Maastricht University

Digital safety

Phishing

In phishing cases, criminals pose as a manager or an organisation in order to deceive students into transferring money or sharing sensitive information. As a major knowledge institution, Maastricht University is regularly targeted. These tips will help you recognise suspicious messages more quickly.

- **Misleading display name**
  Phishing messages often appear to come from someone you know or from a manager. If you are in doubt, always check both the display name and the email address.

- **Unusual language**
  Phishing messages are often short and impersonal, deviate from normal working practices, and/or may contain language errors.

- **Requests for money or for opening links or attachments**
  Examples include payment requests, purchasing items such as gift cards, or entering your login details.

  UM will **never** ask you to buy *Apple gift cards*.

- **Urgency and time pressure**
  Phishing messages often create a sense of urgency. You are told to act quickly while the sender applies pressure or claims something is time sensitive.

- **Generic opening**
  Phishing messages often contain generic opening lines such as “There is a problem with your account” or “You have been selected for an important action.”

What to do when you receive a (possible) phishing message:

- If in doubt, **do not click** on any links or attachments. Check with the ICTS Service Desk.
- If you have accidentally clicked a link or made a payment, **report this immediately** to the ICTS Service Desk.

ICTS Service Desk: servicedesk-icts@maastrichtuniversity.nl

UM considers students affected by phishing to be victims, not at fault.

Scan the QR code for more information