BEDROHUNGS-BIBLIOTHEK

JULITH GmbH
Awareness-as-a-Service

Phishing erkennen & abwehren — der vollständige Leitfaden

94% aller erfolgreichen Cyber-Angriffe beginnen mit einer Phishing-E-Mail. Hier erfahren Sie, wie Sie sie in drei Sekunden enttarnen — und was zu tun ist, wenn jemand bereits geklickt hat.

min Lesezeit: 9 min **Aktualisiert:** 14. März 2026 **Risiko:** Sehr hohes Risiko
Quelle: awareness-as-a-service.com/de/resources/threats/phishing

Was ist Phishing?

Phishing ist der Versuch, Sie zur Preisgabe von Zugangsdaten, Zahlungsinformationen oder zur Ausführung schädlicher Aktionen zu bewegen — meist per E-Mail, zunehmend auch per SMS (`Smishing`), QR-Code (`Quishing`) oder Anruf (`Vishing`).

Anders als technische Angriffe richtet sich Phishing direkt an Menschen. Es nutzt psychologische Hebel: Zeitdruck, Autorität, Neugier, Angst. Genau deshalb scheitern technische Schutzmaßnahmen regelmäßig — und Awareness ist die wirksamste Verteidigungslinie.

Auf einen Blick

01
Häufigste Angriffsart
94% der Vorfälle starten mit Phishing — vor allem Business-E-Mail-Compromise (BEC).

02
11 Minuten bis zum Klick
Durchschnittliche Zeit zwischen Empfang und Klick. Reagieren muss daher das System, nicht nur der SOC.

03
3 Sekunden zur Erkennung
Sender, Anrede, Link-Vorschau — ein 3-Sekunden-Check reicht in 80% der Fälle.

Woran erkennen Sie Phishing?

Sechs Warnsignale, die zusammen oder einzeln auf Phishing hindeuten:

! Künstlicher Zeitdruck
"Innerhalb von 24 Stunden", "letzte Mahnung", "Konto wird gesperrt".

! Aufforderung zum Rückruf
"Bitte rufen Sie sofort die Nummer +49… zurück" — Vishing-Verkettung.

! Verdächtige Domain
`microsoft-365.support` statt `microsoft.com`, Tippfehler, Unicode-Tricks.

! Unpersönliche Anrede
"Sehr geehrter Kunde", obwohl der Absender Sie eigentlich kennt.

! Verdächtige Links
Hover-Vorschau passt nicht zum Klartext-Link, oder Link via URL-Shortener.

! Ungefragte Anhänge
Office-Dokumente mit Makros, ZIP-Archive, HTML-Dateien — besonders kritisch.

So schützen Sie sich

Für Mitarbeitende

- 3-Sekunden-Check vor jedem Klick: Absender, Domain, Link-Vorschau.
- Bei Zweifel: **Sender über bekannten Kanal verifizieren** (Telefon, Chat) — nicht über die E-Mail antworten.
- Verdächtige E-Mails über den "Phishing melden"-Button weiterleiten, nicht löschen.
- Niemals Zugangsdaten oder MFA-Codes auf via E-Mail verlinkten Seiten eingeben.

Für Administratoren

- SPF, DKIM, DMARC (Policy `p=reject`) für alle ausgehenden Domains konfigurieren.
- External-E-Mail-Banner in Outlook / Gmail Workspace aktivieren.
- "Phishing melden"-Button (z.B. via Add-in) ausrollen — direkter Kanal an SOC.
- MFA erzwingen — Phishing-resistente Methoden (FIDO2, Passkeys) bevorzugen.
- Quartalsweise Phishing-Simulationen mit Lernmoment bei Klick.

Echte Beispiele

FALL 01 · MITTELSTÄNDISCHER MASCHINENBAUER · DE · Q2/2025

Eine vermeintliche Microsoft-365-E-Mail forderte zur "Verifizierung des Postfachs" auf. Ein Buchhalter klickte den Link, gab Zugangsdaten und MFA-Code ein. **Innerhalb von 90 Minuten** versandten Angreifer eine gefälschte Rechnung an einen Lieferanten — über das echte Postfach.

Schaden: EUR 38.000 · **Erkennung:** 4 Tage später durch Bank-Rückfrage · **Lehre:** Phishing-resistente MFA hätte den Angriff verhindert.

FALL 02 · KOMMUNALVERWALTUNG · CH · Q4/2025

QR-Code in einem ausgedruckten "Sicherheits-Brief" am Empfang. Mitarbeitende scannten ihn und landeten auf einer gefälschten Single-Sign-On-Seite. Der Angreifer hatte zuvor öffentliche Pressemitteilungen genutzt, um Mitarbeiternamen zu sammeln.

Schaden: kein Datenabfluss · **Erkennung:** aufmerksamer IT-Leiter · **Lehre:** Quishing-Awareness in Standard-Module aufnehmen.

Was tun, wenn es passiert ist?

DIE ERSTEN 15 MINUTEN

1. **Ruhig bleiben, nicht löschen.** Die E-Mail ist Beweismittel.
2. **Sofort melden:** IT-Helpdesk / SOC / ISB. Keine "ich-warte-mal-ab"-Reflexe.
3. **Geräte vom Netz trennen,** wenn ein Anhang ausgeführt oder Zugangsdaten eingegeben wurden.
4. **Passwort sofort ändern** (von einem anderen Gerät aus). Falls SSO: Sessions invalidieren.
5. **MFA-Geräte überprüfen:** wurden zusätzliche Geräte ohne Ihre Zustimmung registriert?
6. **Banken / Buchhaltung informieren,** wenn Zahlungsdaten möglicherweise abgeflossen sind.

Häufige Fragen

Wie unterscheide ich Phishing von Spear-Phishing?

Phishing wird in Masse versendet. Spear-Phishing richtet sich gezielt an einzelne Personen mit recherchierten Details (Position, Projekte, persönliche Kontakte). Whaling ist Spear-Phishing gegen Geschäftsleitung. Die Schutzmaßnahmen sind ähnlich — die Erkennungs-Schwelle bei Spear-Phishing aber höher.

Kann mein Spam-Filter Phishing erkennen?

Teilweise. Massen-Phishing wird oft gefiltert. BEC und Spear-Phishing sind technisch unauffällig — sie kommen über echte (kompromittierte) Konten, ohne Anhänge, ohne verdächtige Links. Genau deshalb sind Awareness und prozessuale Kontrollen unverzichtbar.

Sind Phishing-Simulationen rechtlich problematisch?

In der Schweiz und Deutschland zulässig, wenn die Personalvertretung / der Betriebsrat informiert ist und die Maßnahme nicht zur individuellen Leistungskontrolle dient. Wir liefern Mustervereinbarungen für CH (OR), DE (BetrVG) und AT.

Was kostet ein erfolgreicher Phishing-Angriff im Schnitt?

EUR 4,5 Mio. in der DACH-Region (IBM 2025). Direkte Schäden (Überweisungen, Ransom) machen etwa ein Drittel aus — der Rest sind Forensik, Ausfallzeit, Reputationsschaden und Regulierungs-Folgen.

Weitere Themen

Diese Bedrohungen ergänzen sich häufig — wer Phishing versteht, sollte auch CEO-Fraud, Quishing und KI-basierte Manipulation kennen.