Phishing erkennen

🪝 Was ist Phishing?

Phishing ist der Versuch, über gefälschte E-Mails, Nachrichten oder Webseiten an vertrauliche Daten wie Passwörter, Bankdaten oder Zugangsdaten zu gelangen.
Die Angreifer geben sich häufig als vertrauenswürdige Quellen aus (z. B. Kollegen, Vorgesetzte, Banken, Paketdienste oder IT-Abteilungen).

So erkennst du Phishing-Mails:

🔍 Ungewöhnliche Absenderadresse

Die E-Mail-Adresse des Absenders stimmt nicht mit dem Namen des Unternehmens oder der Person überein, von der die E-Mail angeblich stammt. Untenstehend findest du einige Beispiele:

Gefälschte Unternehmensadressen:
security-update@micr0soft.com („0“ statt „o“)
info@aple.com (falsche Apple-Domäne – korrekt wäre apple.com)

➔ Prüfen auf korrekte Schreibweise und ob die Domäne z.B. https: verschlüsselt ist

Absender mit falschen Subdomänen:
info@microsoft.emea.com (die korrekte Subdomäne lautet emea.microsoft.com)
billing@amazon.accounting.ru (accounting.ru deutet auf eine falsche Subdomäne hin)

➔ Subdomänen werden durch einen zusätzlichen Punkt in der URL erstellt (z.B. gemeinde.biberist.ch). Wichtig ist, was vor und nach dem letzten Punkt steht. (gemeinde.biberist.ch)

Ungewöhnliche Domänen:
support@microsoft-login.tk (tk ist eine ungewöhnliche Top-Level-Domäne)
service@globalbanking.ga (ga ist eine ungewöhnliche Top-Level-Domäne)

➔ Gängige Top-Level-Domänen sind beispielsweise .ch, .de, .com.

Griechische Zeichen:
support@citibαnk.com (anstelle des "a" wird "Alpha" aus dem griechischen Alphabet verwendet).

➔ Korrekt wäre support@citibank.com

🌎 Link überprüfen

Überprüfe verdächtige Links, in dem du mit dem Mauszeiger über den Link fährst (nicht klicken). Falls die angezeigte URL nicht mit dem Link übereinstimmt oder verdächtig aussieht, empfehlen wir, den Link nicht zu öffnen.

📎 Unerwartete Anhänge oder Links

Öffne keine Anhänge oder Links, wenn du den Absender nicht eindeutig kennst oder die Nachricht verdächtig wirkt.

📝 Rechtschreibfehler

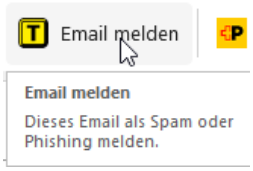
Rechtschreibfehler in der E-Mail, unlogische Formulierungen oder ungewöhnliches Layout sind ein Warnsignal.

🔑 Aufforderung zur Eingabe von Daten

Seriöse Unternehmen fordern niemals per E-Mail zur Eingabe von Passwörtern auf.

So verhältst du dich im Verdachtsfall:

1. 📩 Nicht antworten, nichts anklicken!
2. 🟨 Verdächtige E-Mails via Button "E-Mail melden" in Outlook melden
3. 🛑 Bei versehentlichem Klick: IT-Abteilung telefonisch informieren!
4. 🔐 Passwörter ändern, falls du Daten preisgegeben hast.



Unsere IT-Abteilung steht dir bei Fragen gerne zur Verfügung:

✉️ informatik@biberist.ch
☎️ Christoph Wieland: intern 207 / Christoph Aemmer: intern 217