Whitepaper & Notfall-Checkliste

Auf Phishing-Link geklickt

MENSCH

✓ Richtig vorbeugen

- Absenderadresse immer genau prüfen, nicht nur den angezeigten Namen.
- Bei Links: Mauszeiger über den Link halten und Ziel-URL prüfen, bevor geklickt wird.
- Niemals Zugangsdaten über einen Link aus einer E-Mail eingeben.
- Bei Unsicherheit: E-Mail nicht öffnen, sondern der IT-Abteilung melden.
- Zwei-Faktor-Authentifizierung überall aktivieren, wo möglich.
- Regelmäßige Phishing-Awareness-Schulungen für alle Mitarbeitenden.

■ Im Ernstfall – Schritt für Schritt

Vorfall-Protokoll (bitte ausfüllen)

Datum:	
Uhrzeit:	
Betroffenes System / Gerät:	
Gemeldet durch:	
Gemeldet an (IT-Verantwortlicher):	

- ■ **1.** Ruhe bewahren – Panik führt zu weiteren Fehlern.
- ■ **2.** Gerät sofort vom Netzwerk trennen (WLAN/LAN-Kabel), falls Daten eingegeben wurden.
- ■ **3.** Betroffene Zugangsdaten unverzüglich ändern (von einem anderen, sauberen Gerät aus).
- ■ **4.** IT-Abteilung / IT-Dienstleister sofort informieren.
- ■ **5.** Betroffenes Konto auf ungewöhnliche Aktivitäten prüfen lassen.
- ■ **6.** Bei Zahlungsdaten: Bank/Kreditkarteninstitut informieren und Karte ggf. sperren.
- ■ **7.** Vorfall dokumentieren (Screenshot der E-Mail sichern).
- ■ **8.** Kolleg*innen warnen, falls die Mail an mehrere Personen ging.