INTERNET-SICHERHEIT FÜR EINSTEIGER

PASSWORT SICHERHEIT

Wichtige Tipps zur sicheren Internetnutzung

Martin W. Steinbach

martinwsteinbach@gmail.com

WAS DENKEN SIE?

„WIE VIEL PROZENT ALLER ERFOLGREICHEN CYBERANGRIFFE GELINGEN AUFGRUND SCHWACHER ODER GESTOHLENER PASSWÖRTER?“

👉 QUELLE: VERIZON DATA BREACH INVESTIGATIONS REPORT (DBIR)

Antwort:
Über 80 %

„WIE VIELE MINUTEN BRAUCHT EIN ANGREIFER, UM EIN 8-STELLIGES PASSWORT OHNE SONDERZEICHEN ZU KNACKEN?“

👉 QUELLE: HIVE SYSTEMS. HTTPS://WWW.HIVESYSTEMS.IO/BLOG/PASSWORD-TABLE-2023

< 1
Sekunde

EINFÜHRUNG IN DIE INTERNET-SICHERHEIT

WARUM INTERNET-SICHERHEIT WICHTIG IST

Schutz persönlicher Informationen

Die Sicherheit im Internet ist entscheidend, um persönliche Informationen vor unbefugtem Zugriff zu schützen und Identitätsdiebstahl zu vermeiden.

Zielgruppe Senioren

Senioren sind oft Ziel von Betrügern, die versuchen, an ihre sensiblen Daten zu gelangen. Aufklärung ist wichtig.

Grundlagen der Internet-Sicherheit

Ein grundlegendes Verständnis der Internet-Sicherheit kann helfen, Bedrohungen zu erkennen und zu minimieren.

G IST

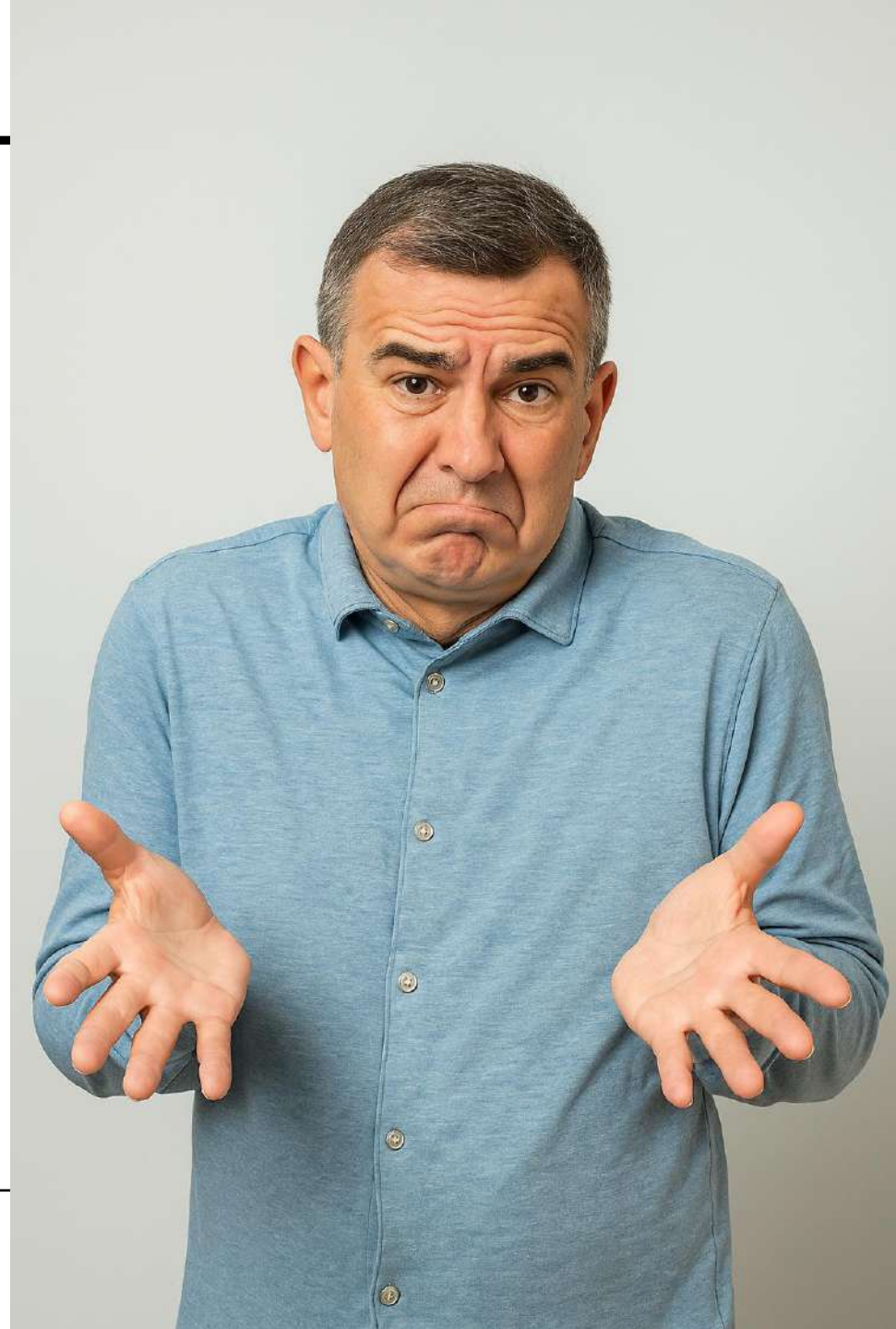
e Informationen vor
vermeiden.

