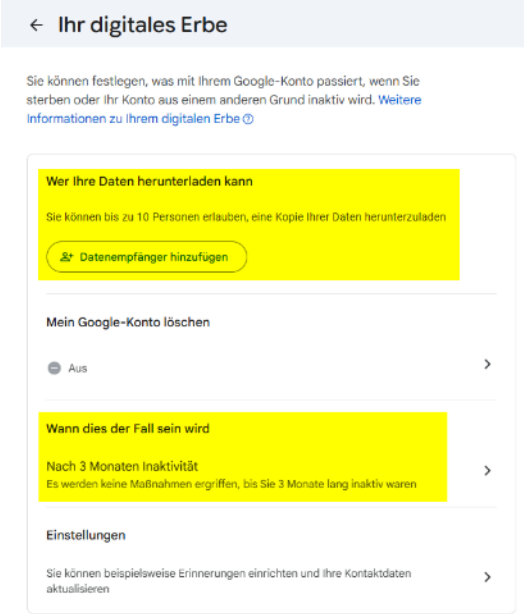
Hinweis 26 Daten und Datenschutz

Zum Digitalen Erbe navigieren:



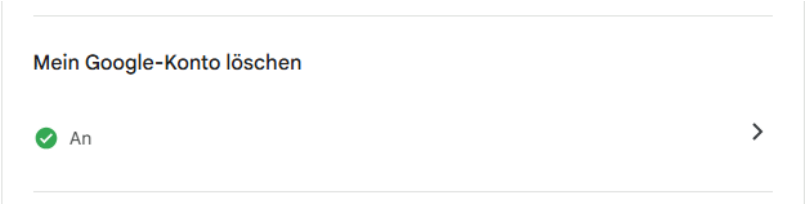
Hinweis 27 Digitales Erbe

Einstellungen zum Digitalen Erbe:



Hinweis 28 Einstellungen Digitales Erbe

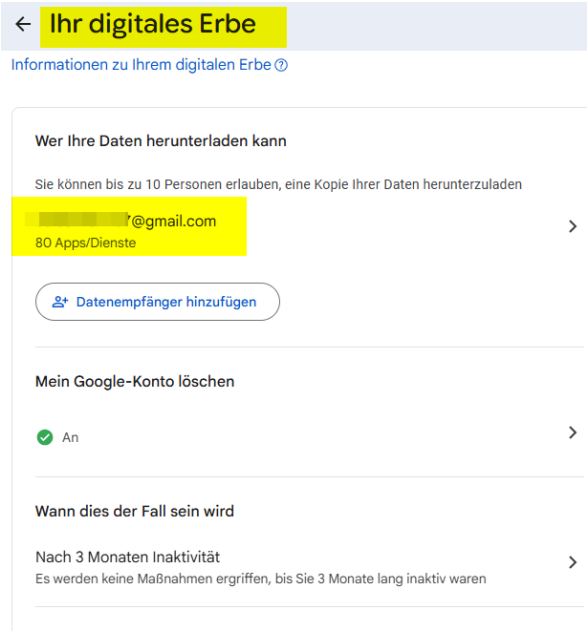
Dann zum Eintrag: Mein Google Konto löschen:



Hinweis 29 Google Kontolöschen

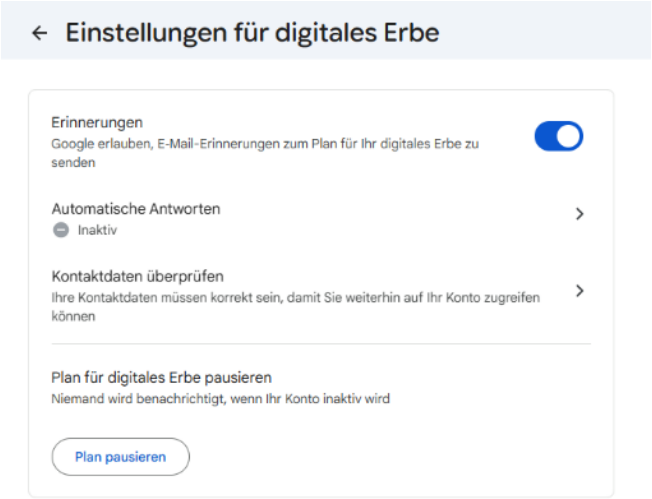
„Sie löschen Ihr Konto nicht heute, sondern bestimmen nur, was Google irgendwann automatisch tun soll."

Wer darf das Konto verwalten?



Hinweis 30 Google: Verwaltung Nutzer

Einstellungen „Digitales Erbe:



Hinweis 31 Einstellungen „Digitales Erbe

12.2.2. Digitaler Nachlass bei Apple-Konten

Die Apple-ID und der Nachlasskontakt

Ein Apple-Konto, auch Apple-ID genannt, ist für viele Nutzer der zentrale Zugang zu ihren Geräten und Daten. Wer ein iPhone, iPad oder einen Mac verwendet, speichert darüber häufig einen großen Teil seines digitalen Lebens. Gerade deshalb spielt die Apple-ID im digitalen Nachlass eine wichtige Rolle.

Welche Daten sind mit der Apple-ID verknüpft?

Über ein Apple-Konto können unter anderem gespeichert sein:

- iCloud-Fotos mit oft jahrelangen Erinnerungen
- Kontakte und Kalender
- Dokumente in iCloud Drive
- Notizen und E-Mails
- Gerätesicherungen von iPhone oder iPad
- gekaufte Apps, Musik oder Filme
- Geräteverwaltung wie „Wo ist?"

Die Apple-ID ist somit nicht nur ein Benutzerkonto, sondern der Schlüssel zu zahlreichen persönlichen Daten.

Gibt es eine Nachlassregelung bei Apple?

Ja. Apple bietet eine offizielle Funktion an, den sogenannten Nachlasskontakt. Mit dieser Einstellung kann der Kontoinhaber bereits zu Lebzeiten eine Vertrauensperson bestimmen. Diese Person darf nach dem Todesfall Zugriff auf bestimmte Daten beantragen.

Wichtig ist dabei:

Der Zugriff entsteht nicht sofort und zu Lebzeiten hat der Nachlasskontakt keinen Einblick in das Konto. Erst nach dem Todesfall kann ein Antrag gestellt werden.

Wie funktioniert der Apple-Nachlasskontakt?

Die Einrichtung erfolgt direkt in den Einstellungen des Apple-Geräts. Der Kontoinhaber legt fest:

- Wer als Nachlasskontakt benannt wird
- Welche Person berechtigt sein soll, später Zugriff zu beantragen

Apple erstellt dafür einen speziellen Zugriffsschlüssel. Nach dem Todesfall benötigt der Nachlasskontakt:

- den Zugriffsschlüssel
- eine Sterbeurkunde

Erst nach Prüfung durch Apple wird der Zugang freigegeben.

Welche Daten erhält der Nachlasskontakt?

