Identitätsdiebstahl – Erste Hilfe in den ersten 60 Minuten

Schnelle Orientierung: Sichern, Sperren, Informieren, Dokumentieren.

Die Schritte

• Ruhe bewahren und Beweise sichern: Screenshots, E-Mails (inkl. Header), URLs, Zeitstempel, Chat-/Anrufverläufe.

• Zugänge sichern: Alle betroffenen Passwörter sofort ändern (lang + einzigartig), aktive Sitzungen beenden, Wiederherstellungs-E-Mail/Telefon prüfen.

• MFA aktivieren/wechseln: App/Hardware-Token statt SMS. Notfallcodes sicher ablegen.

• Geld schützen: Bank/Zahlungsdienste (Karte, PayPal, Kreditkarte) informieren und ggf. sperren. Transaktions-Alerts einschalten.

• Geräte prüfen: Updates einspielen, Malware-Scan durchführen, verdächtige Browser-Add-ons/Apps entfernen.

• Plattformen informieren: Missbrauch bei Mail, Cloud, Social Media, Marktplätzen melden; Kontowiederherstellung starten.

• Unerlaubte Forderungen bestreiten: Inkasso/Firmen schriftlich widersprechen, Anzeige ankündigen; niemals ungeprüft zahlen.

• Behörden kontaktieren: Anzeige bei der Polizei erstatten; Aktenzeichen dokumentieren.

• Mobilfunk absichern (SIM-Swap): Anbieter kontaktieren, Hotline-PIN setzen; MFA von SMS auf App/Hardware umstellen.

Kurzhinweise

• Nutzen Sie einen Passwortmanager und vergeben Sie pro Dienst ein einzigartiges Passwort.

• Ihre E-Mail ist der Generalschlüssel für Passwort-Resets – besonders absichern.

• Dokumentieren Sie alles (Zeit, Kanal, Inhalt). Das hilft bei Polizei, Bank und Plattformen.

• Bei KI-Deepfake-/Voice-Phishing: Rückruf über bekannte Nummern, Codewörter in der Familie/Organisation.