Cheat Sheet: Phishing-Mails erkennen

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

E-Mail - Checkliste

- 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?

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

Gefährliche Anhänge erkennen

Nicht öffnen:

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

Achten Sie bei Office-Dokumenten auf die Endung!

Nur öffnen, wenn erwartet:

- Office-Dokumente mit Makros: doc**m**, .xls**m**, .ppt**m**
  (Makros nur nach telefonischer Rücksprache mit dem/der Absender/in aktivieren)
- Archivierte Dateien: .zip, .rar, .gz

Vorsichtig öffnen:

- Aktuelle Office-Dokumente: .doc**x**, .xsl**x**,. .ppt**x**
- .pdf
- ► enthaltene Links trotzdem prüfen

Phishing-Links erkennen

- Auf welche Seite führt der Link?
- Links vor dem Aufrufen kopieren und in ein Textverarbeitungsprogramm oder eine Suchmaschine kopieren
- Was steht vor dem dritten „/“?
  - ► https://uni-marburg.de.**malware.com/**xxx
- Sind Tippfehler oder Buchstabendreher in der Hauptadresse des Links vorhanden?
  - ► uni-marbrug.de?

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

Philipps Universität Marburg

Erfahren Sie noch mehr über Phishing, Social Engineering und sichere Passwörter in unserer **Online-Schulung**.
https://uni-marburg.de/zozuS