Der Zugriff umfasst in der Regel:

- iCloud-Daten wie Fotos und Dokumente
- Kontakte
- Notizen
- Gerätesicherungen

Nicht enthalten sind:

- gespeicherte Passwörter im Schlüsselbund
- Apple Pay-Daten
- bestimmte lizenzierte Medieninhalte

Apple schützt besonders sensible Bereiche gesondert.

Wichtig: Der Nachlasskontakt muss selbst ein eigenes Apple-Konto besitzen.

Warum ist diese Funktion sinnvoll?

Ohne vorherige Einrichtung müssen Angehörige einen aufwendigen Antrag stellen und umfangreiche Nachweise einreichen. Der Prozess kann kompliziert und langwierig sein. Mit dem Nachlasskontakt wird zu Lebzeiten klar geregelt, wer im Ernstfall handeln darf. Das schafft Sicherheit und vermeidet Unsicherheiten. Zugleich bleibt der Schutz der Privatsphäre gewahrt, da kein Zugriff zu Lebzeiten möglich ist.

Fazit

Die Apple-ID bündelt zahlreiche persönliche Daten. Wer iCloud, iPhone oder iPad nutzt, sollte sich bewusst sein, dass diese Inhalte Teil des digitalen Nachlasses werden können. Die Einrichtung eines Nachlasskontakts ist eine einfache Möglichkeit, Vorsorge zu treffen und gleichzeitig die eigene Privatsphäre zu schützen.

Wie geht man vor?

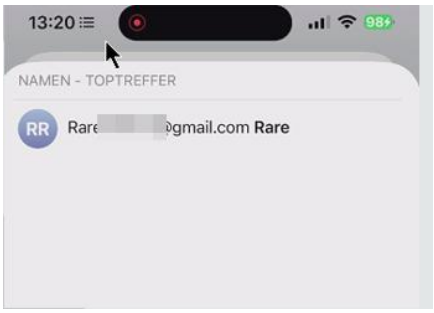
Einloggen in das Apple Konto:

Hinweis 32 Apple Konto Einloggen

Navigieren Sie zum Punkt „Anmeldung & Sicherheit →

Hinweis 33 Apple Nachlasskontakt

Wählen Sie den Namen des Nachlasskontakts aus



Hinweis 34 Nachlasskontakt auswählen

Erstellen eines Nachlass-Schlüssels für das Apple Konto, Kopie drucken oder speichern

Hinweis 35 Apple Zugriffs-Schlüssel speichern

Beispiel Zugriffs-Schlüssel

Zugriffsschlüssel für den Nachlasskontakt

Accounteigentümer:in: (null)
Eigentümer-Apple Account: (null)
Nachlasskontakt: Raret[redacted]gmail.com Rare

Als Nachlasskontakt von (null) kannst du auf die iCloud-Daten zugreifen, wenn die Person verstirbt. Dazu gehören Fotos, Nachrichten, Videos, Notizen, Dokumente und persönliche Daten. Außerdem kannst du die Aktivierungssperre auf den Apple-Geräten der Person entfernen.

Um Zugriff auf die Accountdaten von (null) anzufordern, besuche die Website digital-legacy.apple.com. Dort musst du deinen Zugriffsschlüssel und eine Kopie der Sterbeurkunde von (null) oder je nach Land oder Region ein gleichwertiges Dokument vorweisen.

Sobald deine Zugriffsanfrage genehmigt wurde, kannst du die Daten von (null) auf icloud.com anzeigen oder eine Kopie der Daten unter privacy.apple.com laden. Du kannst auf die Daten von (null) auch auf einem Apple-Gerät zugreifen.

LC: C7B7-EJVL-TZMW-X5J4-MZTS-DL34-SCJA-[redacted]
CRQP-PBGT-RSLX-LRAM-LN4Y-UZLA-3A28-BPY8

Wichtig: Bewahre diesen Schlüssel an einem sicheren Ort auf und teile ihn nicht mit anderen Personen.

Hinweis 36 Apple Zugriffs-Schlüssel

12.2.3. Microsoft-Konto im digitalen Nachlass

Ein Microsoft-Konto ist für viele Nutzer der zentrale Zugang zu:

- Outlook E-Mail
- OneDrive Cloud-Speicher
- Windows-Anmeldung
- Microsoft 365 Abonnement
- Skype
- Xbox-Konto
- gespeicherte Geräte-Backups

Gerade OneDrive und Outlook enthalten häufig sehr persönliche oder geschäftliche Daten. Das Konto ist personenbezogen und kann finanzielle sowie datenschutzrechtliche Relevanz haben.

Gibt es eine Nachlassfunktion?

Microsoft bietet keinen klassischen „Nachlasskontakt" wie Apple an. Es gibt:

- keine vorab benennbare Vertrauensperson
- keine automatische Kontoübertragung
- keine direkte Kontovererbung

Im Todesfall müssen Angehörige einen offiziellen Antrag bei Microsoft stellen. Erforderlich sind in der Regel:

- Sterbeurkunde
- Nachweis der Erbenstellung
- Identitätsnachweis

Microsoft prüft jeden Fall individuell.

Was passiert mit Daten und Abonnements?

Ein Microsoft-Konto kann enthalten:

- E-Mails
- Dokumente in OneDrive
- laufende Microsoft-365-Abonnements
- gespeicherte Zahlungsdaten

Ohne Kündigung können kostenpflichtige Abos weiterlaufen. **Wichtig:**

Microsoft kann unter bestimmten Voraussetzungen Datenzugang gewähren oder das Konto schließen.

Eine automatische Freigabe erfolgt nicht. Auch hier gilt: Eigenständiges Einloggen durch Angehörige ist rechtlich problematisch, selbst wenn Zugangsdaten bekannt sind.

Microsoft-Konten werden häufig unterschätzt, da sie oft „nur" als Windows-Anmeldung wahrgenommen werden. Tatsächlich enthalten sie jedoch häufig zentrale E-Mails, Cloud-Dokumente und laufende Abonnements.

12.2.4. Facebook: Gedenkzustand und Konto-Verwaltung

Facebook begleitet viele Menschen über Jahre hinweg. Dort werden Fotos geteilt, Lebensereignisse dokumentiert und Kontakte gepflegt. Entsprechend persönlich ist der Inhalt eines solchen Profils. Im digitalen Nachlass stellt sich daher die Frage: Was geschieht mit dem Facebook-Konto nach dem Tod?

Der Gedenkzustand

Facebook bietet die Möglichkeit, ein Profil in den sogenannten Gedenkzustand zu versetzen.

Ein Gedenkprofil:

- bleibt sichtbar
- kennzeichnet das Konto als „In Erinnerung an …"
- schützt vor unbefugter Anmeldung
- verhindert Änderungen am bestehenden Inhalt

Freunde und Familie können weiterhin Beiträge teilen oder Erinnerungen hinterlassen, sofern die Privatsphäre-Einstellungen dies erlauben. **Wichtig ist**: Niemand kann sich nach der Umwandlung in das Konto einloggen.

