Universiteit Maastricht

Veilig digitaal werken

Phishing

Bij phishing doen criminelen zich voor als een leidinggevende of organisatie om studenten te misleiden, geld over te maken of gevoelige informatie te verkrijgen. Ook binnen de universiteit komen phishingpogingen regelmatig voor. Met deze tips herken je verdachte berichten

- **Misleidende afzender**
  Phishingberichten lijken vaak van een bekende of leidinggevende te komen. Controleer de weergavenaam en het mailadres.

- **Ongebruikelijke taal**
  Berichten zijn vaak kort, onpersoonlijk, wijken af van werkafspraken en/of bevatten taalfouten.

- **Verzoeken om geld of het openen van links of bijlages**
  Denk hierbij aan betalingsverzoeken, aankoop van bijvoorbeeld cadeaukaarten of het invullen van inloggegevens.

  De UM vraagt NOOIT om 'Apple giftcards' te kopen.

- **Dringendheid en (tijds)druk**
  Phishingberichten zijn vaak urgent: je moet snel handelen, terwijl de afzender slecht

- **Algemene opening / aanhef**
  Phishing mails bevatten vaak algemene openingszinnen zoals, "Er is een probleem met uw account." of "U bent geselecteerd voor een belangrijke actie."

Dit moet je doen als je een (mogelijk) phishingbericht ontvangt:
Bij twijfel: niet klikken op links of bijlagen, maar maar bel met ICTS Servicedesk.

- Heb je per ongeluk op een link geklikt of betaling gedaan? Meld ook dit direct bij de ICTS Servicedesk.

ICTS Servicedesk: servicedesk-icts@maastrichtuniversity.nl

De UM beschouwt studenten die door phishing worden geraakt als slachtoffers, niet als schuldigen.

Scan de QR-code voor meer informatie