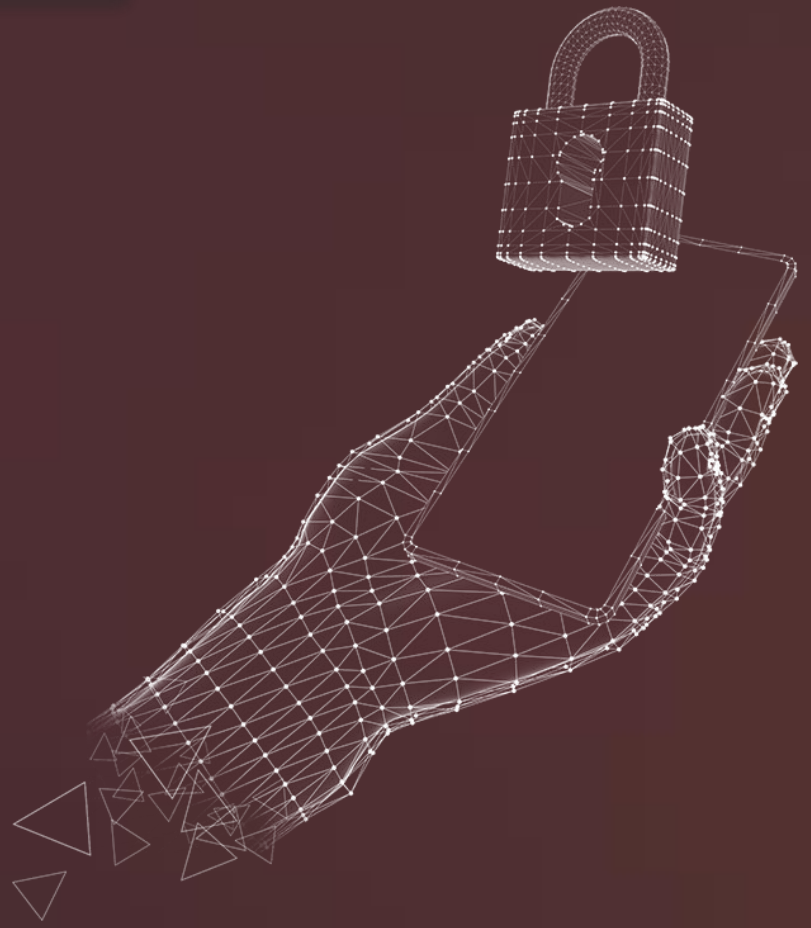
WebGuide

1 Phishing

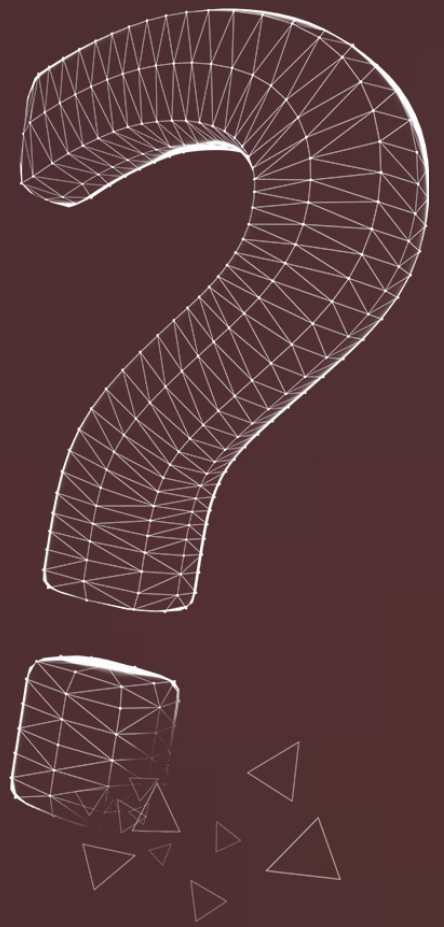
Phishing ist eine Form des Social Engineering, bei der E-Mails oder bösartige Websites verwendet werden, um persönliche Informationen zu erfragen oder Sie dazu zu bringen, schädliche Software herunterzuladen, indem sie sich als vertrauenswürdige Entität ausgeben.



WebGuide

2 Arten von Phishing

- **Spearphishing**: Gezieltes Phishing auf eine Einzelperson, indem spezifische Informationen über sie verwendet werden.
- **Whaling**: Phishing, das auf hochrangige Persönlichkeiten abzielt, um sensible und wertvolle Informationen zu stehlen.
- **Vishing**: Phishing über Sprachkommunikation, um das Opfer zu einem Gespräch zu verleiten und Vertrauen aufzubauen.
- **Smishing**: Phishing über Textnachrichten, um das Opfer zum Anklicken eines Links, zum Herunterladen von Dateien und Anwendungen oder zum Beginn eines Gesprächs zu bewegen.
- **Clone Phishing**: Hierbei wird eine legitime, bereits versendete E-Mail kopiert, aber mit bösartigen Links oder Anhängen versehen.
- **Pharming**: Umlenken von Internetnutzern von legitimen Websites auf gefälschte Websites, um Informationen zu stehlen.



WebGuide

3 Einfache Tipps

- **Bei Zweifeln melden**: Wenn es verdächtig aussieht, als „Junk“ markieren und an Ihre IT-Abteilung weiterleiten.
- **Denken, bevor Sie handeln**: Seien Sie vorsichtig bei Kommunikationen, die Sie zu sofortigem Handeln auffordern, etwas zu Gutes anbieten oder nach persönlichen Informationen fragen.
- **Vorsicht bei Hyperlinks**: Vermeiden Sie es, auf Hyperlinks in E-Mails zu klicken; fahren Sie mit dem Cursor über Links im Text der E-Mail – wenn die Links nicht mit dem Text übereinstimmen, der beim Darüberfahren erscheint, könnte der Link gefälscht sein.
- **Bestätigen Sie die Identität des Absenders**: Wenn Sie Zweifel an der Glaubwürdigkeit einer Nachricht haben, kontaktieren Sie die Organisation direkt über eine bekannte und vertrauenswürdige Telefonnummer oder Website.
- **Informieren Sie sich über gängige Betrugsmaschen**: Regelmäßige Information über neue Phishing-Taktiken kann helfen, verdächtige Nachrichten zu erkennen.
- **Verwenden Sie starke, einzigartige Passwörter**: Erstellen Sie für jeden Online-Dienst ein eigenes Passwort und verwenden Sie Kombinationen aus Buchstaben, Zahlen und Sonderzeichen.

4 Anzeichen für Phishing

- Verdächtige **Absenderadresse**, die ein legitimes Unternehmen nachahmen könnte.
- Allgemeine Begrüßungen und Signaturen und ein **Mangel** an Kontaktinformationen im Signaturblock.
- **Gefälschte** Hyperlinks und Websites, die nicht mit dem Text übereinstimmen, wenn man darüberfährt.
- **Rechtschreibfehler**, schlechte Grammatik oder Satzbau und inkonsistente Formatierung.
- Verdächtige Anhänge oder **Aufforderungen**, einen Anhang herunterzuladen und zu öffnen.