Amsterdam University of Applied Sciences

IS IT PHISHING? CHECK THE LINK!

An important indicator for phishing is the url where the link refers to. How do you know if it can be trusted? Read it here.

1 **Check the official url of the sender. In doubt? Search it on the Internet or call the sender.**

2 **Move your mouse over the link in the email, then the url will emerge.**

Short url

(like bit.ly)

More difficult to check and can therefore be malicious. Be extra alert. Check the url on *checkjelinkje.nl*

Regular url

Pay close attention to the position and the spelling of the second level domain (SLD), eg “hva” and the top level domain (TLD), eg “.nl”. How? Check here.

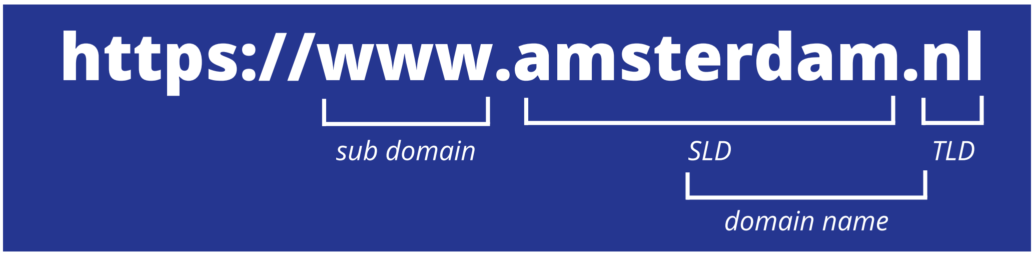
Safelink

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

Microsoft checks the url. When malicious, you get a warning. Also pay attention to other phishing indicators.

The subdomain and domain name should be separated with a dot.

SLD and TLD should be directly behind each other, separated by a dot (.) Like this: amsterdamuas.com



https://www.amsterdam.nl

sub domain

SLD

TLD

domain name

Subdomain: the part of the url that comes before an SLD. Usually www, but also, for example: id.hva.nl

Extra text after domain name must be separated with a slash (/). For example: amsterdamuas.com/research

Pay close attention to the TLD. Is it an e-mail from a Dutch organization? Then the url is likely to have ‘.nl’ as TLD. Is the TLD .tk (Tokelau), .in (India) or .ru (Russia)? Be extra alert.

Any questions? ciso@hva.nl

May 2020