Der Nachlasskontakt

Zusätzlich kann zu Lebzeiten ein Nachlasskontakt bestimmt werden. Diese Person darf nach dem Todesfall:

- das Profilbild ändern
- einen angehefteten Beitrag veröffentlichen
- Freundschaftsanfragen verwalten
- das Konto gegebenenfalls löschen lassen

Der Nachlasskontakt erhält jedoch keinen vollständigen Zugriff auf private Nachrichten oder alte Chatverläufe. Der Schutz persönlicher Kommunikation bleibt bestehen. Die Benennung erfolgt in den Facebook-Einstellungen unter dem Bereich „Gedenkzustand".

Alternative: Dauerhafte Löschung

Wer nicht möchte, dass das Profil als Gedenkseite bestehen bleibt, kann bereits zu Lebzeiten festlegen, dass das Konto im Todesfall vollständig gelöscht werden soll. Diese Entscheidung liegt allein beim Kontoinhaber.

Warum ist diese Regelung sinnvoll? Ohne entsprechende Festlegung bleibt ein Facebook-Profil zunächst aktiv. Angehörige müssen dann eigenständig eine Meldung an Facebook vornehmen und entsprechende Nachweise einreichen. Die vorherige Benennung eines Nachlasskontakts schafft Klarheit. Gleichzeitig bleibt die Privatsphäre gewahrt, da kein vollständiger Zugriff auf persönliche Nachrichten möglich ist.

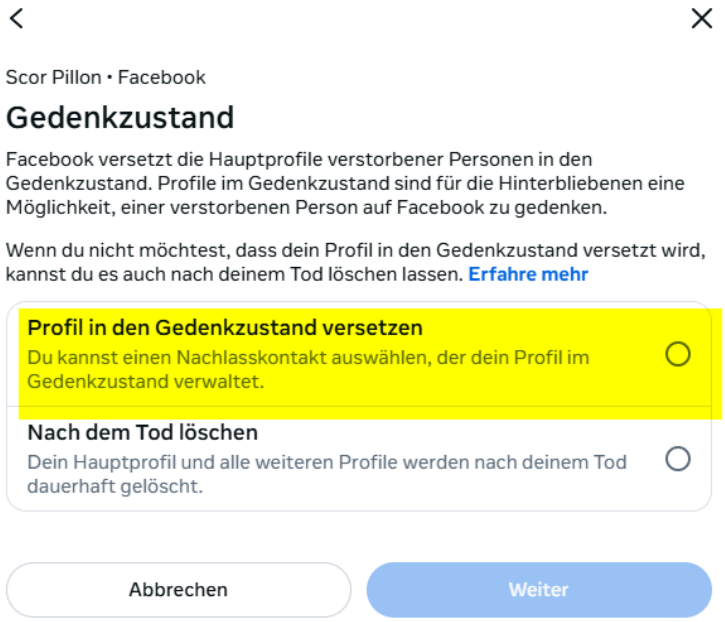
Bedeutung für Angehörige: Weltweit befinden sich Millionen Profile im Gedenkzustand. Das zeigt, wie relevant dieses Thema geworden ist. Ein Facebook-Konto enthält oft:

- persönliche Fotos
- Kommentare und Erinnerungen
- Kontakte und Netzwerke

Eine bewusste Entscheidung zu Lebzeiten sorgt dafür, dass respektvoll mit diesen Inhalten umgegangen wird.

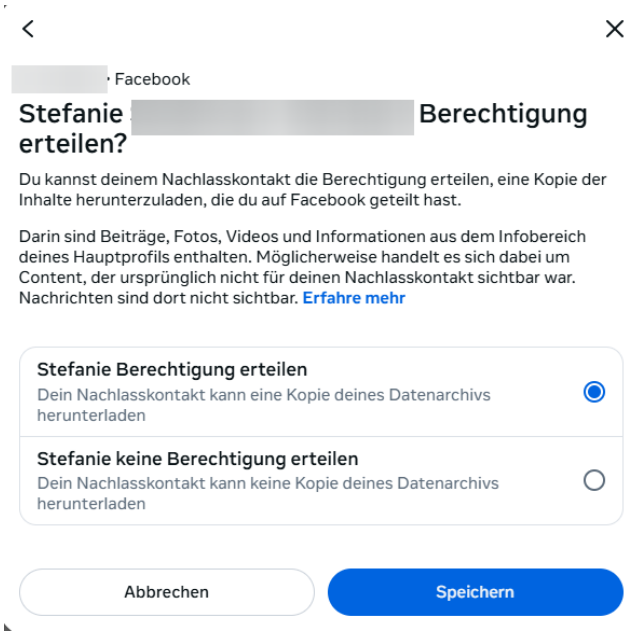
Facebook: Gedenkzustand und Konto-Verwaltung

Einloggen ins Facebook Konto „Gedenkzustand etc.:



Hinweis 37 Facebook Gedenkzustand

Berechtigten für Facebook auswählen:



Hinweis 38 Facebook Berechtigter

12.2.5. Umgang mit WhatsApp-Konten

WhatsApp im digitalen Nachlass

WhatsApp gehört für viele Menschen zum täglichen Kommunikationsmittel. Über den Messenger werden Nachrichten ausgetauscht, Fotos versendet, Sprachnachrichten gespeichert und Gruppenchats geführt. Entsprechend persönlich sind die Inhalte eines WhatsApp-Kontos. Im Gegensatz zu einigen sozialen Netzwerken bietet WhatsApp jedoch keine klassische Nachlassverwaltung an.

Keine offizielle Nachlassregelung

WhatsApp erlaubt keine Verwaltung digitaler Nachlässe durch Dritte. Es gibt:

- keinen offiziellen Nachlasskontakt
- keine Möglichkeit zur Kontoübertragung
- keinen Gedenkstatus

Ein WhatsApp-Konto ist streng personenbezogen und an eine konkrete Telefonnummer gebunden. Eine formelle Übergabe an Angehörige ist nicht vorgesehen.

Automatische Löschung bei Inaktivität

Statt einer Nachlassfunktion verfolgt WhatsApp einen anderen Ansatz: Konten werden nach längerer Inaktivität automatisch gelöscht. Nach der aktuellen Regelung wird ein Konto in der Regel nach 120 Tagen Inaktivität entfernt.

Voraussetzung ist:

- Es besteht keine Verbindung mehr zu den WhatsApp-Servern.
- Die App wird auf keinem Gerät mehr geöffnet.

Sobald über einen längeren Zeitraum keine Aktivität erfolgt, gilt das Konto als inaktiv. Was bedeutet das praktisch?

Wird ein Konto gelöscht,

- verschwindet das Profil aus dem System,
- wird der Chatverlauf auf den Servern entfernt,
- enden bestehende Gruppenmitgliedschaften automatisch.

Andere Nutzer sehen dann lediglich, dass die betreffende Person nicht mehr bei WhatsApp registriert ist. Zu beachten ist jedoch: Lokale Backups auf dem Smartphone oder in einer Cloud-Sicherung können unter Umständen weiterhin bestehen, sofern sie nicht gelöscht wurden. Welche Konsequenzen ergeben sich daraus?

