Amfortas

Phishing-Checkliste für Unternehmen

Dieses Dokument zeigt Ihnen, wie Sie betrügerische Phishing-E-Mails erkennen und sich vor digitalen Bedrohungen schützen können. Folgen Sie den Prüfschritten, um verdächtige Merkmale zu identifizieren und angemessen zu reagieren.

Klicken Sie nicht auf Links und öffnen Sie keine Dateien im Anhang, ohne vorher die fünf Prüfschritte durchzugehen! Nach einiger Übung haben Sie die Schritte verinnerlicht.

Wenn Sie glauben, dass Sie eine Phishing-E-Mail gefunden haben, zeigen Sie es der zuständigen Person im Unternehmen. Leiten Sie die E-Mail nicht unaufgefordert weiter!

Achtung: Angriffe sind vielfältig

Diese Checkliste bietet einen ersten Schutz gegen die gängigsten Phishing-Maßnahmen. Betrüger nutzen aber eine Vielzahl an Methoden, um an Ihre sensiblen Daten zu gelangen. **Um Social-Engineering-Angriffe sicher erkennen zu können sein, ist professionelles Training erforderlich.** Unsere Workshops und Simulationen vermitteln Ihnen die notwendigen Kompetenzen, um Phishing-Versuche zuverlässig zu erkennen und Ihre Firma effektiv vor Angriffen zu schützen.

Mehr Informationen zu unseren Trainings, weitere Ressourcen und aktuelle Informationen, um Ihr Unternehmen umfassend zu schützen, finden Sie auf unserer Webseite:

www.amfortas.at

Schritt 1: Den Absender kritisch prüfen

Überprüfen Sie den Absender genau. Betrüger verwenden oft E-Mail-Adressen, die auf den ersten Blick legitim erscheinen, aber kleine Unterschiede zur originalen Adresse aufweisen.

Achten Sie auf Veränderungen in der Domain, fehlende oder vertauschte Buchstaben, oder fremdartige Domains. Bewegen Sie den Mauszeiger über den Absendernamen, um die vollständige Adresse zu sehen.

Beispiel verdächtiger E-Mail-Adressen:

- service@amaz0n.com (statt amazon.com)
- support@bank-secure-login.com (statt Domain der Bank)
- kontakt@post-lieferung.at (statt post.at)
- paypal-sicherheit@gmail.com (fremde Domain mit bekanntem Markennamen)

Schritt 2: Betreff und Tonfall als Warnsignale

Der Betreff einer E-Mail und der allgemeine Tonfall des Textes liefern wichtige Hinweise auf mögliche Phishing-Versuche. Betrüger setzen gezielt auf emotionale Reaktionen wie Angst, Dringlichkeit oder Neugier, um die kritische Beurteilung zu unterdrücken und zu übereilten Handlungen zu verleiten.

Dringlichkeit und Drohungen

Betreffs wie "SOFORT ZAHLEN!", "LETZTE WARNUNG" oder "Ihr Konto wird in 24 Stunden gesperrt!" sind typische Anzeichen für Phishing. Seriöse Unternehmen vermeiden unnötigen Druck und übertriebene Dringlichkeit in ihrer Kommunikation.

Unpersönliche Anrede

Wenn Sie mit "Sehr geehrte/r Kunde/in" oder "Lieber Nutzer" angesprochen werden, obwohl das Unternehmen Ihren Namen kennen sollte, ist Vorsicht geboten. Legitime Emails verwenden in der Regel Ihren tatsächlichen Namen.

Ungewöhnlicher Sprachstil

Achten Sie auf einen auffällig formellen oder ungewöhnlich lockeren Ton, der nicht zum üblichen Kommunikationsstil des vermeintlichen Absenders passt. Wenn die E-Mail unprofessionell wirkt, ist besondere Vorsicht geboten.

> Beispiel einer verdächtigen E-Mail: "WICHTIG: Ihre Paket-Lieferung wurde gestoppt! Sie müssen JETZT handeln und auf den Link klicken, sonst wird Ihr wertvolles Paket zurückgeschickt!!!"

Schritt 3: Links und Anhänge kontrollieren

Links und Anhänge sind die primären Werkzeuge für Cyberkriminelle, um Schadsoftware zu verbreiten oder Sie auf gefälschte Webseiten zu locken. Eine gründliche Prüfung dieser Elemente ist daher besonders wichtig.

