

## Warum einfache Passwörter so gefährlich sind

„123456“, „passwort“, „hallo123“ – das sind echte Beispiele für die meistgenutzten Passwörter weltweit.

Sie sind bequem, leicht zu merken – und genau das ist das Problem.

Denn:

- Solche Passwörter lassen sich **in Sekunden knacken** – mit automatisierten Programmen.
- Hacker haben Zugang zu **riesigen Listen mit Millionen gestohlener Passwörter**.

Sie testen sie einfach durch – bei E-Mails, Onlineshops, sozialen Netzwerken.

- Viele Menschen verwenden **dasselbe Passwort für mehrere Konten** – wenn eins gehackt wird, sind oft alle anderen mitgefährdet.

### Was kann passieren?

- Fremde lesen deine Mails mit
- Bestellungen auf deinen Namen
- Zugriff auf Cloud, Fotos, Kontakte
- Und im schlimmsten Fall: **Identitätsdiebstahl**

### Aber ich bin doch kein Promi?

Auch egal.

Angreifer suchen nicht gezielt nach berühmten Menschen – sie greifen **tausende Konten automatisch** an und nehmen, was sie kriegen. Und: Viele Datenlecks passieren nicht durch „Hacker mit Kapuze“ – sondern schlicht durch **unsichere Passwörter**.

Ein schlechtes Passwort ist wie eine Wohnungstür ohne Schloss. Du brauchst keinen Alarm – du brauchst erstmal einen Riegel, der hält.

## Was ein gutes Passwort wirklich ausmacht

Ein gutes Passwort ist **wie ein starker Schlüssel**:

Es schützt deinen digitalen Raum – auch wenn jemand versucht, ihn aufzubrechen.

Aber was genau macht ein Passwort sicher?

### Die 4 goldenen Regeln:

**Danke sagen?** Kto.Inh: André Hoek, IBAN: BE20 9053 4733 2856, BIC: TRWIBEB1XXX, Wise, Rue de Trone 100, 3rd floor, Brussels, 1050, Belgium; *SEPA-Überweisung- Keine Gebühren* - Verwendungszweck: "Dankeschön"

1. **Lang – mindestens 12 Zeichen, besser 16 oder mehr**

Je länger, desto besser. Kurze Passwörter sind viel leichter zu knacken.

2. **Komplex – Buchstaben, Zahlen, Sonderzeichen mischen**

Kein echtes Wort, kein Geburtsdatum, kein „Hallo123“.

3. **Einzigartig – für jedes Konto ein anderes Passwort**

Niemals dasselbe Passwort für verschiedene Dienste verwenden.

4. **Nicht erratbar – keine Namen, keine Hobbys, keine Klassiker**

Also kein „Schatz123“, kein „Sommer2023“ und bitte kein „123456“.

**Ein sicheres Passwort könnte z. B. so aussehen:**

Gr8!jPfR#w4Z\$91m

Das ist schwer zu merken – aber **du musst es dir gar nicht merken**, wenn du einen Passwort-Manager nutzt (dazu gleich mehr).

**Tipp für ein „merkbares“ starkes Passwort (wenn du doch eins brauchst):**

Nutze einen **Satz aus vier oder fünf zufälligen Wörtern**, z. B.:

Mütze-Apfel-Mond3-Regal!

Einfach zu merken – aber trotzdem schwer zu knacken.

Je länger, einzigartiger und unlogischer dein Passwort ist,

desto schwerer ist es zu knacken – und desto sicherer bist du.

## Warum du dir das alles nicht merken musst – Passwort-Manager erklärt

Viele Menschen wissen: Man sollte für jeden Dienst ein eigenes, langes Passwort verwenden. Aber dann kommt sofort die nächste Frage: „**Wie soll ich mir das alles merken?**“ Die Antwort: **Gar nicht.**

Dafür gibt es Passwort-Manager.