Da es keine offizielle Nachlassverwaltung gibt, ist ein geordneter Zugriff für Angehörige nur eingeschränkt möglich. Ist das Smartphone vorhanden und entsperrbar, können Nachrichten lokal eingesehen werden. Ohne Zugang zum Gerät oder ohne Kenntnis der Entsperrdaten ist ein Zugriff praktisch nicht realisierbar. Eine formelle Datenherausgabe durch WhatsApp ist in der Regel nicht vorgesehen.

Warum ist Vorsorge dennoch sinnvoll?

Auch wenn WhatsApp-Konten automatisch gelöscht werden, können sie persönliche Inhalte enthalten, die für Angehörige von emotionaler Bedeutung sind. Wer hier vorsorgen möchte, kann:

- regelmäßige Backups bewusst verwalten,
- wichtige Nachrichten separat sichern,
- Vertrauenspersonen über Gerätezugänge informieren.

Dabei sollte stets der Datenschutz und die Privatsphäre aller Beteiligten berücksichtigt werden.

Fazit

WhatsApp unterscheidet sich deutlich von anderen Plattformen. Es gibt keine aktive Nachlassregelung, sondern eine automatische Löschung bei längerer Inaktivität. Das schützt zwar die Privatsphäre, erschwert jedoch die spätere Einsicht für Angehörige. Eine bewusste Entscheidung zu Lebzeiten kann helfen, Klarheit zu schaffen und persönliche Erinnerungen gegebenenfalls zu sichern.

12.2.6. Umgang mit Telegram-Konten

Telegram ist ein Messenger-Dienst, der ähnlich wie WhatsApp für Nachrichten, Fotos, Videos und Gruppenchats genutzt wird. Viele Menschen schätzen Telegram wegen seiner großen Gruppenfunktionen und zusätzlichen Sicherheitsoptionen. Auch bei Telegram stellt sich im digitalen Nachlass die Frage: Was geschieht mit dem Konto, wenn es nicht mehr genutzt wird?

Keine klassische Nachlassverwaltung

Telegram bietet derzeit:

- keinen offiziellen Nachlasskontakt
- keinen Gedenkmodus
- keine Kontoübertragung an Angehörige

Ein Telegram-Konto ist ebenfalls personenbezogen und an eine Telefonnummer gebunden. Eine formelle Weitergabe oder Übernahme durch Dritte ist nicht vorgesehen.

Automatische Selbstlöschung bei Inaktivität

Telegram verfolgt einen anderen Ansatz als viele soziale Netzwerke: Konten löschen sich automatisch nach einer festgelegten Zeit ohne Nutzung. Standardmäßig wird ein Konto nach sechs Monaten Inaktivität gelöscht. Der Nutzer kann diesen Zeitraum jedoch selbst anpassen. Möglich sind je nach Einstellung:

- 1 Monat
- 3 Monate
- 6 Monate
- 12 Monate
- bis zu 24 Monate

Wenn innerhalb dieses Zeitraums:

- keine Anmeldung erfolgt
- die App nicht geöffnet wird

wird das Konto automatisch entfernt.

Was bedeutet das praktisch?

Nach der automatischen Löschung:

- verschwindet das Profil vollständig
- werden Nachrichten auf den Telegram-Servern entfernt
- enden Gruppenmitgliedschaften
- ist das Konto nicht mehr auffindbar

Für andere Nutzer wirkt es so, als habe die Person Telegram verlassen.

Zugriff für Angehörige

Da es keine Nachlassfunktion gibt, ist ein offizieller Zugriff durch Angehörige nicht vorgesehen. Ist das Smartphone vorhanden und entsperrbar, können vorhandene Chats eingesehen werden, solange das Konto noch aktiv ist. Ohne Zugang zum Gerät oder ohne Kenntnis der Entsperrdaten ist ein Zugriff praktisch nicht möglich. Eine Herausgabe von Daten durch Telegram erfolgt in der Regel nicht ohne entsprechende rechtliche Grundlage.

Besonderheit im Vergleich zu anderen Plattformen

Im Unterschied zu Facebook oder Apple bietet Telegram keine Möglichkeit, zu Lebzeiten eine Vertrauensperson zu benennen. Stattdessen setzt der Dienst auf automatische Löschung. Das stärkt den Datenschutz und schützt die Privatsphäre, kann jedoch dazu führen, dass persönliche Inhalte nach Ablauf der Frist dauerhaft verloren sind.

Fazit

Telegram-Konten werden bei längerer Inaktivität automatisch gelöscht. Eine aktive Nachlassregelung existiert nicht. Wer wichtige Inhalte sichern möchte, sollte sich zu Lebzeiten Gedanken machen und gegebenenfalls persönliche Daten separat speichern. Die automatische Selbstlöschung schützt zwar die Privatsphäre, ersetzt jedoch keine bewusste Vorsorgeplanung.

12.2.7. Umgang mit Instagram, X (Twitter) & TikTok-Konten

Soziale Netzwerke wie Instagram, X oder TikTok sind für viele Menschen ein fester Bestandteil des Alltags. Dort werden Fotos veröffentlicht, Videos geteilt, Meinungen geäußert und Kontakte gepflegt. Entsprechend persönlich sind die Inhalte dieser Profile.

Gibt es einen Nachlasskontakt?

Im Gegensatz zu Facebook oder Apple bieten diese Dienste keine klassische Nachlassfunktion an. Es gibt:

- keinen offiziellen Nachlassverwalter
- keinen Vertreter, der zu Lebzeiten bestimmt werden kann
- keine Kontovererbung
- keinen direkten Zugriff für Angehörige

Eine vollständige Übernahme oder Weiterführung des Accounts ist nicht vorgesehen.

Was können Angehörige tun?

Angehörige können in der Regel lediglich die Löschung oder – je nach Plattform – eine Umwandlung in einen Erinnerungszustand beantragen. Dafür werden üblicherweise folgende Angaben verlangt:

- Name des Kontoinhabers
- Link zum Profil
- Nachweis des Todes
- Sterbeurkunde oder offizieller Nachruf

Nach Einreichung der Unterlagen erfolgt eine manuelle Prüfung durch den jeweiligen Anbieter. Ein direkter Zugang zu privaten Nachrichten, gespeicherten Inhalten oder vollständigen Kontodaten wird in der Regel nicht gewährt. Was bedeutet das für die Praxis?

Profile bleiben ohne Antrag zunächst bestehen. Inhalte sind weiterhin sichtbar, sofern sie öffentlich waren. Da keine Zugriffsmöglichkeit eingerichtet werden kann, sollten wichtige Inhalte zu Lebzeiten bewusst gesichert werden, wenn sie erhalten bleiben sollen. Gleichzeitig schützt diese restriktive Handhabung die Privatsphäre der verstorbenen Person, da keine unbefugte Einsicht in private Kommunikation möglich ist.

