Phishing und Social Engineering

4.1 Was ist Phishing?

Phishing versucht, Menschen mit gefälschten Nachrichten oder Webseiten zu täuschen. Ziel können Passwörter, Zahlungsdaten, vertrauliche Informationen oder das Öffnen schädlicher Dateien sein.

Vergleich aus dem Alltag

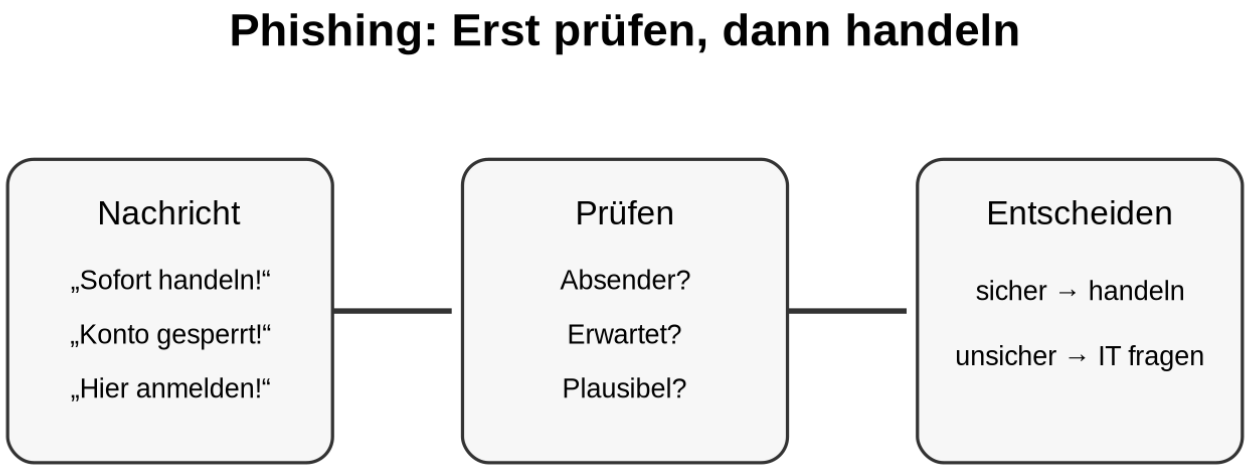
Phishing ist Trickbetrug in digitaler Form.

Beispiel aus dem Arbeitsalltag

Eine Nachricht behauptet, dein Postfach müsse sofort neu bestätigt werden und führt auf eine gefälschte Anmeldeseite.

Was soll ich tun?

Phishing greift zuerst deine Entscheidung an – nicht unbedingt deinen Computer.



> **Merke:** Nicht über den enthaltenen Link anmelden. Im Zweifel den bekannten normalen Weg zum Dienst verwenden.

4.2 Typische Warnzeichen

Ein einzelnes Merkmal beweist noch keinen Angriff. Mehrere Auffälligkeiten zusammen sollten dich aber besonders vorsichtig machen.

Vergleich aus dem Alltag

Bei einem gefälschten Ausweis kann ein Detail unauffällig sein. Mehrere falsche Details ergeben ein deutliches Bild.

Beispiel aus dem Arbeitsalltag

Ungewöhnlicher Absender, unerwartete Rechnung, großer Zeitdruck und Aufforderung zur sofortigen Anmeldung treten gemeinsam auf.

Was soll ich tun?

Überraschung + Zeitdruck + ungewöhnliche Handlung = besonders genau prüfen.

Warnzeichen

- ungewöhnlicher oder leicht veränderter Absender
- unerwarteter Anhang
- angebliche Kontosperre
- ungewöhnliche Zahlungsanweisung
- Aufforderung zur Preisgabe von Zugangsdaten
- starker Zeitdruck

> **Merke:** Absender, Anlass, Sprache, Linkziel und erwarteten Geschäftsprozess prüfen.

4.3 Gefälschte Absender

Ein sichtbarer Anzeigename ist kein sicherer Beweis für die Identität eines Absenders. Angreifer verwenden ähnlich aussehende Adressen oder Namen bekannter Personen und Firmen.

Vergleich aus dem Alltag

Auf einem Briefumschlag kann jemand ebenfalls einen bekannten Namen als Absender aufschreiben.

Beispiel aus dem Arbeitsalltag

Die Nachricht zeigt den Namen eines Kollegen, die tatsächliche Absenderadresse gehört aber zu einer fremden Domain.

Was soll ich tun?

Der angezeigte Name allein beweist nicht, wer eine Nachricht wirklich gesendet hat.

> **Merke:** Bei ungewöhnlichen Anweisungen die vollständige Absenderadresse prüfen und über einen bekannten zweiten Weg rückfragen.

4.4 Zeitdruck und Autorität

Social Engineering nutzt menschliche Reaktionen. Besonders wirksam sind angebliche Dringlichkeit, Angst, Hilfsbereitschaft oder eine vermeintliche Anweisung einer Führungskraft.

Vergleich aus dem Alltag

Ein Betrüger will verhindern, dass du Zeit zum Nachdenken oder Nachfragen hast.

Beispiel aus dem Arbeitsalltag

Eine angebliche Führungskraft verlangt eine ungewöhnliche Zahlung und schreibt, sie sei gerade nicht telefonisch erreichbar.

Was soll ich tun?

Dringlichkeit ist kein Grund, Sicherheitsregeln zu überspringen.

> **Merke:** Ungewöhnliche oder finanzielle Anweisungen über einen bekannten unabhängigen Kontaktweg bestätigen lassen.

4.5 QR-Code-Phishing

Auch QR-Codes können auf gefälschte Webseiten führen. Da das Ziel vor dem Scannen nicht immer sofort sichtbar ist, werden QR-Codes zunehmend für Phishing genutzt.

Vergleich aus dem Alltag

Ein QR-Code ist nur ein anderer Weg, eine Adresse zu verpacken. Er macht die Adresse nicht automatisch sicher.

Beispiel aus dem Arbeitsalltag

Eine E-Mail fordert dazu auf, einen QR-Code mit dem Smartphone zu scannen und das Firmenkonto anzumelden.

Was soll ich tun?

Ein QR-Code ist kein Vertrauenssiegel.

> **Merke:** Bei unerwarteten QR-Anmeldungen besonders vorsichtig sein und bekannte Zugangswege verwenden.