e sensiblen Daten zu

n helfen, Bedrohungen zu

WARUM SOLLTE GERADE ICH EIN SICHERES PASSWORT BRAUCHEN?

- **Automatisierte Angriffe:**
  Hacker wählen keine Personen aus, sondern greifen massenhaft an.
- **Identitätsdiebstahl:**
  Ein kompromittiertes Konto kann missbraucht werden.
- **Zugänge sind wertvoll:**
  Selbst ohne Geld werden Konten für Betrug genutzt.
- **Schutz anderer:**
  Dein Konto kann zur Verbreitung von Malware oder Phishing dienen.



WAS BEDEUTET PASSWORTSICHERHEIT

DIE ROLLE VON PASSWÖRTERN IM ALLTAG

Sicherheit von Passwörtern

Passwörter sind entscheidend für die Sicherheit unserer digitalen Identität und schützen wichtige persönliche Informationen vor Cyberangriffen.

Schutz von Online-Konten

Ein sicheres Passwort schützt unsere E-Mails, Bankkonten und sozialen Medien vor unbefugtem Zugriff und Missbrauch.

Best Practices für Passwörter

Sichere Passwörter sollten komplex und einzigartig sein, um die Wahrscheinlichkeit eines erfolgreichen Hackerangriffs zu verringern.

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.

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/

Vermeidung unsicherer Passwörter

Unsichere Passwörter machen Ihr Konto anfällig für Angriffe. Verwenden Sie stärkere Alternativen.

Erforderliche Passwortstärke

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

WIE ERSTELLE ICH SICHERE UND LEICHT MERKBARE PASSWÖRTER

FALLBEISPIEL: SICHERES PASSWORT ERSTELLEN

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"

Sicherheitsbewusstsein

Es ist wichtig, sich des Sicherheitsbewusstseins bewusst zu sein, um Phishing und andere Bedrohungen zu vermeiden.