Fazit

Instagram, X und TikTok bieten keine aktive Nachlassverwaltung an. Angehörige können in der Regel nur eine Löschung beantragen, jedoch keinen vollständigen Zugriff erhalten. Wer hier Vorsorge treffen möchte, sollte frühzeitig entscheiden, welche Inhalte dauerhaft erhalten bleiben sollen und entsprechende Sicherungen vornehmen.

12.2.8. Vergleich Soziale Medien

Plattform	Nachlasskontakt möglich	Gedenkstatus	Kontoübernahme Datenzugriff
Facebook	Ja	Ja	eingeschränkt möglich
Instagram	Nein	Ja	Nein
X (Twitter)	Nein	Nein	Nein
TikTok	Nein	Nein	Nein
Google Account	Ja (über Inaktivitätsmanager)	Nein	Ja, vorher festlegbar
Apple Account (Apple ID)	Ja (Nachlasskontakt)	Nein	Ja, mit Zugriffsschlüssel

Hinweis 39 Vergleich Soziale Medien

12.3. Strategien für den verantwortungsvollen Umgang mit dem digitalen Nachlass

Digitale Konten, E-Mails, Fotos, Online-Verträge und Bezahldienste sind heute fester Bestandteil unseres Lebens. Dennoch haben viele Menschen keine klare Regelung getroffen, was mit diesen Daten im Ernstfall geschehen soll. Ein strukturierter Umgang mit dem digitalen Nachlass schützt nicht nur persönliche Informationen, sondern entlastet auch Angehörige.

Vorbereitung zu Lebzeiten

Eine frühzeitige Planung schafft Sicherheit. Bereits wenige Maßnahmen können später viel Aufwand vermeiden. Dazu gehören:

- Erstellung einer Übersicht aller wichtigen Online-Konten
- Dokumentation laufender Abonnements
- sichere Aufbewahrung von Zugangsdaten
- Nutzung eines Passwortmanagers
- Benennung einer Vertrauensperson

Wichtig ist, dass Zugangsdaten nicht offen zugänglich sind, sondern geschützt und nachvollziehbar hinterlegt werden.

Erbenregelungen und Vollmachten

Digitale Konten unterliegen rechtlichen Rahmenbedingungen. In Deutschland regeln das Bürgerliche Gesetzbuch sowie Datenschutzvorschriften den Umgang mit digitalen Vermögenswerten. Sinnvoll kann es sein:

- eine Vollmacht für digitale Konten zu erteilen
- ergänzende Regelungen im Testament aufzunehmen
- festzulegen, welche Konten gelöscht oder erhalten bleiben sollen

Klare Festlegungen vermeiden Streitigkeiten und Missverständnisse.

Bedeutung technischer Hilfsmittel

Technische Lösungen erleichtern die Organisation erheblich. Dabei ermöglichen Passwortmanager eine strukturierte Verwaltung von Zugangsdaten. Digitale Nachlassverfügungen schaffen Klarheit und Anbieterspezifische Funktionen wie Nachlasskontakte oder Inaktivitätsmanager können zusätzlich genutzt werden. Solche Instrumente sorgen für eine kontrollierte und sichere Weitergabe von Informationen.

Daher die Empfehlungen für Angehörige im Todesfall ist eine geordnete Bestandsaufnahme entscheidend.

Angehörige sollten:

- vorhandene Online-Konten ermitteln
- laufende Zahlungen überprüfen
- Anbieter offiziell informieren
- rechtliche Nachweise bereithalten

Ein systematisches Vorgehen verhindert finanzielle Nachteile und schützt persönliche Daten.

Schlussgedanke

Der digitale Nachlass ist kein Randthema mehr. Er gehört heute ebenso zur Vorsorge wie Bankunterlagen oder Versicherungen. Wer rechtzeitig klare Regelungen trifft, sorgt für Transparenz, schützt seine Privatsphäre und entlastet seine Familie. Digitale Sicherheit endet nicht beim starken Passwort. Sie umfasst auch die Verantwortung dafür, was eines Tages mit unseren Daten geschieht.

13. Was ist Linux – eine sichere, kostenlose Alternative für Ihren PC

Viele Seniorinnen und Senioren nutzen einen Windows-PC. Doch es gibt eine interessante Alternative: **Linux**. Linux ist ein freies, kostenloses Betriebssystem, das besonders **sicher und stabil** ist – und hervorragend für den Alltag geeignet. Da wir das meiste am PC online machen oder Daten in der Cloud liegen reicht diese Alternative vollkommen aus. Die Bedienung von Linux ähnelt dabei meist sehr stark and die Bedienung von Windows als Betriebssystem.

Es gibt einige kostenlose Linux-Distributionen, die sich optisch und funktional stark an Windows orientieren und besonders für Umsteiger geeignet sind:

1. **Linux Mint (**https://www.linuxmint.com/**)**: Eine der beliebtesten Distributionen für Windows-Umsteiger. Es bietet eine benutzerfreundliche Oberfläche und ein Startmenü, das dem von Windows ähnelt.
2. **Zorin OS (**https://zorin.com/**)**: Diese Distribution ist speziell darauf ausgelegt, Windows-Nutzer anzusprechen. Sie bietet ein Windows-ähnliches Design und ist einfach zu bedienen.
3. **Winux** (https://winuxos.org/): Diese Distribution imitiert das Aussehen von Windows 11 und bietet ähnliche Systemeinstellungen.

Alle drei Systeme sind kostenlos erhältlich und eignen sich hervorragend für den Einstieg in die Linux-Welt. Sie bieten eine benutzerfreundliche Oberfläche und laufen auch auf älteren Computern zuverlässig. So können Sie Ihren bestehenden PC sicher und effizient weiter nutzen. Updates erfolgen automatisch und sorgen für einen aktuellen Schutz. Gleichzeitig werden Ihre Daten besser vor Schadsoftware und unerwünschten Zugriffen geschützt.

🚀 **Vorteile von Linux:**

1. Hohe Sicherheit:

Linux ist weniger anfällig für Viren, weil es eine andere Struktur als Windows hat und Angreifer seltener auf Linux-Systeme zielen.

2. Keine Kosten:

Linux-Betriebssysteme wie **Ubuntu**, **Linux Mint** oder **Zorin OS** sind komplett kostenlos – Sie müssen keine Lizenzen kaufen oder erneuern. Es wird in der Regel auch immer ein kostenloses Office Programm mitgeliefert zur freien Nutzung. Am verbreiteten sind **OpenOffice** (https://www.openoffice.de/) und **LibreOffice** (https://de.libreoffice.org/). Beide Programme können auch unter Windows (10 oder 11) installiert werden und bieten auch dort einen kostenlosen Ersatz für Microsofts Office Paket, welches gekauft werden muss.

3. Einfache Bedienung:

Moderne Linux-Varianten sind leicht zu bedienen und sehen ähnlich aus wie Windows.

4. Regelmäßige Updates:

Linux wird von einer engagierten Gemeinschaft gepflegt – Sicherheitsupdates kommen oft schneller als bei anderen Systemen.

5. Schon ältere Computer:

Linux läuft auch auf älteren Geräten sehr schnell – perfekt, um aus einem älteren Laptop ein sicheres, modernes Gerät zu machen!

