Cheat Sheet: Phishing erkennen

E-Mail - Checkliste

Löschen oder melden Sie E-Mails an virenwarndienst@hrz.uni-marburg.de, wenn Sie eine oder mehrere der folgenden Fragen mit ‚nein' beantworten können.

- Kennen Sie den/die Absender/in?
- Ist die E-Mail-Adresse korrekt bzw. vertrauenswürdig?
- Betrifft mich die E-Mail?
- Werde ich gezielt angesprochen?
- Stimmen Grammatik, Satzbau und Rechtschreibung?
- Führen enthaltene Links zu einer vertrauenswürdigen Seite?
- Sind enthaltene Anhänge vertrauenswürdig?

Hinweis:

Seien Sie besonders vorsichtig, wenn Druck aufgebaut wird oder Sie nach Anmeldedaten gefragt werden!

Phishing-Links erkennen

- Auf welche Seite führt der Link? -> Links prüfen!
- Sind Tippfehler oder Buchstabendreher vorhanden?
  ▸ uni-marbrug.de
- WICHTIG Vor dem dritten „**/**" steht die Hauptadresse, wobei von rechts nach links aufgerufen wird
  ▸ https://uni-marburg.de.malware.com**/**xxx
  ▸ d.h. hier wird auf malware.com verwiesen

Gefährliche Anhänge erkennen

Nicht öffnen:
- Veraltete Office-Dokumente: .doc, .xls, .ppt
- Ausführbare Dateien: .exe, .vbs, .js, .ps1

Nur öffnen, wenn erwartet:
- Office-Dokumente mit Makros: docm, .xlsm, .pptm
  (Makros nur nach telefonischer Rücksprache mit dem/der Absender/in aktivieren)
- Archivierte Dateien: .zip, .rar, .7z

Vorsichtig öffnen:
- Aktuelle Office-Dokumente: .docx, .xslx,. .pptx
- .pdf
  ▸ enthaltene Links trotzdem prüfen

Stabsstelle Informationssicherheit
Hans-Meerwein-Straße 6
35032 Marburg
IT-Notfallrufnummer: 06421 28-28281
E-Mail: it-sicherheit@uni-marburg.de

Universität Marburg

Erfahren Sie mehr über Phishing, Social Engineering und sichere Passwörter in **unserer Online-Schulung**.

https://uni-marburg.de/zozuS