SECURITY-MINDED

Praktisches Sicherheitswissen
für den Alltag

DIE FAKTEN ZU PHISHING

Betrügerische E-Mails sind auf Arbeit wie auch zu Hause eine Bedrohung

Was würden Sie tun, wenn ein verdächtiger Fremder Sie auf der Straße ansprechen und Sie in eine dunkle Seitengasse locken würde? Sie würden vermutlich die Gefahr spüren und weglaufen oder um Hilfe rufen.

Doch was ist, wenn dieser Fremde Sie per E-Mail anspricht? Vielleicht fühlen Sie sich sicher genug, um auf einen Link in der E-Mail zu klicken oder eine angehängte Datei zu öffnen – und tappen damit in die Falle.

Jeden Tag versuchen Cyberkriminelle mithilfe schädlicher E-Mails, Einzelpersonen und Unternehmen zu betrügen, was als „Phishing“ bezeichnet wird. Wenn Sie mit Phishing-E-Mails interagieren, bringt das ernsthafte Risiken für Sie, Ihren Arbeitgeber und sogar Ihre Familie und Freunde mit sich. Zum Glück ist es nicht schwer, das Erkennen und Vermeiden dieser Angriffe zu erlernen.

Was ist Phishing?

Bei einem Phishing-Angriff versuchen Cyberkriminelle mit betrügerischen E-Mail-Ködern, Informationen „zu angeln“ und Benutzer „an den Haken“ zu bekommen. Diese E-Mails sind raffiniert gestaltet, um Sie zur Preisgabe von Finanzdaten, Anmeldeinformationen oder sonstigen vertraulichen Daten zu verleiten. Die Kriminellen können auch heimlich schädliche Software (Malware) installieren, die Ihren Computer und die darauf gespeicherten Dateien infizieren.

Phishing-E-Mails setzen Sie meist unter Druck, damit Sie ohne Nachzudenken handeln. Dabei setzen sie auf starke Emotionen wie Neugierde, Angst oder Gier. Diese psychologischen Manipulationsmethoden werden auch als „Social Engineering“ bezeichnet.

Phishing-E-Mails nutzen auch verschiedenste technische Tricks, um Informationen zu stehlen:

- **Schädliche Weblinks:** Sie werden gebeten, auf einen Link zu klicken, der Sie auf eine betrügerische oder mit Malware infizierte Website führt.
- **Schädliche Anhänge:** Sie werden dazu gedrängt, einen unerwarteten Anhang zu öffnen, der Malware enthält.
- **Betrügerische Daten-eingabeformulare:** Sie werden aufgefordert, vertrauliche Informationen wie Benutzer-IDs, Kennwörter, Kreditkartendaten und Telefonnummern einzugeben.

Jeden Tag versuchen Cyberkriminelle mithilfe schädlicher E-Mails, Einzelpersonen und Unternehmen zu betrügen, was als „Phishing“ bezeichnet wird.

TIPPS FÜR FAMILIE UND FREUNDE

Geben Sie Ihr Wissen über Phishing weiter. Fragen Sie die Familie und Freunde nach deren Kompetenzen und Erfahrungen mit Cybersicherheit.

1. **Denken Sie nach, bevor Sie klicken.** Sie sollten E-Mails nicht automatisch vertrauen, insbesondere bei Angstmache oder verdächtig guten Angeboten. Bekannte Logos, Absendernamen und persönliche Informationen werden häufig von Betrügern gefälscht.
2. **Vorsicht bei unerwarteten Anfragen nach persönlichen Informationen.** Geben Sie niemals Kontonummern, PINs oder Anmeldedaten per E-Mail weiter, selbst wenn die Anfrage dringend klingt.
3. **Überprüfen Sie Anhänge vor dem Öffnen oder Herunterladen.** Selbst wenn eine E-Mail scheinbar von einem bekannten Unternehmen oder einer vertrauten Person stammt, sollten Sie unerwartete Anhänge nicht öffnen. Um sicherzustellen, dass die Datei legitim ist, kontaktieren Sie das Unternehmen oder die Person direkt über die Website oder eine bekannte Telefonnummer.

Ist Phishing wirklich ein Problem für mich?

Viele Unternehmen müssen mit ernsthaften Datenschutzverletzungen fertig werden, bei denen alles von Geschäftsgeheimnissen bis zu vertraulichen Daten von Millionen Menschen kompromittiert wurde. Diese Datenschutzverletzungen beginnen häufig damit, dass eine Person mit einer Phishing-E-Mail hereingelegt wird und Kriminellen Zutritt gewährt.

Phishing kann auch Ihr Privatleben beeinträchtigen. Ganz gleich, ob zu Hause oder auf Arbeit: Auf eine Phishing-E-Mail hereinzufallen kann schwerwiegende und lange anhaltende Konsequenzen haben.

Die Folgen erfolgreicher Phishing-Versuche

Auf Arbeit	Im Privatleben
• Verlust von Unternehmensgeldern • Kompromittierte personenbezogene Informationen von Kunden und Kollegen • Außenstehende greifen auf vertrauliche Kommunikation, Dateien und Systeme zu • Dateien werden gesperrt und unbenutzbar • Rufschädigung des Arbeitgebers	• Geld wird von Ihrem Bankkonto gestohlen • Betrügerische Belastung Ihrer Kreditkarte • In Ihrem Namen eingereichte Steuererklärungen • In Ihrem Namen abgeschlossene Kredite • Verlorener Zugriff auf Fotos, Videos und Dateien • Gefälschte Social-Media-Posts in Ihren Konten

Was kann ich tun?

- **Trainieren Sie Ihre Anti-Phishing-Kompetenzen.** Die Mitarbeit beim unternehmenseigenen Schulungsprogramm zur Steigerung des Sicherheitsbewusstseins ist eine sehr gute Möglichkeit, die Erkennung von Anzeichen für einen Phishing-Versuch zu üben.
- **Suchen Sie nach Möglichkeiten, mehr über Phishing zu erfahren.** Weitere Artikel in dieser Serie stellen bestimmte Phishing-Typen und weitere Sicherheitsprobleme detailliert vor.
- **Finden Sie heraus, wie Sie verdächtige E-Mails melden können.** Die E-Mail-Plattform Ihres Unternehmens hat möglicherweise eine Schaltfläche, mit der Sie potenzielle Phishing-Versuche schnell melden können. Vielleicht müssen Sie die Nachricht aber auch an ein bestimmtes IT-Postfach weiterleiten.