WIE SICHER IST IHR PASSWORT? EINE EINSCHÄTZUNG

Sicherheitsüberprüfung

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

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

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

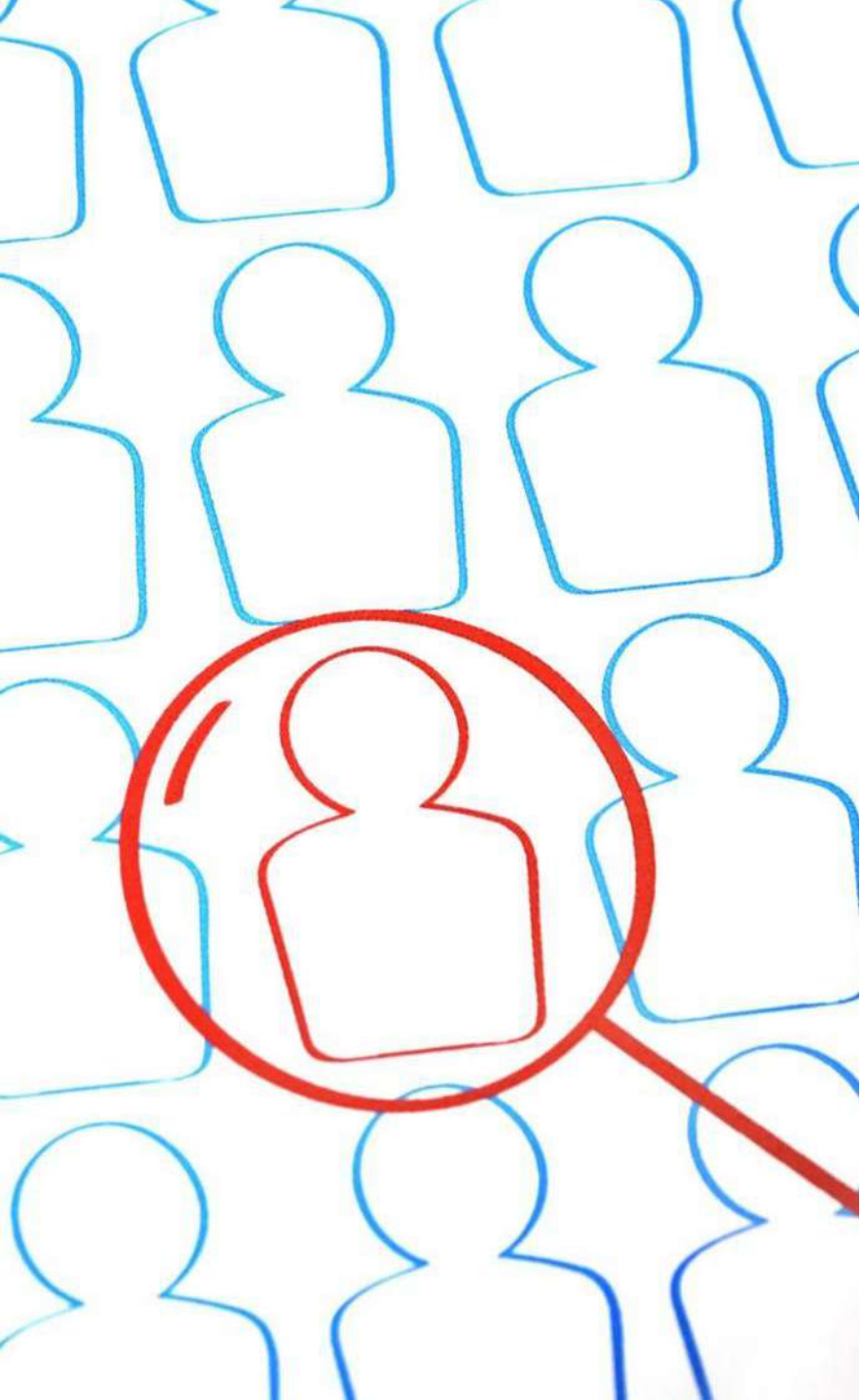
haveibeenpwned.com

Anfälligkeit für Angriffe

Passwörter können anfällig für verschiedene Arten von Angriffen sein, daher ist die Überprüfung entscheidend.

Tipps zur Verbesserung

Das Verwenden von komplexen Passwörtern und Passwort-Managern kann die Sicherheit erheblich verbessern.



SO MACHEN SIE IHR PASSWORT SICHER: TECHNIKEN UND TIPPS

Verwendung von Passphrasen

Passphrasen sind länger und komplexer, was die Sicherheit erhöht und es Hackern erschwert, sie zu knacken.