👓 Fallbeispiel: Umstieg auf Linux

Herr Weber, 72 Jahre alt, wollte seinen alten Laptop nicht wegwerfen. Er installierte zusammen mit seinem Enkel **Linux Mint**. Sein Fazit nach drei Monaten:

"Ich surfe im Internet, schreibe E-Mails und erledige Bankgeschäfte – und das alles ohne Sorgen. Mein Computer läuft schneller als je zuvor!"

🔧 Hinweis:

Die erste Installation und Einrichtung kann für Anfänger etwas kompliziert sein. Es lohnt sich, sich von Familie, Freunden oder einem Computerkurs unterstützen zu lassen. Viele Volkshochschulen bieten inzwischen auch **Linux-Kurse** für Einsteiger an.

☑ Zusammenfassung:

Vorteil	Beschreibung
Kostenlos	Keine Lizenzgebühren
Sicher	Sehr geringe Gefahr durch Viren
Einfach	Benutzerfreundliche Oberflächen
Langlebig	Auch für alte PCs und Laptops ideal

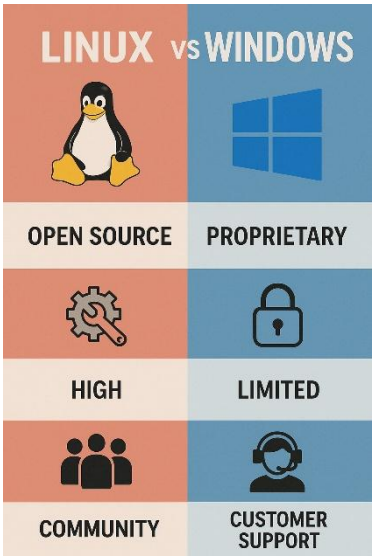
Hinweis 40 Linux Vorteile

Unterschiede und Vergleiche Linux zu Microsoft Windows ®

Eigenschaft	Linux	Windows
Lizenzmodell	Open Source, kostenlos	Proprietär, kostenpflichtig
Anpassbarkeit	Hoch (Konfigurationsmöglichkeiten)	Begrenzt
Benutzer-Freundlichkeit	Für Einsteiger und Experten (je nach Distribution)	Sehr einsteigerfreundlich
Softwareangebot	Große Auswahl an Open-Source-Software	Große Auswahl, oft kostenpflichtig
Community-Support	Aktiv und umfassend	Hauptsächlich kommerzieller Support

Eigenschaft	Linux	Windows
Sicherheit	Robust gegen Malware	Anfälliger für Angriffe
Performance	Effizient, besonders auf älterer Hardware	Anspruchsvoller auf Ressourcen
Kompatibilität	Unterstützt viele Geräte und Architekturen	Optimiert für gängige Hardware

Hinweis 41 Vergleich Windows - Linux



Hinweis 42 Windows - Linux in aller Kürze

Quellen:

- Linux Mint Projektseite: linuxmint.com
- Ubuntu Projektseite: ubuntu.com
- Verbraucherzentrale: verbraucherzentrale.de

14. Zusammenfassung

Internet-Sicherheit für Seniorinnen und Senioren

1. Warum ist Sicherheit im Internet so wichtig?

→ Schutz vor Betrug, Diebstahl und Missbrauch persönlicher Daten.

2. Was sind die größten Gefahren im Internet?

→ Viren, Phishing, Betrugsversuche, falsche Webseiten.

3. Wie erkenne ich eine sichere Internetseite?

→ Schloss-Symbol und „https" in der Adresszeile beachten.

4. Welche Passwörter sind wirklich sicher?

→ Längere, komplizierte Passwörter nutzen, jedes Konto eigenes Passwort.

5. Warum sind Updates so wichtig?

→ Sie schließen Sicherheitslücken und schützen Ihr Gerät.

6. Brauche ich ein Virenschutzprogramm?

→ Ja, es schützt zuverlässig vor Schadsoftware und Gefahren.

7. Was tun bei verdächtigen E-Mails und Nachrichten?

→ Niemals auf Links klicken oder Anhänge öffnen – Absender prüfen!

8. Online-Shopping: Woran erkenne ich sichere Shops?

→ Gütesiegel, sichere Zahlungsarten, vollständige Kontaktangaben.

9. Wie schütze ich meine Daten in sozialen Netzwerken?

→ Privatsphäre-Einstellungen anpassen, sparsam mit persönlichen Infos umgehen.

10. Was bedeutet Zwei-Faktor-Authentifizierung?

→ Zusätzliche Sicherheitsabfrage beim Einloggen (z. B. per SMS-Code).

11. Vorsicht vor kostenlosen Angeboten und Gewinnspielen

→ Oft verstecken sich dahinter Abo-Fallen oder Datensammler.

12. Was ist Phishing und wie schütze ich mich davor?

→ Betrugsversuche per E-Mail oder SMS – Links und Eingabefelder meiden.

13. Warum sind öffentliche WLAN-Netze gefährlich?

→ Daten können leicht mitgelesen werden – für sensible Dinge lieber mobile Daten nutzen.

14. Welche Einstellungen auf meinem Gerät erhöhen meine Sicherheit?

→ Automatische Updates, Geräte-Sperre, Standortfreigabe nur bei Bedarf.

15. Wie erkenne ich vertrauenswürdige Apps – und welche sollte ich meiden?

→ Nur Apps aus offiziellen App-Stores laden, Bewertungen beachten.

16. Was sollte ich beim Umgang mit sozialen Netzwerken beachten?

→ Vorsicht bei Freundschaftsanfragen, keine persönlichen Daten an Fremde senden.

17. Welche Warnzeichen deuten auf Betrug oder Datendiebstahl hin?

→ Ungewöhnliche Abbuchungen, fremde Logins, seltsame E-Mails oder SMS.

18. Was tun im Notfall? – Erste Hilfe bei Betrugsverdacht

→ Passwörter ändern, Bank informieren, Polizei kontaktieren.

19. Sicherheits-Checkliste: Bin ich gut geschützt?

→ Liste zum Abhaken: Passwörter, Virenschutz, Backups, Updates.

20. Nützliche Links, Telefonnummern und weitere Hilfsangebote

→ Polizei, Verbraucherschutz, Sperr-Notruf, hilfreiche Internetseiten für Senioren.

15. Schlusswort

Liebe Leserinnen und Leser,

Sie haben sich in dieser Broschüre mit vielen Themen rund um IT-Sicherheit beschäftigt – von sicheren Passwörtern über Schutzmaßnahmen am Smartphone bis hin zu Betrugserkennung und sicherem Online-Einkauf. Vielleicht war das für Sie eine neue Welt, vielleicht auch ein mutiger Schritt aus der eigenen Komfortzone. Wenn das so ist, dann dürfen Sie eines wissen: **Sie haben genau das Richtige getan.**

In unserer Gemeinde **Eching in Niederbayern** wird Zusammenhalt großgeschrieben. Wir helfen einander, wir tauschen uns aus und wir lassen niemanden zurück. **Genau dieses Miteinander ist auch im digitalen Leben wichtig.** Denn die Digitalisierung ist längst ein Teil unseres Alltags geworden – und sie bietet uns viele Möglichkeiten: Kontakt zu Familie und Freunden, sichere Bankgeschäfte von zu Hause, medizinische Beratung, Einkaufsmöglichkeiten und Zugang zu Wissen aus aller Welt. Aber diese Chancen können wir nur dann nutzen, wenn wir wissen, wie wir uns sicher bewegen.

