NOTFALL-CHECKLISTE

Internetbetrug: Was jetzt sofort zu tun ist

Stand: 7. März 2026 | Zum Abhaken, Ausdrucken und neben den Computer legen

SOFORT WICHTIG:

Karten / Banking sperren: 116 116 | Polizei: 110

Diese Reihenfolge minimiert den Schaden: erst sperren, dann Zugang sichern, dann Beweise und Anzeige.

1

1. Karten & Konto sperren

- [ ] Sperr-Notruf 116 116 anrufen
- [ ] Bank zusätzlich direkt informieren
- [ ] Bei App-Zugang: Online-Banking sperren lassen

2

2. Passwörter ändern

- [ ] Zuerst Ihr E-Mail-Konto sichern
- [ ] Dann Banking, PayPal und andere Zahlungsdienste
- [ ] Neue Passwörter nicht wiederverwenden

3

3. Verdächtiges Gerät stoppen

- [ ] Nicht weiter fürs Banking benutzen
- [ ] Bei Malware-Verdacht WLAN trennen
- [ ] Updates / Sicherheitsprüfung auf sauberem Gerät

4

4. Beweise sichern

- [ ] Screenshots von SMS, Mail, Chat und Website
- [ ] Kontoauszug oder Kartenumsatz speichern
- [ ] Datum, Uhrzeit und Kontaktversuche notieren

5

5. Anzeige erstatten

- [ ] Onlinewache oder Polizei nutzen
- [ ] Aktenzeichen sofort notieren
- [ ] Ablauf kurz und chronologisch festhalten

6

6. Geld zurück prüfen

- [ ] Chargeback, PayPal-Fall oder Käuferschutz
- [ ] Nicht autorisierte Zahlungen sofort reklamieren
- [ ] Bei Ablehnung schriftlich widersprechen

Wichtige Daten zum Eintragen

Datum / Uhrzeit des Vorfalls

Betroffene Bank / Karte / Plattform

Aktenzeichen / Bank-Fallnummer

Kontakt der Bank / Hotline

Mehr Hilfe: online-sicher.de/pages/geld-zurueckholen.html

Merksätze für den Ernstfall

- Keine Links aus Bank-SMS oder E-Mails öffnen.
- Keine TAN oder App-Freigabe unter Telefon-Druck bestätigen.
- Erst sperren, dann erklären.
- Wenn Geld schon weg ist: erst Bank, dann Anzeige, dann Rückholweg prüfen.

Download + Hintergrund:

online-sicher.de/pages/notfall-checkliste.html

Unabhängige Hilfe zur Selbsthilfe bei Internetbetrug