Verdächtige Links erkennen:

Links in Phishing-E-Mails führen oft zu täuschend ähnlichen Webseiten, die legitime Dienste imitieren. Die Betrüger setzen dabei auf kleine, leicht zu übersehende Veränderungen in der URL. Um die tatsächliche Zieladresse eines Links zu prüfen, fahren Sie mit der Maus darüber (ohne zu klicken!) - die eigentliche URL wird dann meist in der Statusleiste Ihres E-Mail-Programms oder als Tooltip angezeigt.

1

Typische URL-Manipulationen

- Ähnliche Domains: "paypa1.com" statt "paypal.com" (Ziffer "1" statt Buchstabe "l")
- Zusätzliche Subdomains: "amazon-konto.sicherheit-check.com" statt "amazon.com"
- Falsche TLDs: "deutsche-bank.xyz" statt "deutsche-bank.de"
- Verschleierte Links: Text zeigt "https://www.paypal.com", Link führt aber woanders hin

2

Gefährliche Anhänge

- Ausführbare Dateien: .exe, .bat, .cmd, .scr, .js
- Doppelte Dateiendungen: "Rechnung.pdf.exe"
- Office-Dateien mit Makros: .docm, .xlsm
- Archive mit versteckten Dateien: .zip, .rar mit Schadsoftware

3

Sicherheitsmaßnahmen

- Immer direkt die offizielle Website aufrufen statt auf Links zu klicken
- Bei Unsicherheit: URL manuell im Browser eingeben
- Verdächtige Anhänge niemals öffnen
- Im Zweifels beim vermeintlichen Absender nachfragen (über bekannte Adressen)

Besonders verdächtig sind Links, die Sie auffordern, sich einzuloggen oder persönliche Daten einzugeben. Bei Anhängen gilt grundsätzlich: Öffnen Sie keine Dateien von unbekannten Absendern oder wenn Sie solche Anhänge nicht erwarten.

Schritt 4: Rechtschreibung und Grammatik

Die sprachliche Qualität einer E-Mail kann ein entscheidender Hinweis auf ihre Legitimität sein. Während seriöse Unternehmen in der Regel großen Wert auf eine fehlerfreie und professionelle Kommunikation legen, enthalten Phishing-E-Mails häufig auffällige sprachliche Mängel. Diese entstehen oft durch maschinelle Übersetzungen oder durch Absender, deren Muttersprache nicht Deutsch ist.

Achten Sie besonders auf folgende sprachliche Warnsignale:

- **Offensichtliche Rechtschreibfehler:** Falsch geschriebene alltägliche Wörter oder Firmennamen (z.B. "Deustche Bank" statt "Deutsche Bank")
- **Grammatikalische Fehler:** Falsche Artikel, fehlerhafte Zeitformen oder unpassende Präpositionen
- **Ungewöhnliche Satzkonstruktionen:** Formulierungen, die im Deutschen unnatürlich klingen und vermutlich direkt aus einer anderen Sprache übersetzt wurden
- **Inkonsistente Formatierung:** Wechselnde Schriftarten, uneinheitliche Absätze oder unregelmäßige Abstände
- **Sprachmischungen:** Plötzlicher Wechsel zwischen Deutsch und anderen Sprachen oder die Verwendung fremdsprachiger Begriffe, wo deutsche Ausdrücke üblich wären

Schritt 5: Verdächtige Aufforderungen

Ein zentrales Ziel von Phishing-Attacken ist es, an Ihre persönlichen Daten, Zugangsdaten oder sogar direkt an Ihr Geld zu gelangen. Besondere Vorsicht ist daher geboten, wenn eine E-Mail Sie zu bestimmten Handlungen auffordert, besonders wenn diese mit der Preisgabe sensibler Informationen verbunden sind.

Anfrage nach Login-Daten

Seriöse Unternehmen fordern Sie niemals per E-Mail auf, Ihre Passwörter mitzuteilen oder über einen mitgesendeten Link einzugeben. Banken und Online-Dienste betonen sogar, dass Sie Ihre Zugangsdaten niemals preisgeben sollten.

Anfrage nach persönlichen Daten

Geben Sie niemals vertrauliche Informationen wie Kreditkartennummern, Kontoauszüge oder andere sensible Daten per E-Mail weiter. Seriöse Unternehmen fragen solche Informationen normalerweise nicht auf diesem Weg ab.

Aufforderungen zu Geldzahlungen

Seien Sie vorsichtig bei E-Mails, die Sie zu Geldüberweisungen auffordern, z.B. um angebliche Rechnungen zu begleichen. Überprüfen Sie solche Zahlungsaufforderungen immer separat, bevor Sie darauf reagieren.