WEITERE INFOS

https://phishing-master.secuso.org

https://www.hs-anhalt.de/
informationssicherheit/
sicherheitstipps/
email-sicherheit

ISI
Phishing-Tipps

Vor Phishing schützen

HOCHSCHULE ANHALT University of Applied Sciences

www.hs-anhalt.de

Phishing-E-Mails:
Woran man sie erkennt und worauf zu achten ist!

Phishing bezeichnet das „Angeln“ nach persönlichen Daten, Berechtigungen, Passwörtern, PINs, TANs oder Kreditkartendaten. Die Cyberkriminellen können mit Ihrer Kennung einkaufen, E-Mails schreiben, soziale Kontake manipulieren, Geld von Ihnen fordern und/oder Überweisungen in Ihrem Namen tätigen.

Doch wie erkennen wir eine Phishing-Nachricht?
Wer wissen möchte, ob es sich um eine Phishing-E-Mail handelt, sollte den **WER-Bereich einer Webadresse** kennen oder regelmäßig z. B. mit dem Spiel „Phishing Master“ üben, Webadressen richtig zu lesen und Phishing-Nachrichten zu erkennen.

14 typische Anzeichen für einen Phishing-Versuch

1. Passen Absender und Nachrichtentext inhaltlich zusammen?
2. Ergibt die Nachricht einen Sinn bzw. kann die Behauptung stimmen?
3. Wird Druck ausgeübt und dringender Handlungsbedarf suggeriert?
4. Sollen bestehende Sicherheitsregularien umgangen werden?
5. Ist die Empfänger-Adresse die richtige?
6. Klingt der Betreff der E-Mail verdächtig?
7. Hängt an der E-Mail ein überprüfbares, korrektes Signaturzertifikat?
8. Wie korrekt sind Ausdruck, Rechtschreibung und Sprache?
9. Werden Sie persönlich angesprochen?
10. Auf welche Webseite führt Sie der angegebene Link tatsächlich und ist es eine sichere Webseite mit `https://` ?
11. Wo ist der **WER-Bereich** der Webadresse (vor dem 1. einfachen Schrägstrich)
    Achtung – Phish-Adresse! `https://www.mein-dhlpkaet.de.host123.com/login`
12. Ist der WER-Bereich **korrekt** geschrieben?
    Auch hier handelt es sich um eine Phish-Adresse! `https://www.mein-dlhpaket.de/login`
13. Besteht der WER-Bereich (nur) aus **Zahlen**?
    Noch ein Beispiel für eine Phish-Adresse! `https://mein-dhlpaket.129.15.140.7/login`
14. Enthält die Nachricht gefährliche, ausführbare oder unbekannte **Dateianhänge**?
    Vorsicht ist geboten! `.exe, .bat, .cmd, .docm, .xlsm, .zip, unbekanntes Format`

Wenn Sie den Verdacht haben, eine Phishing-Nachricht auf Ihrer Hochschuladresse erhalten zu haben, schicken Sie diese bitte **als Anhang** an: *phishing@hs-anhalt.de* oder kontaktieren Sie den zuständigen Administrator Ihres Bereiches.