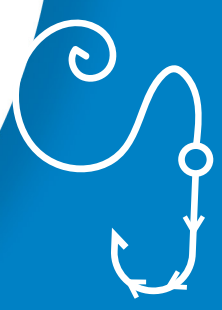
PHISHING

Eerste controle

Phishingmails zullen altijd iets van je vragen, soms met een schijnbaar legitieme reden. Duidelijke rode vlag is wanneer het 'zeer dringend' is. Controleer ook altijd of het gebruikte mailadres en domeinnaam overeenkomen met deze van jouw contact en of links wel naar de juiste locatie verwijzen, door er even met je muis op te blijven staan.

Klik niet op deze links!



Phishing?

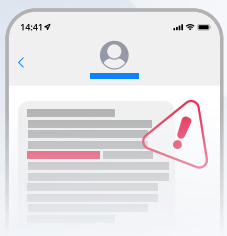
Cybercriminaliteit waarbij een aanvaller zich voordoet als een betrouwbare bron om gevoelige informatie van een slachtoffer te ontfutselen.

Typosquatting? Niet zo gezond!

Typosquatting is het gebruik van verkeerd gespelde domeinnamen om gebruikers te laten denken dat de site die ze proberen te bezoeken legitiem is. Ben je niet zeker? Surf dan zelf naar de website.

Extra opletten bij spear phishing

De aanvaller zoekt persoonlijke gegevens op van een specifiek doelwit, zoals de werkgever (en dus collega's), recente online aankopen, etc. Met deze gegevens kan de aanvaller een authentiek uitziend bericht sturen dat afkomstig lijkt te zijn van een vertrouwde bron, zoals een werkgever, collega of bedrijf waar je recent bestelde. Krijg je plots een vreemde mail van een collega? Opgelet!



Vishing en smishing

Ook via telefoon (= vishing) of sms (= smishing) probeert men aan gegevens te raken. Geef dus ook via deze wegen nooit wachtwoorden door, klik niet op verdachte links en vermijd het communiceren van gevoelige informatie.

Verdacht bericht ontvangen?

verdacht@safeonweb.be

Geautomatiseerde security awareness training en simulaties.

↘ **www.k-force.be/nl/phishing**

HERKEN

K-force Computer Solutions

YOUR PARTNER IN CLOUD, IT & TELECOM

Twijfel? Contacteer K-Force!

Helpdesk	**helpdesk@k-force.be**
Sales	**sales@k-force.be**
Proximus	**proximus@k-force.be**
Algemeen	**info@k-force.be**
Administratie	**administration@k-force.be**
Telefoon	**02 380 23 32**
Ma - vrij	8h - 12h & 13h - 17h

Geef nooit zomaar je wachtwoord of gevoelige info aan derden!