Cheat sheet: Recognising phishing emails

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

E-Mail - Checklist

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

Be particularly careful if you are pressurised
or if you are asked for login details!

Recognising dangerous attachments

Do not open:

- Outdated Office documents: .doc, .xls, .ppt
- Executable files: .exe, .vbs, .js

Pay attention to the the ending of Office documents!

Only open if expected:

- Office documents with macros: docm, .xlsm, .pptm
  (Only activate macros after telephone consultation with the sender)
- Archived files: .zip, .rar, .gz

Open carefully:

- Current Office documents: .doc**x**, .xsl**x**, .ppt**x**
- .pdf
- ► Check links contained anyway

Recognising phishing links

- Which page does the link lead to?
- Copy links before calling them up and paste them into a word processing programme or a search engine.
- What comes before the third „/“?
  - ► https://uni-marburg.de.**malware.com**/xxx
- Are there any typing errors or misspellings in the main address of the link?
  - ► uni-marbrug.de?

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

Philipps Universität Marburg

Discover even more about phishing, social engineering and secure passwords in our **online training course**.
https://uni-marburg.de/4TOtel