



Checkliste: Phishing-Mails erkennen

Was ist Phishing?

Der Begriff Phishing setzt sich aus den englischen Wörtern „Password“ und „Fishing“ zusammen. Dabei versuchen Angreifer, über täuschend echte Nachrichten an vertrauliche Informationen zu gelangen oder Schadsoftware einzuschleusen – zum Beispiel über gefälschte E Mails, Webseiten, SMS oder QR Codes.

Ziel sind u. a. Passwörter, Zahlungsdaten, Unternehmenszugänge oder interne Informationen.

Phishing ist eine der häufigsten Formen von Cyberkriminalität und Angriffe sind heute – auch aufgrund des Einsatzes von Künstlicher Intelligenz – oft fehlerfrei formuliert, personalisiert und kaum von echten Nachrichten zu unterscheiden.

Welche Risiken entstehen?

Für Privatpersonen

- Identitätsdiebstahl (z. B. Übernahme von E-Mail- oder Social-Media-Accounts)
- Finanzielle Schäden durch missbräuchliche Zahlungen
- Verlust persönlicher Daten

Für Selbstständige & Unternehmen

- Abfluss sensibler Daten und Know-how
- Manipulierte Rechnungen und Fehlüberweisungen (z. B. CEO-Fraud)
- Betriebsunterbrechungen durch Schadsoftware oder Ransomware
- Reputationsschäden und mögliche DSGVO-Folgen

Häufige Formen von Phishing

- E-Mail-Phishing: Gefälschte Nachrichten mit Links oder Anhängen
- SMS/Messenger-Phishing (Smishing): Kurznachrichten mit Handlungsdruck
- QR-Code-Phishing: Schadlinks hinter QR-Codes (z. B. auf Rechnungen)
- Telefonbetrug (Vishing): Anrufe z. B. mit angeblichem Support- oder Behördenbezug
- Business Email Compromise (BEC): Täuschung im Namen von Geschäftsführung, Kunden oder Lieferanten

Schritt für Schritt: Phishing-Mails erkennen & abwehren

☐ Technische Schutzmaßnahmen nutzen

- ☐ Multi-Faktor-Authentifizierung (MFA)
- ☐ Aktueller Viren- bzw. Endpoint-Schutz
- ☐ E-Mail-Filter, Safe-Links und Sandboxing
- ☐ Regelmäßige Updates von Betriebssystemen und Programmen

☐ Absender kritisch prüfen

- ☐ Passt die E-Mail-Adresse wirklich zum Absender?
- ☐ Gibt es kleine Abweichungen oder ungewöhnliche Domains?
- ☐ Kommt die Nachricht unerwartet?

	Anzeigename	E-Mail-Adresse	Absenderadresse (Domäne)
Von:	Kontosensor Bank	<kontosensor@bank.com>	
Von:	Kontosensor Bank		Nur Anzeigename
Von:	kontosensor@bank.com		Nur Absenderadresse oder Anzeigename
Von:	Kontosensor Bank	<info@hotel123.ru>	

☐ Links und Anhänge prüfen

- ☐ Link bzw. Zieladresse vor dem Klicken prüfen
- ☐ Keine Anhänge öffnen, wenn Herkunft unklar ist
- ☐ QR-Codes nur scannen, wenn Quelle vertrauenswürdig ist

Diagramm zur Link-Prüfung:

1 Start → 2 Erster / → 3 Punkt nach .com → Zieladresse (Domain)

Beispiel: <http://irgend.etwas.paypal.com/> Der Link geht weiter zu <http://paypal.com>

☐ Inhalt & Tonfall hinterfragen

- ☐ Wird Druck aufgebaut oder Angst erzeugt?
- ☐ Wird zu ungewöhnlichem Verhalten aufgefordert?
- ☐ Passt die Anfrage zum bisherigen Kommunikationsverlauf?

☐ Kommunikationspartner verifizieren

- ☐ Über bekannte Kontaktwege (z. B. E-Mail oder Anruf) rückfragen
- ☐ Anruf bei Zentrale und durchstellen lassen
- ☐ Interne Rücksprache halten
- ☐ Internetrecherche

Gut zu wissen: Unterstützung im Ernstfall

Als Hiscox Cyber-Kunde profitieren Sie im Schadenfall u. a. von:

- Absicherung bei Hacker-Angriffen wie z. B. Phishing sowie daraus resultierendem Datenverlust und -missbrauch
- Soforthilfe im Krisenfall (auch im Verdachtsfall)
- Umfangreiche Präventionsleistungen wie Cyber-Training und Phishing-Simulationen

Jetzt mehr erfahren

Hiscox

Bernhard-Wicki-Straße 3, 80636 München

T +49 89 54 58 01 700 E hiscox.marketing@hiscox.de

W hiscox.de