### Was ist ein Passwort-Manager?

Ein Passwort-Manager ist wie ein **digitaler Tresor**:

**Danke sagen?** Kto.Inh: André Hoek, IBAN: BE20 9053 4733 2856, BIC: TRWIBEB1XXX, Wise, Rue de Trone 100, 3rd floor, Brussels, 1050, Belgium; *SEPA-Überweisung- Keine Gebühren* - Verwendungszweck: „Dankeschön“

Er speichert all deine Passwörter verschlüsselt – und trägt sie automatisch ein, wenn du dich irgendwo anmeldest. Du brauchst dir nur **ein einziges, starkes Masterpasswort** merken. Den Rest übernimmt das Programm für dich.

### Was bringt dir das?

- Du musst dir keine Passwörter mehr merken
- Du kannst für jeden Dienst ein anderes, sicheres Passwort nutzen
- Du sparst Zeit beim Einloggen
- Du vermeidest doppelte oder unsichere Passwörter
- Deine Daten sind stark verschlüsselt und nur für dich zugänglich

### Wo werden die Daten gespeichert?

Das hängt vom Anbieter ab. Viele Passwort-Manager bieten dir die Wahl:

- **In der Cloud** (praktisch für mehrere Geräte, z. B. Handy & Laptop)
- **Lokal auf deinem Gerät** (nur für dich, ohne Verbindung zum Internet)

Beides kann sicher sein – wichtig ist, **welchen Anbieter du wählst**

(Dazu gleich mehr unter Punkt 4: Bitwarden).

Ein Passwort-Manager macht dein digitales Leben **sicherer und einfacher** – statt ständig neue Passwörter zu erfinden oder unsichere wiederzuverwenden.

## Bitwarden als Einstieg – kostenlos, sicher, einfach

Es gibt viele Passwort-Manager. Aber einer der besten für Einsteiger (und Fortgeschrittene) ist:

**Bitwarden** – kostenlos, quelloffen, sicher und leicht verständlich.

### Warum Bitwarden?

- **Kostenlos** für alle wichtigen Funktionen
- **Open Source** – der Quellcode ist öffentlich einsehbar
- **Verschlüsselte Speicherung** – niemand außer dir kann deine Passwörter lesen
- **Einfach zu bedienen** – auf Handy, PC oder im Browser
- **Synchronisation über Geräte hinweg** – ideal für Alltag & Arbeit

### So funktioniert Bitwarden:

1. Du erstellst ein **Masterpasswort** – das ist der Schlüssel zu deinem Passwort-Tresor
2. Du speicherst deine Passwörter im Programm – oder lässt sie automatisch erzeugen
3. Wenn du dich irgendwo einloggst, **füllt Bitwarden die Felder automatisch aus**
4. Neue Logins werden erkannt und können gespeichert werden

5. Du kannst sichere Passwörter per Klick generieren lassen

### Auf welchen Geräten läuft Bitwarden?

- Als **App** für Android & iPhone
- Als **Browser-Erweiterung** für Firefox, Brave, Chrome etc.
- Als **Web-Zugang** über bitwarden.com
- Als **Desktop-Programm** für Windows, macOS und Linux

### Was kostet es?

- Die Basis-Version ist **dauerhaft kostenlos**
- Es gibt eine „Premium“-Version (ca. 10 € pro Jahr), aber die brauchst du nicht unbedingt

Wenn du einen vertrauenswürdigen, kostenlosen und einfach zu bedienenden Passwort-Manager suchst, ist Bitwarden ein idealer Einstieg – selbst für Menschen, die bisher nichts mit Technik am Hut hatten.

## Zwei-Faktor-Authentifizierung – Der Extra-Schutz

Ein sicheres Passwort ist gut – aber **zwei Faktoren sind besser**.

