Cheat Sheet: Recognising Phishing

E-Mail - Checklist

Delete or report emails to virenwarndienst@hrz.uni-marburg.de, if you can answer one or more of the following questions with 'no'.

- Do you know the author?
- Is the e-mail address correct or trustworthy?
- Does the e-mail refer to me (and my name)?
- Am I being addressed specifically?
- Are grammar, sentence structure and spelling correct?
- Do links contained in the e-mail lead to a trustworthy site?
- Are the attachments included trustworthy?

Note:

Be particularly careful when pressure is built up on you or you are are asked for login details!

Recognising phishing links

- Which page does the link lead to? -> Check links!
- Are there any typos or misspellings?
  ▸ uni-marbrug.de
- IMPORTANT The third '**/**' is preceded by the main address, which is accessed from right to left
  ▸ https://uni-marburg.de.malware.com**/**xxx
  ▸ i.e. this refers to malware.com

Recognising dangerous attachments

Do not open:
- Outdated Office documents: .doc, .xls, .ppt
- Executable files: .exe, .vbs, .js, .ps1

Only open if expected:
- Office documents with macros: docm, .xlsm, .pptm
  (only activate macros after telephone consultation with the sender)
- Archived files: .zip, .rar, .7z

Open carefully:
- Current Office documents: .docx, .xslx, .pptx
- .pdf
  ▸ nevertheless check the contained links therein

SIS | Staff Unit Information Security
Hans-Meerwein-Straße 6
35032 Marburg
IT-Emergency Phone: 06421 28-28281
E-Mail: it-sicherheit@uni-marburg.de

Marburg University

Find out more about phishing, social engineering and secure passwords in **our online training course.**

https://uni-marburg.de/4TOtel