IT / FORENSIK SCHWEIZ · ARBEITSVORLAGE

Phishing: sicher melden

Ein Meldeablauf für Mitarbeitende in Schweizer KMU · Oktober 2026

Grundsatz: Nicht weiter interagieren. Offen melden.

Ein früh gemeldeter Klick ist besser als ein verschwiegener Klick. Niemand soll aus Angst vor Schuldzuweisung eine Passwort-Eingabe oder einen geöffneten Anhang verbergen.

Wenn eine Nachricht verdächtig wirkt

- [ ] Keinen Link, QR-Code oder Button weiter anklicken und keinen Anhang öffnen.
- [ ] Keine Zugangsdaten, Mehrfaktor-Codes oder Zahlungsdaten eingeben.
- [ ] Absender, Betreff und Zeitpunkt über den internen Meldeweg an IT oder Security weitergeben.
- [ ] Nachricht nicht an externe Kontakte weiterleiten und nicht eigenständig löschen, wenn der interne Ablauf etwas anderes vorsieht.

Wenn ein Link angeklickt wurde

- [ ] Browserfenster schliessen und keine weiteren Angaben auf der geöffneten Seite machen.
- [ ] IT oder Security unverzüglich informieren; Zeitpunkt, Link und sichtbare Reaktion beschreiben.
- [ ] Gerät nicht vorschnell zurücksetzen oder bereinigen; nächste Schritte abstimmen.
- [ ] Keine weiteren Links aus derselben Nachricht ausprobieren.

Wenn Zugangsdaten eingegeben oder ein Anhang ausgeführt wurde

- [ ] Vorgang sofort über Telefon oder den vorgesehenen dringlichen Kanal melden.
- [ ] Genau sagen, welche E-Mail-Adresse, welche Seite und welche Handlung betroffen sind.
- [ ] Mit der IT einen koordinierten Schutz des Kontos, laufender Sitzungen und möglicher Weiterleitungen planen.
- [ ] Ausgeführten Anhang als möglichen Untersuchungsfall behandeln und nicht eigenmächtig verändern.

Was Führungskräfte vorbereiten

- [ ] Sichtbaren, einfachen und sanktionsfreien Meldeweg kommunizieren.
- [ ] Erreichbare Stelle für dringliche Fälle benennen und Ablauf regelmässig üben.
- [ ] Meldungen dokumentieren und bei Bedarf technisch einordnen lassen.
- [ ] Mehrfaktorauthentisierung und Wiederherstellung von Konten geplant abstimmen.

Nicht tun

Nicht aus Scham schweigen, nicht auf eigene Faust Passwörter überall ändern und nicht Beweismittel löschen. Die zuständige IT kann nur mit einer offenen Meldung sinnvoll unterstützen.

Fallnotizen

Zeitpunkt: ..... Absender/Betreff: ..... Bereits passiert: .....

Nächster Schritt

Akut-Check für einen konkreten Vorfall anfragen: it-forensik.ch/akut-check-it-vorfall/ · +41 41 562 70 30

Diese Vorlage unterstützt die interne Meldung und ersetzt keine technische, rechtliche oder versicherungsbezogene Einzelfallberatung. Grundlage: BACS, Gefälschte Sprachnachrichten zielen auf Zugangsdaten (Woche 25/2026).

Copyright by Dr. René Bäder (PhDs) · V1.2