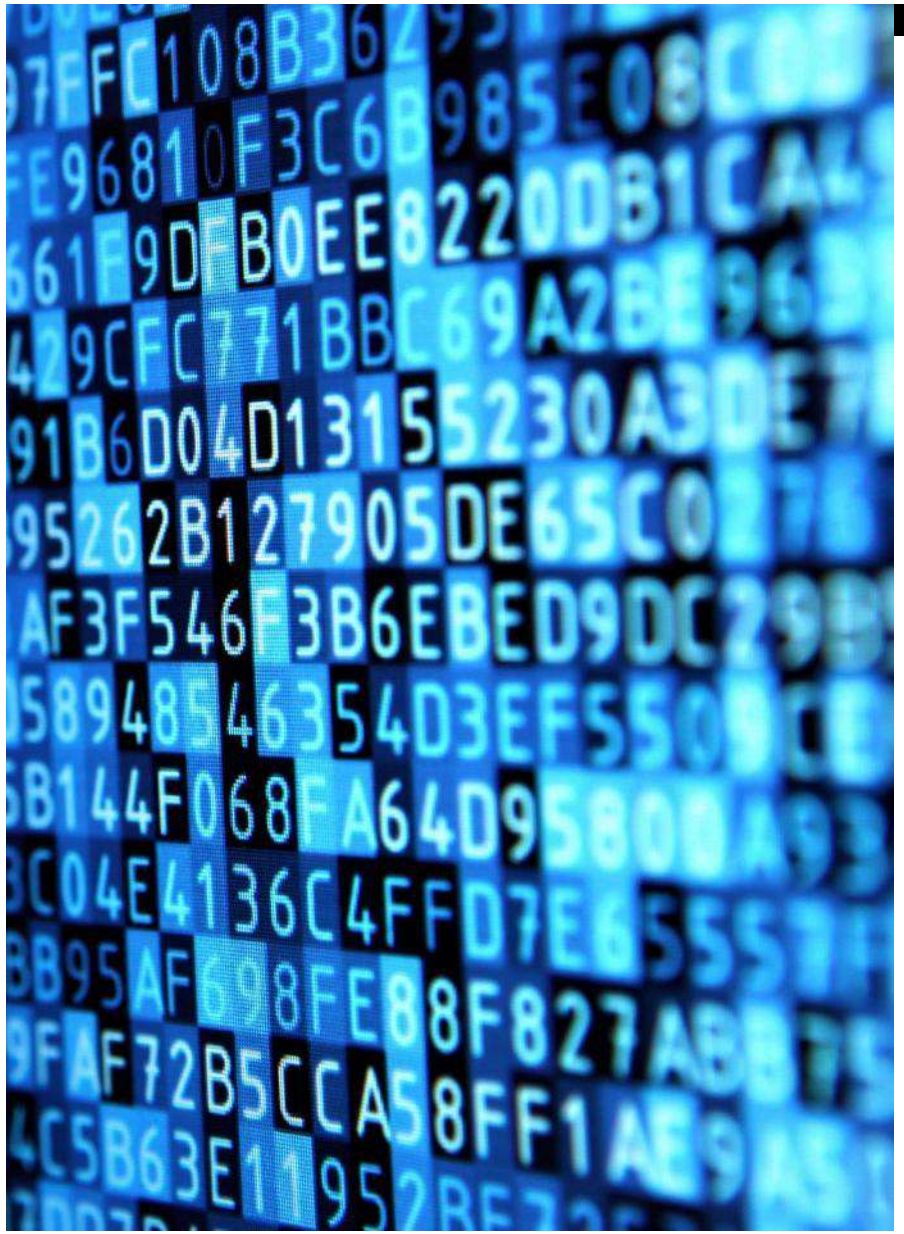
Kombination von Zeichen

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.

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



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

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

PASSWORT-MANAGER (1)
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.

PASSWORT-MANAGER ()

🛡️ 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

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.

WAS IST ZWEI-FAKTOR-AUTHENTIFIZIERUNG

WIE FUNKTIONIERT ZWEI-FAKTOR-AUTHENTIFIZIERUNG (2FA)?

Zwei Identifikationsformen

Die Zwei-Faktor-Authentifizierung (**2FA**) erfordert **zwei verschiedene** Identifikationsmethoden für mehr Sicherheit bei der Anmeldung.

Schutz vor unbefugtem Zugriff

2FA bietet einen **zusätzlichen Schutzschild**, um unbefugten Zugriff auf persönliche oder geschäftliche Konten zu verhindern.

Anwendung von 2FA

Zwei-Faktor-Authentifizierung wird in vielen Online-Diensten eingesetzt, um die **Sicherheit von Benutzerdaten** zu erhöhen.

BEISPIEL 1: LOGIN MIT PASSWORT + SMS-CODE

Zwei-Faktor-Authentifizierung

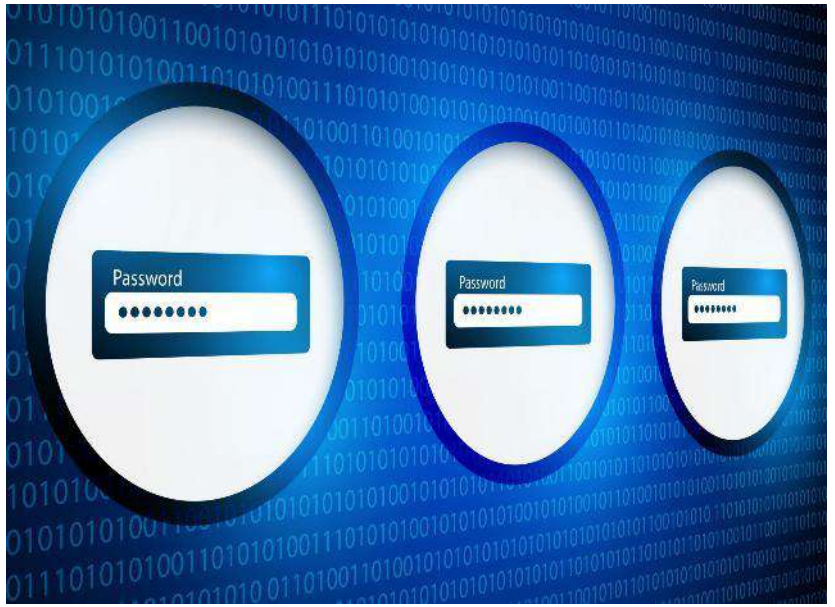
Die Zwei-Faktor-Authentifizierung (2FA) erhöht die Sicherheit, indem sie eine zusätzliche Authentifizierungsebene hinzufügt.

