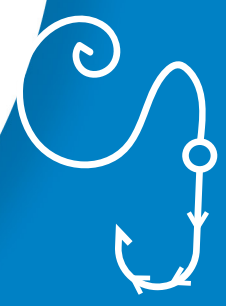
PHISHING

First check

Phishing emails will always ask you for something, sometimes for a seemingly legitimate reason. Clear red flag is when it is 'very urgent'. Always check whether the email address and domain name that are used match the details of your contact. Also check whether links point to the correct location by hovering over them with your mouse. **Do not click these links**!



Phishing?

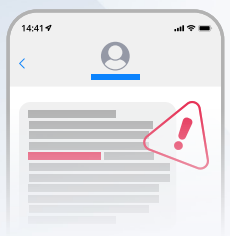
Cybercrime in which an attacker impersonates a trusted source to obtain sensitive information from a victim.

Typosquatting? Not so healthy!

Typosquatting is the use of misspelled domain names to trick users into thinking the site they are trying to visit is legitimate. Not sure? Do not click and surf to the website yourself.

Pay extra attention to spear phishing

The attacker looks up personal information about a specific target, such as the employer (and therefore colleagues), recent online purchases, etc. With this data, the attacker can send an authentic-looking message that appears to come from a trusted source, such as an employer, colleague or company you recently ordered from. Do you suddenly receive a strange email from a colleague? Be aware!



Vishing and smishing

People also try to access data via telephone (= vishing) or SMS (= smishing). So never share passwords via these channels, do not click on suspicious links and avoid communicating sensitive information.

Received a suspicious message?

suspicious@safeonweb.be

Automated security awareness training and simulations.

↘ **www.k-force.be/en/phishing**

RECOGNIZE

K-Force Computer Solutions

YOUR PARTNER IN CLOUD, IT & TELECOM

If in doubt, contact K-Force!

Helpdesk	**helpdesk@k-force.be**
Sales	**sales@k-force.be**
Proximus	**proximus@k-force.be**
General	**info@k-force.be**
Administration	**administration@k-force.be**
Phone	**02 380 23 32**
Mo - Fri	8h - 12h & 13h - 17h

Never share your password or sensitive information with third parties!