

CSBW-Factsheet: Cybersecurity-Wissen kompakt

PHISHING-E-MAILS

Phishing-E-Mails zählen zu den Haupteinfallstoren von Cyberattacken und können sehr hohe wirtschaftliche und betriebliche Schäden verursachen.

Bitte nehmen Sie sich Zeit, Ihre E-Mails gründlich zu überprüfen, und helfen Sie mit, die Verbreitung von schädlichen Nachrichten zu verhindern.

Trotz aller
Vorsicht und
Präventionsmaßnahmen
kann es sein, dass auch
Sie Empfänger einer
Phishing-E-Mail
werden.

PHISHING setzt sich aus **password** und **fishing** zusammen (dt.: **nach Passwörtern angeln**).

Cyberkriminelle schreiben **gefälschte Nachrichten und verlinken auf gefälschte Webseiten**, um an vertrauliche Informationen wie **Passwörter, Zugangsdaten oder Kreditkartennummern** zu gelangen.

Darüber hinaus bergen Phishing-E-Mails aber auch immer mehr Malware-behaftete Datei-Anhänge, die Schadsoftware, wie Trojaner oder Ransomware, einschleusen.

SMISHING bezeichnet dieselbe Betrugsmasche, die jedoch per **SMS** anstatt per E-Mail verbreitet wird.

Handlungsempfehlungen:

- › Überprüfen Sie jede E-Mail auf die unten stehenden Kriterien und kontaktieren Sie bei Verdacht umgehend Ihre zuständige IT-Abteilung.
- › Warnen Sie Ihre Kolleginnen und Kollegen, dass eine verdächtige E-Mail im Umlauf ist.
- › Öffnen Sie niemals Links oder Anhänge von verdächtigen E-Mails und geben Sie keine geheimen Informationen wie Passwörter, Kontodaten, PIN oder TAN ein.

Woran erkenne ich Phishing-E-Mails?

Kontrollieren Sie jede E-Mail auf Grundlage der folgenden Merkmale:

- › Oftmals wird keine **persönliche Anrede** genutzt. Ihre Bank und Online-Zahlungsdienste sprechen Sie in E-Mails grundsätzlich mit Ihrem Namen an und niemals mit „Sehr geehrter Kunde“.
- › Zumeist ist die **Absender-Adresse gefälscht** und durch Zusätze wie „Service“ oder „Info“ ergänzt.
- › Achten Sie besonders auf **Abweichungen zwischen dem angeblichen Absender und der neben dem Absender stehenden E-Mail-Adresse!**
- › Betrugs-E-Mails kommunizieren meist **dringenden Handlungsbedarf** und **drohen mit Konsequenzen**.
- › **Orthografie und Grammatik** sind oft fehlerhaft.
- › Betrugs-E-Mails **enthalten entweder einen schadhaften Link oder einen schadhaften Anhang**.
- › Kein seriöser Absender fordert Sie zur Eingabe Ihrer persönlichen Daten per E-Mail oder SMS auf!
- › Die Zieladresse des Links können Sie einsehen, indem Sie mit der Maus über den Link fahren, ohne darauf zu klicken.
Kontrollieren Sie folgende Kriterien:
 - Fake-Webseiten enthalten oftmals nicht-lateinische Buchstaben, falsch aufgelöste Umlaute z.B. „ae“ statt „ä“, **andere Schreibweisen**, beispielsweise eine 0 (Null) statt des Buchstabens O, oder **Website-Endungen** wie .ru, .pl oder .to.
 - Fake-Webseiten fehlen oftmals die Sicherheitsmerkmale: **https://** und das **Schlosssymbol**. **Aber Achtung: Immer mehr Betrüger erwerben ein SSL-Zertifikat**
→ https: bedeutet heute also keine Entwarnung mehr!
- › Phishing-E-Mails sind oftmals **in fremder Sprache verfasst** bspw. Englisch oder Französisch oder sind fehlerhaft ins Deutsche übersetzt.