Sicherheits-Checkliste

Digitale Sicherheit für Erwachsene 50+ – zum Ausdrucken und Abhaken

E-Mails & Phishing

- ■ Absender genau prüfen: stimmt die Adresse hinter dem Namen wirklich?
- ■ Keine Links in E-Mails von Banken oder Behörden anklicken – Webseite immer selbst im Browser eintippen.
- ■ Bei Druck ("sofort handeln", "Konto gesperrt") misstrauisch werden.
- ■ Anhänge nur öffnen, wenn der Absender persönlich bekannt ist und der Anhang erwartet wird.
- ■ Im Zweifel: Bank oder Anbieter unter der offiziellen Telefonnummer anrufen.

Passwörter

- ■ Für jedes wichtige Konto ein eigenes Passwort verwenden.
- ■ Mindestens 12 Zeichen, mit Zahlen und Sonderzeichen – oder einen merkbaren Satz nutzen.
- ■ Passwörter niemals per E-Mail oder Telefon weitergeben.
- ■ Einen Passwort-Manager oder ein sicher verwahrtes Notizbuch zu Hause nutzen.
- ■ Zwei-Faktor-Authentifizierung (2FA) überall einschalten, wo möglich.

Online-Banking

- ■ Banking nur über die offizielle App oder die selbst eingetippte Webadresse.
- ■ Nie über Links aus E-Mails oder SMS einloggen.
- ■ Kontoauszüge regelmäßig prüfen – auch kleine Beträge.
- ■ Push-TAN / mobileTAN-Freigaben nur erteilen, wenn man die Überweisung selbst gerade ausgelöst hat.
- ■ Bei verdächtigen Vorgängen sofort die Bank anrufen und Karte sperren lassen.

Sicher online einkaufen

- ■ Vor dem Kauf den Shop kurz prüfen: Impressum, Adresse in der Schweiz/Deutschland/Österreich, Bewertungen außerhalb des Shops.
- ■ https:// und Schloss-Symbol in der Adressleiste – aber: das allein ist kein Beweis für Seriosität.
- ■ Vorsicht bei extrem niedrigen Preisen bekannter Marken.
- ■ Sicher bezahlen: Rechnung, Kreditkarte oder PayPal mit Käuferschutz – keine Vorkasse an Unbekannte.
- ■ Bestellbestätigung und Belege aufbewahren.

Gerät & Updates

- ■ Updates für Betriebssystem, Browser und Apps zeitnah installieren.
- ■ Virenschutz aktiv lassen (Windows Defender genügt für die meisten Fälle).
- ■ Bildschirmsperre mit PIN, Code oder Fingerabdruck einschalten.
- ■ Daten regelmäßig sichern (z. B. externe Festplatte oder Cloud).
- ■ Öffentliches WLAN meiden für Banking und Einkäufe – Mobilfunk ist sicherer.

Im Verdachtsfall – ruhig bleiben

- Nicht weiterklicken, Seite/App schließen.
- Betroffenes Passwort sofort von einem sauberen Gerät aus ändern.
- Bank anrufen (Notfallnummer 116 116 in DACH zum Sperren).
- Vorfall bei der Polizei melden – auch kleine Beträge zählen.
- Mit Vertrauensperson sprechen. Schweigen hilft nur den Betrügern.