Universität Münster

Checklist:
How to Detect Scam E-Mails
8 Points to recognize phishing, spam and other harmful e-mails

Is the sender unknown?
Is the e-mail address not suitable?
1

- Scam e-mails are often sent from unsuitable or implausible e-mail addresses.
- Be careful if you do not know the person sending the e-mail.
- Check whether the e-mail address matches the person sending the e-mail, such as "...@uni-muenster.de" for e-mails from members of the University of Münster.
- Check for a valid digital signature. Scam e-mails are usually **not** signed.

Are unrealistic benefits promised?
2

- Unrealistic winnings, discount or voucher cards (e.g. Amazon or Paysafecard) are often promised for advertising and fraud purposes.
- Be suspicious of free services. Such services often hide illegal offers or your login data is resold.

Does the sender create pressure?
3

- Calls for immediate action indicate fraud, such as logging onto a website immediately or making a money transfer.
- Threats of negative consequences can also be part of fraud attempts (e.g., blocking access).
- Verify supposed requests for action by the CIT. Legitimate messages from the CIT can also be found under operational messages on the CIT website.

Is confidential information requested?
4

- Scam e-mails often demand the disclosure of confidential data via e-mail or on a linked website (e.g. passwords).
- Before entering confidential data on a website, check whether the address is plausible and the connection is encrypted (http**s** instead of http).
- Enter login details from the University of Münster only on University websites.

Is the form of address impersonal?
5

- In scam e-mails, the form of address is often impersonal, missing or deviates from the usual form.
- Most companies or institutions will use your full name in the form of address. In fake messages, the form of address is often generic, such as "Dear Customer" or simply "Good afternoon".

Am I asked to click on a link?
6

- It is not always possible to see where links lead to. **Never** click on links from unknown senders without consideration.
- Check the Internet address by hovering the mouse pointer over the link: Links from scam e-mails are often confusingly similar (e.g. "uni-meunster.de" or "uni-muenster.de.com" instead of "**uni-muenster.de**").

Does the e-mail contain unexpected attachments?
7

- Do not open unknown or unexpected file attachments.
- If the e-mail is from a known person, in case of doubt, find out by other methods (telephone, Mattermost) whether this person actually sent the e-mail before you open it.
- Do not activate the edit mode or macros for attached Office files.

Does the e-mail contain errors?
8

- Texts from scam e-mails are often generated with the help of translation tools, leading to incorrect grammar or spelling (especially umlauts).

If one or more of the points apply, it is potentially a scam attempt. If you receive a scam e-mail related to the University of Münster, report it to the Computer Emergency Response Team at: spam@uni-muenster.de