Passwort-Schutz

Ein starkes Passwort ist der erste Schritt zum Schutz Ihres Kontos vor unbefugtem Zugriff.

SMS-Code

Der SMS-Code, der an Ihr Mobiltelefon gesendet wird, stellt sicher, dass nur Sie auf Ihr Konto zugreifen können.



BEISPIEL S-CODE

Zw

Die
di
A

Pas

Ein
So

SM

Der
wi
zu

Ist das Endgerät kompromittiert, kann auch der SMS-Code abgefangen werden – Zwei-Faktor heißt nicht automatisch Zwei-Wege-Sicherheit.

BEISPIEL 2: LOGIN MIT PASSWORT + AUTHENTIFIZIERUNGS-APP

Sichere Anmeldung

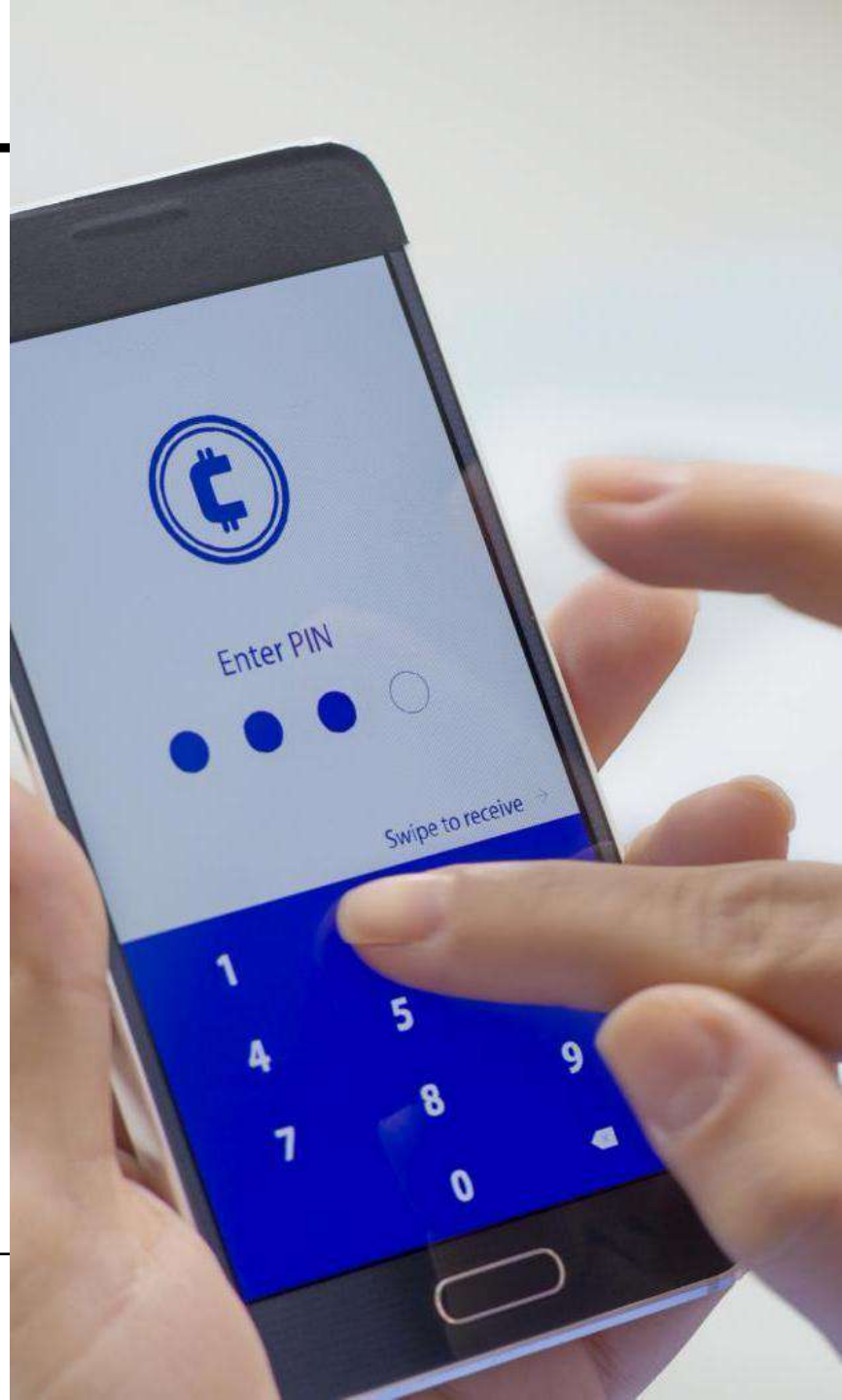
Die Verwendung einer Authentifizierungs-App erhöht die Sicherheit der Anmeldung durch die zusätzliche Eingabe eines zeitlich begrenzten Codes.

