AEDIAEVUM LEITFADENREIHE

Sichere Passwörter & geschützte Accounts

Ihr Leitfaden für mehr Sicherheit im Internet

Für Jugendliche, Eltern und alle, die sicher im Netz unterwegs sein wollen

Herausgegeben von der aediaevum Stiftung · Mühltal · Juni 2026

Ob Online-Banking, E-Mail oder Schulplattform: Überall brauchen wir Passwörter. Doch viele Menschen nutzen Passwörter, die innerhalb von Sekunden geknackt werden können. Dieser Leitfaden zeigt, wie Sie sich mit einfachen Mitteln wirkungsvoll schützen — ohne technisches Vorwissen.

---

1. Warum Passwörter so wichtig sind

Ein schwaches oder mehrfach verwendetes Passwort ist das häufigste Einfallstor für Kriminelle. Einmal geknackt, haben Angreifer Zugang zu E-Mails, Online-Banking, sozialen Netzwerken und Einkaufskonten — oft ohne dass die Betroffenen es bemerken.

Besonders häufig passiert das durch:

- Datenpannen bei Online-Diensten, bei denen Millionen von Passwörtern gestohlen werden
- Phishing-Mails, die zur Eingabe von Zugangsdaten auf gefälschten Seiten verleiten
- Automatisierte Angriffe, die millionenfach gängige Passwörter ausprobieren
- Schadsoftware, die Tastatureingaben aufzeichnet (Keylogger)

Das sagen die Zahlen

• 61 % der Internetnutzer in Deutschland wurden in den letzten 12 Monaten Opfer von Cyberkriminalität (Bitkom Research 2025).

• Der durchschnittliche Schaden je Betroffenem lag bei 219 Euro.

• Nur rund ein Viertel der Betroffenen erstattete Strafanzeige bei der Polizei.

2. Was ein starkes Passwort ausmacht

Ein starkes Passwort ist lang, zufällig und einzigartig. Folgende Eigenschaften machen ein Passwort sicher:

Länge	Mindestens 12 Zeichen, besser 16 oder mehr.
Zeichenvielfalt	Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen kombinieren.
Keine Wörter	Keine echten Wörter, Namen, Geburtstage oder Tastaturmuster wie ‘qwerty’.
Einzigartigkeit	Jeder Dienst bekommt ein eigenes Passwort — niemals wiederverwenden.

Gut und schlecht im Vergleich

■ So nicht	✓ So besser
hund123	rT!9mX#qLv2@wZ
Maria1990	Kaffee-Regenschirm-7-Sterne
Dasselbe Passwort überall	Für jeden Dienst ein eigenes Passwort
geheim	Einen Passwort-Manager nutzen

3. Der einfache Trick: Passphrasen

Wer sich kein zufälliges Passwort merken kann, nutzt am besten eine Passphrase: eine Kette aus vier oder mehr zufälligen, nicht zusammenhängenden Wörtern.

Beispiel einer Passphrase

• Tasse · Wolke · Fahrrad · 17 · Stern

• → Ergibt: TasseWolkeFahrrad17Stern

• Lang, leicht zu merken, schwer zu knacken.

4. Passwort-Manager: Das Gedächtnis, das nie vergisst

Für jeden Dienst ein eigenes, starkes Passwort zu nutzen ist nur realistisch, wenn man sich nicht alle merken muss. Genau dafür gibt es Passwort-Manager.

Empfehlenswerte kostenlose Passwort-Manager:

- Bitwarden (Open Source, kostenlos, für alle Geräte)

• KeePassXC (lokal gespeichert, kein Cloud-Zwang)

5. Zwei-Faktor-Authentifizierung (2FA)

Selbst das stärkste Passwort kann gestohlen werden. Die Zwei-Faktor-Authentifizierung (2FA) ist ein zweiter Schutzriegel: Zusätzlich zum Passwort muss man beim Einloggen einen einmaligen Code eingeben.

1. Gehen Sie in die Einstellungen des jeweiligen Dienstes.
2. Suchen Sie nach ‚Sicherheit' oder ‚Zwei-Faktor-Authentifizierung'.
3. Laden Sie eine Authenticator-App herunter (z. B. Google Authenticator, Aegis).
4. Verknüpfen Sie die App mit dem Dienst — fertig.

6. Ihre persönliche Sicherheits-Checkliste

■	Jeder Online-Dienst hat ein eigenes Passwort.
■	Kein Passwort ist kürzer als 12 Zeichen.
■	Ich nutze einen Passwort-Manager.
■	Mein E-Mail-Konto ist mit 2FA geschützt.
■	Mein Online-Banking ist mit 2FA geschützt.
■	Ich gebe mein Passwort niemals weiter.

aediaevum Stiftung · In der Röde 5 · 64367 Mühltal · Gemeinnützige Stiftung zur Förderung der Kriminalprävention
Stiftungsaufsicht: Regierungspräsidium Darmstadt · Stand: 21.06.2026 · Dieses Dokument darf kostenlos ausgedruckt und weitergegeben werden.