

Deine Konto-Festung in 8 Schritten

Selbst wenn dich ein Betrüger einmal erwischt — mit diesen acht Einstellungen begrenzt du den Schaden auf einen Bruchteil und machst deinem Geld eine Festung.

Betrug ist ein Massenphänomen: Über 6 von 10 Internetnutzern waren 2025 betroffen (Bitkom 2025). Du kannst nicht jeden Angriff verhindern — aber du kannst dafür sorgen, dass ein einzelner Angriff dich nicht ruiniert. Jeder Haken auf dieser Liste ist eine zusätzliche Mauer. Du musst nicht alles an einem Tag erledigen. Arbeite dich von oben nach unten durch.

Wichtiger Hinweis: Diese Checkliste ist eine Orientierungshilfe, keine Rechts- oder Finanzberatung. Stand 2026. Die genauen Menüpunkte heißen in jeder Banking-App etwas anders — im Zweifel ruf die Servicenummer deiner Bank an und lass dich durchführen.

Schritt 1 — Tageslimit senken

Das Tageslimit bestimmt, wie viel an einem Tag von deinem Konto abgehen kann. Ein niedriges Limit deckelt jeden Schaden.

- ☐ In der Banking-App den Menüpunkt für Limits/Verfügungsrahmen gefunden
- ☐ Tageslimit auf einen Betrag gesenkt, der zu deinem normalen Alltag passt (z. B. 500–1.000 €)
- ☐ Notiert, dass du das Limit vor einer geplanten Großzahlung kurz hochsetzen und danach wieder senken kannst

Schritt 2 — Überweisungslimit setzen

Neben dem Tageslimit gibt es oft ein eigenes Limit pro Überweisung. Auch das gehört gedeckelt.

- ☐ Überweisungslimit (pro Auftrag) auf einen realistischen Wert gesetzt
- ☐ Bei Bedarf ein separates, niedriges Limit für Überweisungen ins Online-Banking gewählt
- ☐ Gemerkt: Kein Betrüger kann mehr abziehen, als dein Limit erlaubt

Schritt 3 — Echtzeitüberweisung entschärfen

Eine normale SEPA-Überweisung kann die Bank im Betrugsfall noch zurückzuholen versuchen (SEPA-Recall). Eine **Echtzeitüberweisung** (SEPA Instant) ist in Sekunden beim Empfänger und praktisch **nicht** rückholbar — deshalb lieben Betrüger sie.

- ☐ In den Einstellungen geprüft, ob Echtzeitüberweisung aktiv ist
- ☐ Echtzeitüberweisung deaktiviert **oder** mit einem sehr niedrigen Limit versehen
- ☐ Verstanden: Für den Alltag reicht die normale Überweisung völlig aus

Schritt 4 — Sperr-Notruf 116 116 speichern

Die **116 116** ist die zentrale Nummer, um im Ernstfall Karten und Online-Banking-Zugang sofort sperren zu lassen. Jede Sekunde zählt — die Nummer muss griffbereit sein.

- ☐ 116 116 im Handy als Kontakt „Sperr-Notruf“ gespeichert
- ☐ Nummer zusätzlich auf einen Zettel geschrieben und an den Kühlschrank/ans Telefon geklebt
- ☐ Aus dem Ausland gemerkt: +49 116 116 (Vorwahl davor)

Schritt 5 — Push-TAN-Regeln verinnerlichen

Jede TAN, die du freigibst, ist eine echte, unwiderrufliche Zahlung. Betrüger versuchen mit allen Tricks, dass du eine TAN „nur zur Bestätigung“ freigibst.

- ☐ Verinnerlicht: **Eine TAN gebe ich NIE weiter, lese sie NIE vor und tippe sie nur für meine eigene, selbst gestartete Zahlung ein**
- ☐ In der App geprüft, dass jede TAN-Freigabe den echten Empfänger und Betrag anzeigt — immer beides kontrollieren
- ☐ Gemerkt: Weder Bank noch Polizei noch „Support“ fragen jemals nach einer TAN

Schritt 6 — Zwei-Faktor-Authentifizierung (2FA) aktivieren

2FA bedeutet: Selbst wenn jemand dein Passwort kennt, kommt er ohne den zweiten Faktor (z. B. Code aufs Handy) nicht rein. Aktivier es überall, wo es wichtig wird.

- ☐ 2FA fürs Online-Banking aktiv
- ☐ 2FA fürs E-Mail-Konto aktiv (siehe auch Schritt 8)
- ☐ 2-Schritt-Verifizierung bei WhatsApp aktiviert (schützt vor Konto-Klau per Verifizierungscode)
- ☐ 2FA bei weiteren wichtigen Konten (Online-Shops, Cloud) eingerichtet

Schritt 7 — Passwort-Manager einrichten

Ein Passwort-Manager merkt sich für jedes Konto ein eigenes, starkes Passwort — du musst dir nur noch ein einziges Master-Passwort merken. Das ist sicherer als jeder Zettel und jedes mehrfach benutzte „Sommer2024“.

- ☐ Einen Passwort-Manager ausgewählt und installiert
- ☐ Ein starkes Master-Passwort als Passphrase gewählt (mehrere Wörter, z. B. „Ahorn-Wolke-Fahrrad-7“)
- ☐ Für Banking und E-Mail je ein eigenes, langes Passwort erzeugt und gespeichert
- ☐ Gemerkt: Nie dasselbe Passwort für zwei wichtige Konten

Schritt 8 — E-Mail-Konto absichern (der Generalschlüssel)

Wer dein E-Mail-Postfach kapert, kann bei fast allen anderen Diensten das Passwort zurücksetzen — die E-Mail ist der Generalschlüssel zu deinem digitalen Leben.

- ☐ Ein starkes, einzigartiges Passwort fürs E-Mail-Konto (aus dem Passwort-Manager)
 - ☐ 2FA fürs E-Mail-Konto aktiv
 - ☐ Wiederherstellungs-Optionen geprüft (aktuelle Handynummer/Zweit-Adresse hinterlegt)
 - ☐ Alte, unbenutzte Weiterleitungen und fremde Zugriffe kontrolliert und entfernt
-

Deine Festung auf einen Blick

- Limits gedeckelt → **ein Betrug kann nur begrenzten Schaden anrichten.**
 - Echtzeitüberweisung entschärft → **im Ernstfall bleibt Zeit für den Rückruf.**
 - 116 116 griffbereit → **Sperren in Sekunden statt in Stunden.**
 - TAN-Reflex sitzt → **die häufigste Falle greift bei dir nicht.**
 - 2FA + Passwort-Manager + E-Mail-Schutz → **gestohlene Passwörter allein nützen nichts mehr.**
-

Dein Schritt heute: Nimm dir Schritt 1 und Schritt 4 vor — Tageslimit senken und die 116 116 speichern. Das sind zehn Minuten, und sie bringen dir sofort die zwei wichtigsten Mauern.