Zeitlich begrenzte Codes

Die Authentifizierungs-App generiert Codes, die nur für eine kurze Zeit gültig sind, was das Risiko unerlaubter Zugriffe verringert.

Benutzerfreundlichkeit

Die Kombination von Passwort und zeitlich begrenztem Code macht die Anmeldung benutzerfreundlich und sicher.



BEISPIEL AUTHENTIF

Sichere Anmeldung

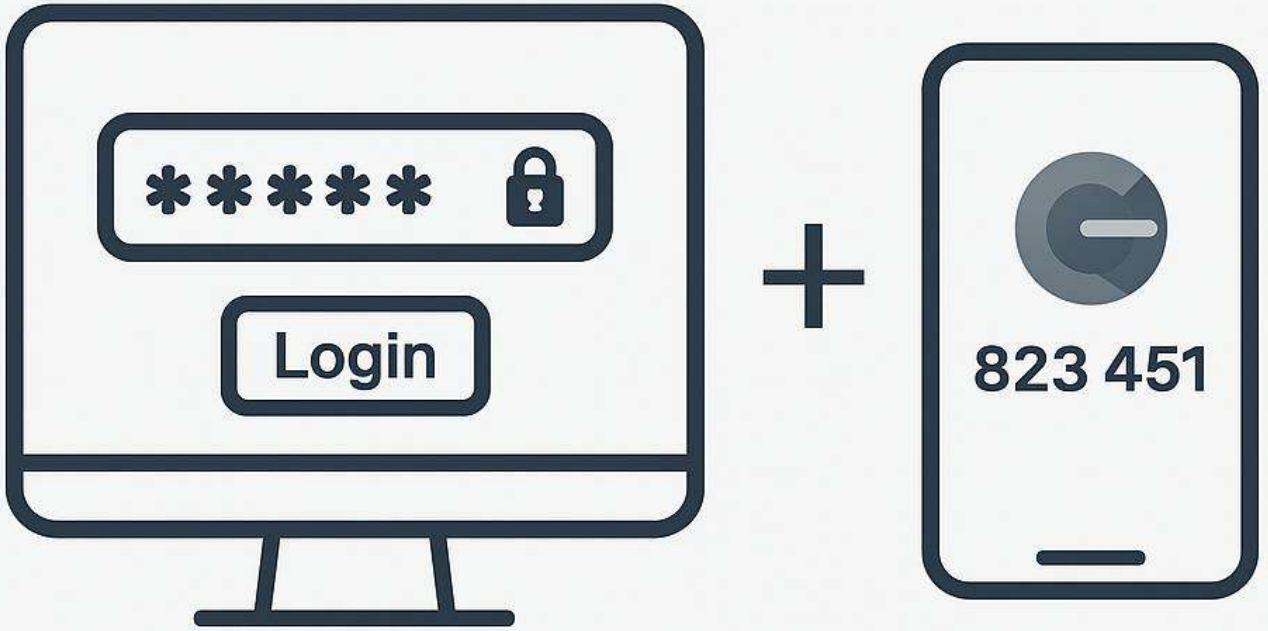
Die Verwendung einer A
durch die zusätzliche Ein

