Universiteit van Amsterdam

IS HET PHISHING? CHECK DE LINK!

Een belangrijke indicator voor phishing is de url waar de link naar verwijst. Hoe weet je of deze te vertrouwen is? Lees het hier.

1 **Check de officiële url van de afzender. Twijfel je? Check op het internet of bel de afzender.**

2 **Beweeg je muis over de link in de e-mail, dan komt de url in beeld.**

Verkorte url

(zoals bit.ly)

Lastiger te controleren en kan dus malafide zijn. Wees extra alert. Controleer de url op *checkjelinkje.nl*

‘Gewone’ url

Let goed op de positie en de spelling van het hoofddomein (bijv. “uva”) en het topdomein (bijv. “.nl”). Hoe? Check hier

Safelink

(https://eur04.safelinks.protection.outlook.com...)

Microsoft checkt de url. Is deze malafide? Dan krijg je een waarschuwing. Let ook op andere phishing indicatoren.

- Het subdomein en de domeinnaam moeten gescheiden zijn met een punt.
- Hoofddomein en topdomein (of top-level-domein) moeten direct achter elkaar staan, gescheiden door een punt (.) Dus: uva.nl.

- Subdomein: het gedeelte van het adres dat vóór een domeinnaam kan staan. Meestal www, maar bijvoorbeeld ook: id.uva.nl
- Extra tekst achter de domeinnaam moet gescheiden zijn met een schuine streep (/). Dus: uva.nl/onderzoek
- Let goed op het topdomein. E-mail van Nederlandse organisatie? Grote kans op .nl-domeinnaam. Is topdomein dan .tk (Tokelau), .in (India) of .ru (Rusland)? Wees extra alert.

Vragen? ciso@uva.nl

September 2020