Diese Broschüre soll Ihnen kein schlechtes Gefühl machen oder Angst verbreiten. Im Gegenteil: **Sie soll Ihnen Selbstvertrauen geben.** Digitale Sicherheit ist kein kompliziertes Spezialthema für Technikexperten – sie besteht aus einfachen und machbaren Schritten. Wer sichere Passwörter verwendet, Betrugsversuche erkennt und sein Smartphone schützt, ist bereits sehr gut vorbereitet. Sie haben nun das Rüstzeug, um bewusster und sicherer mit Technik umzugehen.

Niemand muss diesen Weg allein gehen. Genau dafür gibt es in Eching den **Digitalen Stammtisch**, den ich jeden Monat veranstalte. Dort treffen wir uns in entspannter Atmosphäre, sprechen über Fragen rund um Computer, Smartphones und Internet – verständlich, praktisch und ohne Fachchinesisch. **Sie sind herzlich eingeladen, dabei zu sein.** Denn gemeinsam lernen wir leichter, unterstützen uns gegenseitig und bleiben neugierig – ganz gleich in welchem Alter.

Bleiben Sie offen für Neues. Trauen Sie sich, Fragen zu stellen. Und lassen Sie sich von der digitalen Welt nicht einschüchtern – sie bietet viel Gutes, wenn man sie sicher nutzt.

Ich freue mich darauf, Sie vielleicht beim nächsten **Digitalen Stammtisch in Eching** begrüßen zu dürfen. Bis dahin: **Bleiben Sie sicher – und bleiben Sie digital selbstbestimmt.**

Mit herzlichen Grüßen,

Martin W. Steinbach
Eching / Weixerau
Telefon 0176 2215 3430

Digitaler Stammtisch Eching – Gemeinsam sicher im Internet und bleiben Sie neugierig

Stichwort-Verzeichnis

2

2FA 16, 20, 38, 56, 58

A

Abbuchungen 63, 64
Add-ons 34
Amazon 8, 20, 34, 40, 41, 42, 64, 77, 78, 80, 81
Android 18, 22, 58, 59, 68, 69, 70, 71, 72, 73, 75, 76
Angehörige 63, 77, 78, 79, 80, 81, 82, 83, 84, 85, 89, 93, 95, 96, 97, 98, 99
Anhänge 43, 51, 55, 60
Antiviren-Software 59
Antivirus 9, 44
Antivirus und Antimalware 9
Apple App Store 22, 60
Apple Pay 38
Apple-ID 88
Apple-Konten 88
Apps 8, 20, 22, 23, 24, 58, 59, 60, 61
Authentifikator 20
Automatische Sperre 58
Avira Phantom VPN 39

B

Backup 62, 67, 68, 71, 73, 74, 76
Backups 59, 60
Bankdaten 40, 41, 42, 43, 46
Banken 20, 41, 45, 46
Banking 20
Bankkarten 65
Bankkonto 45, 51
Bankmitarbeiter 45, 46, 49, 50
Bankverbindung 52
Behörden 46
Berechtigungen 23, 24, 59
Betriebssystem 100
Betrug 8, 24, 45, 50, 52, 53, 57, 59, 63, 64
Betrüger 4, 10, 28, 39, 45, 47, 49, 50, 52, 55, 56, 63, 64
Betrugsverdacht 62
Bewertungen 9, 22, 23, 24, 34, 36, 37, 39
Bezahldienste 77
Biometrische Daten 19
Bluetooth 59
Browser 31
BSI 8, 11, 15, 31, 61, 66

C

Checkliste 61, 62, 64
Chrome 29
Cloud-Speicher 77
Computer 4, 8, 10, 45, 59, 61, 101
CyberGhost 39

D

Datendiebstahl 50, 53
Daten-Nachlass 77
Datenschutz 37, 53, 57
Datensicherung 67
digitale Konten 77
Digitalen Erbe 86
Drohungen 41

E

eBay 20, 34, 64, 77, 78, 81, 82, 83
Edge 29, 31
EHI Siegel 36, 37, 38, 39
E-Mail-Konten 20, 77
E-Mails 8, 9, 39, 41, 42, 43, 44, 50, 60, 101
Enkeltrick 8, 45, 47, 48
Entsperrcodes 26
Entsperr-Methoden 25
Erbenregelungen 99
Erbnachweis 77

F

Facebook 10, 20, 23, 53, 55, 56, 57, 58, 62, 63, 64, 77, 93, 94, 97
Fake-Shop 33, 34
Fake-Shops 33, 34
Favoritenliste 39
Finanzamt 52
Fingerabdruck 19, 26, 34, 60, 61
Firefox 28, 29, 31, 55
Fotos 68

G

Gedenkzustand 93
Geldtransfers 46
Geldübergabe 47, 48
Gesichtserkennung 19, 26
Gewinnspiele 52, 56
Gmail 44
Google 17, 31, 58, 59, 60
Google Authenticator 17
Google Chrome 31, 55
Google Fotos 69, 73, 74, 76
Google Maps 23

Google Play Store 22, 60
Google-Konten 84

H

Hacker 13
Handynummern 48
https 28, 31, 34, 36
HTTPS 39, 40

I

IBAN 47, 48
iCloud 59, 69, 70, 71, 72, 74, 76
Instagram 20, 23, 97
Internetkriminalität 65
Internetverbindung 28, 39
iPhone 22, 55, 59, 69, 70, 71, 72, 74, 76
iPhones 58

J

Junk 43

K

Kalenderdaten 71, 72
Kartendaten 62
Käuferschutz 34, 36, 37, 38
Käuferschutzfunktionen 39, 40
Kleinanzeigen 78, 81, 82, 83
Kontakte 8, 22, 23, 56, 57, 59, 61, 67, 68, 71, 72, 73, 75
Kontoinaktivitätsmanager 84
Kreditkarte 31, 33, 34, 40, 45, 65
Kreditkarten 40, 65
Kreditkartenabrechnung 51
Kreditkarteninformationen 52
Kundenbewertungen 33, 39, 53
Kündigung 83
Künstliche-Intelligenz 48

L

LibreOffice 100
Lieferbedingungen 36
Links 9, 39, 41, 42, 43, 51, 53, 55, 57, 60, 61
Linux 100, 101, 102
Linux Mint 100
Login 16, 17, 19, 20, 39, 51

M

Malware 43
Menschenverstand 44
Messenger 43, 47, 48
Microsoft Edge 54
Microsoft Office 100
Mobile Geräte 22
Mobilfunkanbieter 51
Mobiltelefon 16
Mozilla Firefox 55
Muster 25