Zeitlich begrenzte Code

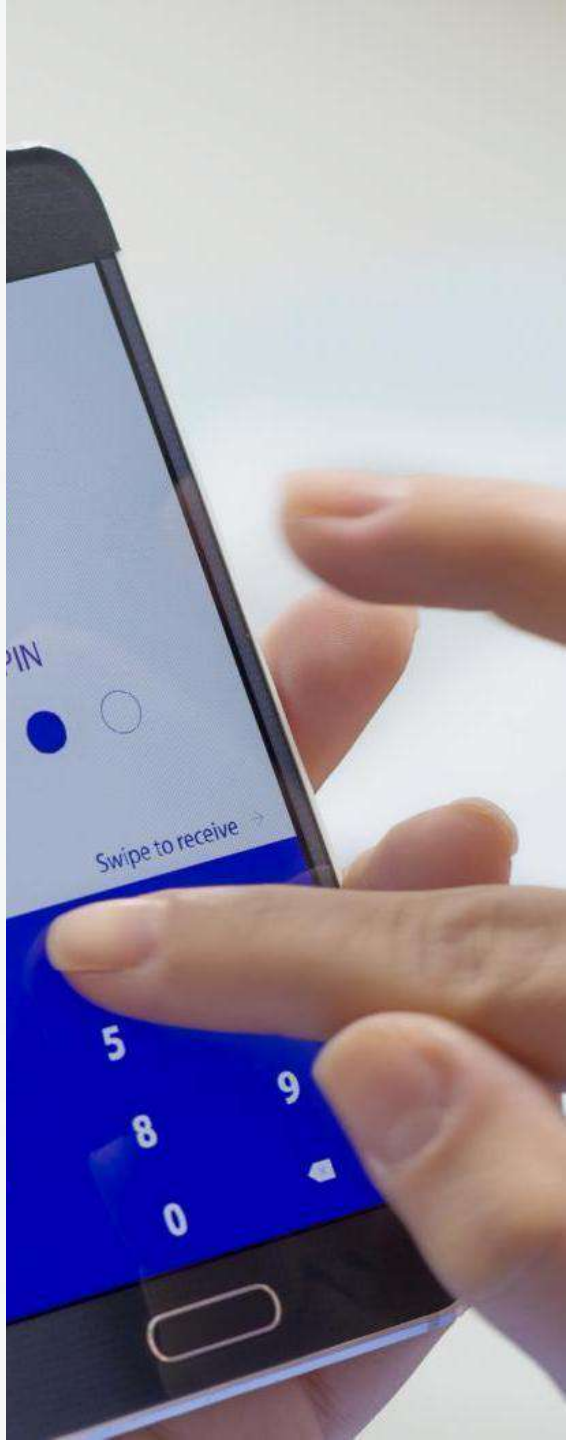
Die Authentifizierungs-A
was das Risiko unerlaubt

