PRAXISLEITFADEN · INFORMATIONSSICHERHEIT

Phishing-E-Mails erkennen

Checkliste zur Überprüfung von Absendern, Inhalten und Links

TRISEC
YOUR WAY INTO SECURITY
Informationssicherheit seit 2001

Phishing-Angriffe sind heute kaum noch von echten E-Mails zu unterscheiden. Diese Checkliste unterstützt Sie dabei, verdächtige Nachrichten systematisch zu prüfen — bevor Sie auf einen Link klicken oder einen Anhang öffnen. Die Punkte sind nach Risikograd priorisiert.

1 Absenderadresse prüfen

Erste Prüfebene

- [ ] 🔴 **Domain genau lesen —** nicht nur den Anzeigenamen. Phishing-Mails nutzen oft Domains wie *paypa1.com* oder *amazon-support.net* statt der echten Domain.
  Tipp: Im Mail-Client auf den Absender klicken, um die vollständige Adresse anzuzeigen.
- [ ] 🔴 **Stimmt die Domain zur Organisation?** Behörden schreiben von *.de*- oder *.bund.de*-Adressen, keine seriöse Bank schreibt von einer Gmail-Adresse.
- [ ] 🟠 **E-Mail-Header auf Umwege prüfen —** fortgeschrittene Prüfung. Tools wie MXToolbox Header Analyzer zeigen, über welche Server die Mail tatsächlich geleitet wurde.
  mxtoolbox.com/EmailHeaders.aspx
- [ ] 🟠 **SPF / DKIM / DMARC —** viele Mail-Clients zeigen an, ob die Signatur gültig ist. Fehlt diese Angabe oder ist sie ungültig, ist Vorsicht geboten.

2 Inhalt und Sprache bewerten

Zweite Prüfebene

- [ ] 🔴 **Dringlichkeit oder Drohung?** „Ihr Konto wird in 24 Stunden gesperrt" ist ein klassisches Muster. Seriöse Unternehmen setzen keine Ultimaten per E-Mail.
- [ ] 🔴 **Wird nach Zugangsdaten, Passwörtern oder Zahlungsinformationen gefragt?** Kein legitimes Unternehmen fordert diese Daten per E-Mail an.
- [ ] 🟠 **Persönliche Anrede prüfen —** allgemeine Anreden wie „Sehr geehrter Kunde" oder „Dear User" deuten auf Massenversand hin, können aber auch legitim sein.
- [ ] 🟠 **Grammatik und Formulierung —** ungewöhnliche Satzstellung, fehlerhafte Umlaute oder maschinell wirkende Formulierungen sind ein Warnsignal.
- [ ] 🟢 **Haben Sie diese E-Mail erwartet?** Rechnungen, Pakete oder Kontobenachrichtigungen, die Sie nicht erwarten, sollten grundsätzlich skeptisch geprüft werden.

3 Links vor dem Klicken prüfen

Dritte Prüfebene

- [ ] 🔴 **Maus über den Link bewegen (nicht klicken) —** die tatsächliche Ziel-URL erscheint in der Statusleiste. Stimmt sie mit dem angezeigten Text überein?
- [ ] 🔴 **Verkürzte URLs (bit.ly, t.co etc.) aufdecken —** nutzen Sie einen URL-Expander (z.B. unshorten.it), um das Ziel zu sehen, bevor Sie klicken.
- [ ] 🔴 **Verdächtige URL auf Reputation prüfen —** Tools wie urlscan.io oder Google Safe Browsing analysieren die Zielseite auf Schadsoftware und Phishing.
  urlscan.io · transparencyreport.google.com/safe-browsing/search
- [ ] 🟠 **Im Zweifel: URL manuell eintippen —** gehen Sie direkt auf die offizielle Website des Anbieters, statt dem Link in der E-Mail zu folgen.

4 Anhänge beurteilen

Vierte Prüfebene

- [ ] 🔴 **Ausführbare Dateien niemals öffnen —** Endungen wie .exe, .js, .vbs, .scr oder .bat in einer E-Mail sind ein klares Warnsignal.
- [ ] 🔴 **Office-Dokumente mit Makros —** wenn ein Word- oder Excel-Dokument auffordert, Makros zu aktivieren, sollten Sie dies verweigern und die Datei löschen.
- [ ] 🟠 **Anhang auf VirusTotal prüfen —** laden Sie unsichere Dateien zunächst bei virustotal.com hoch, bevor Sie sie öffnen.
  Achtung: Keine vertraulichen Dokumente hochladen.

RISIKOGRAD 🔴 Hohes Risiko — immer prüfen 🟠 Mittleres Risiko — im Zweifel prüfen 🟢 Hinweis — situationsabhängig