N

Nachlasskontakt 88, 93
Nachlassregelung 80, 83, 88, 95, 96, 97
Nachrichten 4, 9, 10, 22, 39, 41, 43, 50, 52, 53, 55, 60, 61, 64, 65, 67, 68, 71, 72, 73, 74, 75, 103
Netflix 21, 83, 84
NordVPN 39
Notfall 62, 64
Notfallnummer 63
Notlüge 47

O

offizielle Nummer 50
Online-Banking 8, 31, 77
Online-Konto 63
Online-Shop 9, 16, 33, 36, 38, 39, 40, 51
Online-Zugänge 77
OpenOffice 100
Outlook 44

P

Paketdienste 60
Passphrasen 12
Passwort 9, 10, 11, 16, 17, 19, 20, 38, 40, 44, 49, 56, 58, 59, 60, 61, 62
Passwortänderung 12
Passwort-App 58
Passwörter 8, 10, 11, 15, 28, 41, 42, 43, 46, 51, 53, 55, 58, 61, 62, 64
Passwörtern 15, 20, 31, 45, 52, 60
Passwort-Manager 14, 78
Passwortsicherheit 9
PayPal 20, 33, 34, 38, 39, 40, 41, 44, 78, 79, 80
PC 45, 59, 63, 100
Personalausweisdaten 42
persönliche Informationen 53, 55, 57
Phishing 8, 9, 20, 39, 40, 41, 42, 43, 44, 45, 55, 60
Phishing-E-Mails 8, 41
PIN 45, 46
PINs 42, 43, 45
Polizei 45, 46, 48, 49, 50, 61, 62, 63, 64, 65
Polizisten 49, 50

Preisausschreiben 52
Preisgeld 52

R

Rezensionen 9, 22, 23, 34

S

Safari 31, 55
Schloss-Symbol 28
Senioren 1, 2, 4, 8, 31, 49, 64, 66, 100
Sicherheit 1, 2, 4, 8, 15, 34, 36, 37, 38, 39, 43, 49, 58, 59, 61, 100, 102
Sicherheitsabfrage 61
Sicherheitslücken 23, 60
Sicherheitsüberprüfung 12
Sichern 67
Sicherungskopie 62
Sicherungstools 74
Siegel 36, 37, 38
Smartphone 4, 8, 19, 22, 52, 58, 59, 60, 61, 63
SMS 16, 17, 20, 38, 43, 60
Soziale Medien 20
Sozialen Medien 48
sozialen Netzwerken 20, 53, 55, 56, 57
Spam 43
Sperr-Notruf 65
SSL-Zertifikate 36
Standort 56, 59
Sterbeurkunde 77, 79, 80, 82, 88, 97
Strafzettel 52
Stripe 38
Synchronisierung 71, 72

T

Tablet 4, 58, 59, 61, 63
TAN 34
TANs 42, 43, 45, 46
Telefonbetrug 49
Telefonnummern 57, 65
Telefonseelsorge 66
Telegram 69, 73
Telegram-Konten 96
TikTok 97
TOTP 20
Trojaner 60
Trusted Shops 36, 37, 38, 39

U

Überweisungen 34, 45, 46
Ubuntu 100
Updates 23, 58, 60, 61, 100
USB-Stick 62, 70, 71

V

Verbraucherrechte 37
verbraucherzentrale 8, 31, 46
Verbraucherzentrale 8, 15, 31, 63, 64, 65, 102
verschlüsseln 39, 58
verschlüsselt 28
Vertrauensperson 48
vertrauenswürdig 23, 24, 28, 36
vertrauenswürdige 31, 34
vertrauenswürdigen 22, 23, 24, 34, 39, 40
Verwandte 4, 49
Viren 24, 45, 59, 60, 64, 100, 101
Virenscan 63
Virenschutzprogramm 31, 60
Vollmachten 99
VPN 39, 59

W

Werbeanrufe 52
WhatsApp 4, 8, 10, 22, 23, 47, 48, 49, 53, 56, 57, 60, 63, 64, 69, 72, 73, 76
WhatsApp-Konten 94
Wiederherstellung 67, 68, 71, 72, 73, 74, 75, 76
Windows 100, 101
Winux 100
WLAN 8, 31, 39, 59, 61, 62

X

X (Twitter) 97

Z

Zahlungsmethoden 28, 34
Zahlungsverkehr 38
ZenMate 39
Zertifikat 29, 30, 36
Zorin OS 100
Zugangsdaten 8, 41, 42, 46
Zugangsinformationen 45
Zwei-Faktor-Authentifizierung 16, 19, 20, 21, 34, 38, 40, 56, 57, 58, 61

16. Abbildungsverzeichnis

Hinweis 1 Zwei Faktor 16
Hinweis 2 SMS-Code 17
Hinweis 3 2FA-2Wege 18
Hinweis 4 Google Authenticator 19
Hinweis 5 PIN-Passwort-Muster 25
Hinweis 6 Tabelle mögliche Muster 25
Hinweis 7 Fingerabdruck 26
Hinweis 8 Gesichtserkennung 26
Hinweis 9 Entsperr-Codes 26
Hinweis 10 Sichere Verbindung 28
Hinweis 11 Sichere Webseite 30
Hinweis 12 Unsichere Webseite 30
Hinweis 13 Übersicht sichere Verbindungen 30
Hinweis 14 Prüfsiegel 35
Hinweis 15 Trusted Shop Siegel 36
Hinweis 16 EHI Siegel 37
Hinweis 17 Telefonbetrug 46
Hinweis 18 Enkeltrick 49
Hinweis 19 Betrügerische Anrufe 50
Hinweis 20 Suchmaschinen Alternative 54
Hinweis 21 Google Konto Foto sichern 69
Hinweis 22 iPhone Fotos sichern 70
Hinweis 23WhatsApp sichern 72
Hinweis 24 iCloud Backup 75
Hinweis 25 Einloggen In Google Konto 85
Hinweis 26 Daten und Datenschutz 86
Hinweis 27 Digitales Erbe 86
Hinweis 28 Einstellungen Digitales Erbe 86
Hinweis 29 Google Kontolöschen 87
Hinweis 30 Google: Verwaltung Nutzer 87
Hinweis 31 Einstellungen „Digitales Erbe 87
Hinweis 32 Apple Konto Einloggen 89
Hinweis 33 Apple Nachlasskontakt 90
Hinweis 34 Nachlasskontakt auswählen 90
Hinweis 35 Apple Zugriffs-Schlüssel speichern 91
Hinweis 36 Apple Zugriffs-Schlüssel 91
Hinweis 37 Facebook Gedenkzustand 94
Hinweis 38 Facebook Berechtigter 94
Hinweis 39 Vergleich Soziale Medien 98
Hinweis 40 Linux Vorteile 101
Hinweis 41 Vergleich Windows - Linux 102
Hinweis 42 Windows - Linux in aller Kürze 102