Merkblatt Phishing

Definition: Was ist Phishing?

> Phishing ist Betrug per E-Mail. Kriminelle senden täuschend echte E-Mails, um an Ihre **persönlichen Daten** zu kommen oder Sie zu einer **überstürzten Aktion** zu verleiten. Zum Beispiel gibt sich der Betrüger als Ihre Bank oder als ein Kollege aus. Ziel ist es, dass Sie auf einen Link klicken, einen Anhang öffnen oder geheime Informationen verraten. Im Grunde ist es so, als würde jemand versuchen, Sie mit einer Lügengeschichte hereinzulegen – nur eben per E-Mail.

Woran erkenne ich eine Phishing-Mail?

Es gibt **Anzeichen**, die oft auf eine Phishing-Mail hindeuten:

- **Unpersönliche Begrüßung** (*„Sehr geehrter Kunde“ statt Ihrem Namen*).
- **Unerwartete Absender** oder **seltsame E-Mail-Adressen** (passt nicht zur angeblichen Firma).
- Viele **Rechtschreibfehler** oder **ungewöhnliche Sprache** (manchmal sogar in Englisch, ohne Grund).
- **Inhalt wirkt *dringend*** oder macht Angst (Drohungen wie *„Konto wird gesperrt“*).
- **Aufforderung, persönliche Daten einzugeben** (Passwort, Kontodaten – nicht machen!).
- Aufforderung, auf einen **Link** zu klicken oder einen **Anhang** zu öffnen.
- **Angebot klingt zu schön**, um wahr zu sein (Gewinne, Geschenke von Unbekannten).

> **MERKE:**
> „Wenn's unpersönlich klingt, zu schnell drängt, Fehler hat und was verspricht – klick besser nicht!“

Wie sollte ich auf verdächtige E-Mails reagieren?

Nichts anklicken, nichts öffnen! Klicken Sie nicht auf Links und öffnen Sie keine Anhänge, wenn Ihnen etwas verdächtig vorkommt.

Nicht antworten! Antworten Sie nicht auf eine verdächtige Mail. Geben Sie keine Daten preis.

Im Zweifel Hilfe holen: Fragen Sie eine Kollegin, Ihren Vorgesetzten oder die IT-Abteilung um Rat. Lieber einmal mehr nachfragen.

Melden: Informieren Sie zuständige Stellen. Im Unternehmen z. B. die IT-Abteilung oder einen Sicherheitsbeauftragten. Privat können Sie betrügerische Mails der Verbraucherzentrale oder dem BSI melden.

Löschen: Ist klar, dass die Mail ein Betrugsversuch ist, löschen Sie sie oder verschieben Sie sie in den Spam-Ordner. Blockieren Sie den Absender, falls möglich.

Gut zu wissen:

Keine seriöse Bank oder Institution fordert per E-Mail dazu auf, Passwörter, PINs oder TANs einzugeben. Seien Sie daher grundsätzlich misstrauisch bei Nachrichten, die solche Daten verlangen.

Zudem gilt: E-Mails, die Druck aufbauen oder Sie zu schnellem Handeln drängen, sind fast immer verdächtig. Bleiben Sie ruhig – und denken Sie erst nach, bevor Sie reagieren.

Die folgenden Beispiele zeigen typische Phishing-Versuche, auf die Sie achten sollten:

Beispiel 1: Fake-IT-Abteilung bittet um Passwort

Betreff: *Dringend! Ihr Konto wird deaktiviert*
Absender: *it-support@firmen-it.com*

Sehr geehrter Benutzer,

Aufgrund ungewöhnlicher Aktivitäten wird Ihr Konto in 24 Stunden deaktiviert. Bitte verifizieren Sie Ihre Identität, indem Sie sich unter folgendem Link anmelden und Ihr Passwort eingeben:
f1rm3n-login.com/security-check

Mit freundlichen Grüßen
IT-Support Team

🛑 **Verdächtig, weil:**

- Dringlichkeitsdruck ("in 24 Stunden deaktiviert")
- Falsche Domain (nicht „@deinefirma.de“)
- Passwortabfrage per E-Mail = **immer ein No-Go**

Beispiel 2: Paketbenachrichtigung von einem Fake-Versanddienst

Betreff: *Ihr DHL-Paket konnte nicht zugestellt werden*
Absender: *info@dhl-zustellung.net*

Guten Tag,

Ihr Paket konnte heute leider nicht zugestellt werden. Um eine neue Zustellung zu veranlassen, klicken Sie bitte auf den folgenden Link:
dhl-service-check.net/lieferung

🛑 **Verdächtig, weil:**

- Ungewöhnliche Domain („dhl-zustellung.net“ statt „dhl.de“)
- Kein Paket erwartet? Misstrauisch sein!
- Link führt zu Phishing-Seite