CYBER SECURITY

Verdachte mails? Step back and check!

Is er spoed bij, wordt er gevraagd om een bijlage te openen of je aan te melden?
Bel bij twijfel de afzender of contacteer K-Force.

Ken je deze tips al?

Gebruik ze om veilig digitaal te werken!

Help mee en vergrendel je pc

Voorkom dat anderen je toestel en programma's gebruiken, met je gegevens kunnen aanmelden of handelingen uitvoeren. Vergrendel altijd je toestel als je (even) wegloopt of pauze neemt.

Apple: control + command + Q

Windows: ⊞ + L

Geef nooit je wachtwoord

Vertrouw het niet als men je wachtwoord per e-mail, messenger, sms, enz. vraagt. Banken, overheidsinstellingen, Microsoft, ... vragen nooit om een wachtwoord.

Moet je toch wachtwoorden delen, bvb. met collega's of klanten? Gebruik One Time Secret of een professionele wachtwoordmanager.

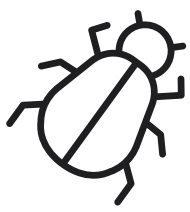
www.onetimesecret.com

Openbare wifi? Nee, kies voor 4/5 G!

Een wifi-netwerk zonder beveiliging (een toegangssleutel)? Hackers kunnen meeluisteren en dus gegevens stelen.

www.k-force.be

k-force
connected by ict



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

PHISHING HERKEN

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 er niet op!

Hoe herken je phishing?

Phishing is cybercriminaliteit waarbij een aanvaller zich voordoet als een betrouwbare bron om gevoelige informatie te ontfutselen.

Typosquatting? Niet zo gezond!

Typosquatting is het gebruik van verkeerd gespelde domeinnamen of varianten om gebruikers te laten denken dat de site die ze proberen te bezoeken legitiem is. Ben je niet zeker? Typ dan manueel het websiteadres.

EXAMPLES FOR ANOMALIBANK.COM

- anomalibank.com ✓
- update-anomalibank.com ✗
- anomalibank-alert.x7462e7.com ✗
- wwwanomalibanksecure.com ✗

EXAMPLES FOR DOMAIN.COM:

- domain.com ✓
- domian.com ✗
- domains.com ✗
- doma1n.com ✗
- domain.cm ✗

Impersonalisatie en onderzoek

Aanvallers zoeken meer en meer persoonlijke gegevens op van een specifiek doelwit, zoals de werkgever (en collega's), recente online aankopen, etc. Met deze gegevens kan men 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!

Aanmelden of betalen

Wees altijd extra alert wanneer er gevraagd wordt naar je logingegevens. Probeer enkel aan te melden als je 100% zeker bent dat de URL van de website correct is. Ook als het gaat om betalingen is extra voorzichtigheid geboden. Is het rekeningnummer nieuw, een buitenlands nummer of moet er betaald worden via een cryptowallet? Dit is extra verdacht!

k-force
connected by ict

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

Verdacht bericht ontvangen?

verdacht@safeonweb.be

Geautomatiseerde security awareness training en simulaties om alert te blijven.

↘ **www.k-force.be/nl/phishing**

SOCIAL ENGINEERING

Piggybacking

Een niet-bevoegde persoon probeert fysiek toegang te krijgen tot afgeschermde ruimtes door mee te liften met een medewerker. Serverruimtes zijn natuurlijk een zeer gewild doelwit. Een goed voorbeeld van deze techniek zijn de experimenten waarbij personen door enkel het dragen van een fluohesje vaak heel ver kunnen binnendringen in een bedrijf.

Social engineering

Social engineering draait om het beïnvloeden van mensen zodat ze gevoelige informatie prijsgeven of handelingen doen die beveiligingssystemen ondermijnen.

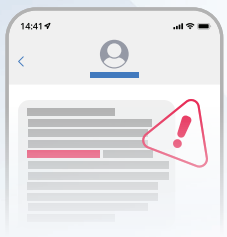
Pretexting en BEC

Pretexting is het verzinnen van een geloofwaardig verhaal om iemand te misleiden. Het klassieke voorbeeld hier zijn zogezegde technici van Microsoft die je willen ‘helpen’ met een computerprobleem. Bij BEC (Business Email Compromise) worden e-mailsystemen gehackt om valse betalingsinstructies of andere schadelijke acties te versturen, vaak in naam van bevoegde personen (met hoge functies) binnen het bedrijf.

Whaling of spear phishing

Hier gaat het om een “grote vangst”: men richt zich namelijk specifiek op sleutelfiguren binnen een bedrijf, zoals de CEO, hoge leidinggevenden of finance medewerkers. Meestal hebben deze personen toegang tot kritieke bedrijfsinformatie én ze beschikken ook nog eens vaak over hoge toegangsrechten.

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.

In opmars: quishing

Slachtoffers worden aangemoedigd om kwaadaardige QR-codes te scannen. Gebruik veilige QR-code scanners.

k-force
connected by ict

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