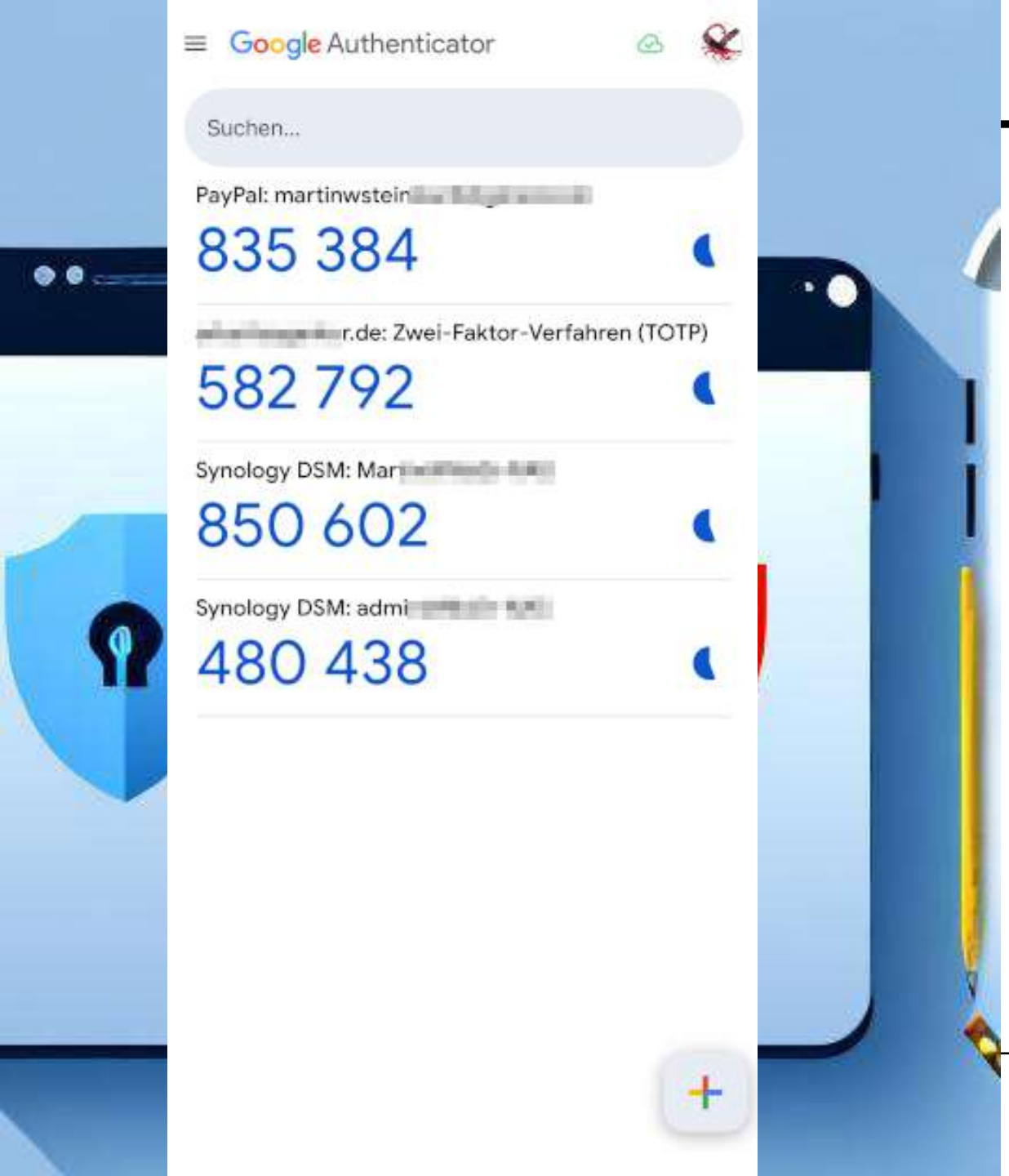
Benutzerfreundlichkeit

Die Kombination von Pa
benutzerfreundlich und s



Besser: Zwei Faktoren UND zwei Wege





🔐 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.

ÜBERSICHT BELIEBTER KONTEN MIT TOTP (1)

- ✅ **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**

ÜBERSICHT BELIEBTER KONTEN MIT TOTP (2)

- ✅ **Online-Shopping & Bezahldienste**
- **Amazon** (TOTP möglich, aber leicht versteckt)
- **PayPal** (TOTP indirekt via Sicherheitsschlüssel oder YubiKey, eingeschränkt mit Tricks)
- **eBay**
- **Etsy**
- **Shopify**

- ✅ **Cloud & Speicher**
- **Dropbox**
- **Google Drive**
- **Microsoft OneDrive**

ÜBERSICHT BELIEBTER KONTEN MIT TOTP (3)

- ✅ **Streaming & Medien**
- **Netflix** *(aktuell kein TOTP – aber account sharing führt zu Missbrauchsrisiko)*
- **Spotify** *(keine native TOTP-2FA, aber 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

BEISPIEL 3: LOGIN MIT PASSWORT + BIOMETRISCHE DATEN (FINGERABDRUCK ODER GESICHTSERKENNUNG)

Sichere Identitätsbestätigung

Die Kombination aus Passwort und biometrischen Daten stellt eine hochsichere Methode zur Bestätigung der Identität dar.

Fingerabdruck-Authentifizierung

Die Verwendung von Fingerabdrücken als Teil der Authentifizierung erhöht die Sicherheit erheblich und minimiert das Risiko unbefugten Zugriffs.

Gesichtserkennungstechnologie

Gesichtserkennung bietet eine benutzerfreundliche Möglichkeit zur Authentifizierung und ergänzt herkömmliche Passwörter.

WARUM IST ZWEI-FAKTOR-AUTHENTIFIZIERUNG WICHTIG?

Zusätzliche Sicherheitsebene

Die Zwei-Faktor-Authentifizierung fügt eine zusätzliche Schicht an Sicherheit hinzu, die für den Schutz von Konten unerlässlich ist.

Schutz bei Passwortkompromittierung

Selbst wenn ein Passwort gestohlen wird, bleibt das Konto durch die zweite Authentifizierung weiterhin geschützt.

ZUSAMMENFASSUNG UND WICHTIGE ASPEKTE

Zusätzliche Sicherheitsebene

Die Zwei-Faktor-Authentifizierung (2FA) bietet eine wichtige zusätzliche Sicherheitsebene zum Schutz von Online-Konten.

Schutz für Senioren

Senioren sollten die Vorteile der 2FA nutzen, um ihre digitalen Konten gezielt zu sichern und vor Cyber-Bedrohungen zu schützen.

SCHLUSSFOLGERUNG

Bedeutung der Internet-Sicherheit

Internet-Sicherheit ist für alle wichtig, besonders für Senioren, die häufig Ziel von Cyberangriffen sind.

Kenntnisse und Werkzeuge

Mit den richtigen Kenntnissen und Werkzeugen können wir uns effektiv vor Cyberbedrohungen schützen.

Lernen und Anwenden

Es ist wichtig, kontinuierlich zu lernen und die erlernten Strategien zur Verbesserung der Online-Sicherheit anzuwenden.