Zwei-Faktor-Authentifizierung (kurz: **2FA**) bedeutet:

Du brauchst **zwei Dinge**, um dich einzuloggen:

1. Dein **Passwort**
2. Einen **zweiten Nachweis**, den nur du hast – z. B. einen Code auf deinem Handy

### Warum ist das so wichtig?

Selbst wenn jemand dein Passwort kennt (z. B. durch ein Datenleck), kann er **ohne den zweiten Faktor** nichts mit deinem Konto anfangen. 2FA ist wie ein zweites Schloss an deiner Tür – und oft das, was einen Angriff **im letzten Moment stoppt**.

### Welche Arten von 2FA gibt es?

- **TAN per SMS oder E-Mail**

Einfach, aber nicht besonders sicher – kann abgefangen werden

- **Authentifizierungs-App**

Z. B. **Aegis**, **FreeOTP**, **Authy** oder **Bitwarden Authenticator**

Diese Apps zeigen alle 30 Sekunden einen neuen Einmal-Code an

Den gibst du beim Login zusätzlich ein

- **Hardware-Token**

Ein physischer USB-Stick, den du beim Einloggen einsteckst Sehr sicher, aber eher etwas für Fortgeschrittene

### **Wie richte ich das ein?**

1. Gehe in den Einstellungen des jeweiligen Kontos (z. B. Mail, Cloud, Bank, Amazon)
2. Suche nach „**Zwei-Faktor-Authentifizierung**“ oder „**Sicherheitsoptionen**“
3. Wähle „per App“ – und scanne den QR-Code mit deiner Authenticator-App
4. Ab jetzt brauchst du beim Einloggen **dein Passwort + den Code aus der App**

### **Tipp:**

2FA lohnt sich vor allem bei wichtigen Konten: E-Mail, Bank, Cloud, Online-Shops, soziale Netzwerke

### **Fazit:**

Zwei-Faktor-Authentifizierung ist ein kleiner Schritt mit großer Wirkung. Ein zusätzlicher Code – und deine wichtigsten Daten sind deutlich besser geschützt.

## **Erste Schritte – So fängst du heute noch an**

Du musst nicht dein ganzes digitales Leben auf einmal umkrempeln.

Schon **ein kleiner erster Schritt** kann einen großen Unterschied machen.

### **Schritt 1: Wähle einen Passwort-Manager**

➔ **Empfehlung für den Einstieg:** [bitwarden.com](https://bitwarden.com)

Lade dir die App oder die Browser-Erweiterung herunter und erstelle dein Masterpasswort.

Ab jetzt brauchst du nur noch **dieses eine Passwort** im Kopf zu behalten.

### **Schritt 2: Ersetze unsichere Passwörter nach und nach**

Starte mit deinen wichtigsten Konten:

- E-Mail
- Online-Banking
- Cloud-Dienste
- Shopping-Portale (z. B. Amazon)
- Soziale Netzwerke

Erstelle für jedes dieser Konten ein neues, sicheres Passwort. Du musst das nicht an einem Tag machen – **eins nach dem anderen reicht.**

### **Schritt 3: Aktiviere Zwei-Faktor-Authentifizierung**

Wo immer es möglich ist: Gehe in die Sicherheitseinstellungen und schalte 2FA ein – am besten mit einer App wie Aegis oder Authy.

### **Schritt 4: Bleib ruhig und geduldig**

Die ersten Minuten mit einem Passwort-Manager sind vielleicht neu – aber nach ein, zwei Tagen willst du ihn nicht mehr missen. Du wirst merken, wie viel einfacher und sicherer es ist, wenn du dich **nicht mehr auf dein Gedächtnis verlassen musst.**

### **Und wenn du Fragen hast?**

Du kannst dich jederzeit bei mir melden – per E-Mail oder Telefon (Kontaktdaten im Impressum). Ich helfe gern weiter.

### **Sicherheit beginnt nicht mit Technik, sondern mit einer Entscheidung.**

Und diese Entscheidung kannst du heute treffen.