

PHISHING ERKENNEN

6 Warnsignale, an denen Sie eine gefährliche E-Mail erkennen — und was Sie im Zweifel tun.



1 · Absender genau prüfen

Der angezeigte Name kann echt wirken — die Adresse dahinter nicht. Domain Zeichen für Zeichen lesen: **paypa1.de** ≠ **paypal.de**.



2 · Druck & Dringlichkeit = Warnsignal

„Konto gesperrt“, „letzte Mahnung“, „sofort handeln“ sollen Sie zum **unüberlegten Klick** treiben. Echte Stellen setzen Sie nicht unter Zeitdruck.



3 · Links prüfen, bevor Sie klicken

Mauszeiger über den Link halten — **nicht klicken!** — und die Ziel-Adresse unten links lesen. Passt sie nicht zum Absender: weg damit.



4 · Unerwartete Anhänge & Bitten

Rechnung, die Sie nicht erwarten? Chef bittet plötzlich um Überweisung oder Gutschein-Codes? **Über einen zweiten Kanal rückfragen** (anrufen), nie direkt antworten.



5 · „Schlechtes Deutsch“ reicht nicht mehr

KI schreibt heute fehlerfreie, persönlich klingende Phishing-Mails. **Perfekte Sprache ist kein Echtheitsbeweis** — prüfen Sie Absender, Link und Plausibilität, nicht die Rechtschreibung.



6 · Im Zweifel: nicht klicken, melden

Lieber einmal zu oft fragen als einmal zu wenig. Verdächtige Mail **nicht löschen** — an den Meldeweg unten weiterleiten. Wer meldet, macht alles richtig.



VERDACHT? SOFORT MELDEN AN:

IT-Ansprechpartner / Meldeweg hier eintragen — z. B. it@ihre-firma.de · Tel. _____