CYBER SECURITY

Do you already know these tips?

Use them in order
to work safely digitally!

Suspicious emails? Step back and check!

Is there an urgent need, are you asked to open an attachment or to log in?

If in doubt, call the sender or contact K-Force.

Help out and lock your PC

Prevent others from using your device and programs, from being able to log in with your data or perform actions.

Always lock your device when you walk away or take a break.

Apple: ^ control + ⌘ command + Q

Windows: ⊞ + L

Never give out your password

Don't trust it when someone asks you for your password by email, messenger, text message, etc.

Banks, governments agencies, Microsoft, ... never ask for a password.

Do you nevertheless still need to share passwords, e.g. with colleagues or customers? Use One Time Secret or a professional password manager.

www.onetimesecret.com

Avoid using public WiFi networks. Use 4/5 G instead!

A WiFi network without security (an access key)? Hackers can easily listen in and thus steal data.

k-force

connected by ict

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

www.k-force.be

PHISHING

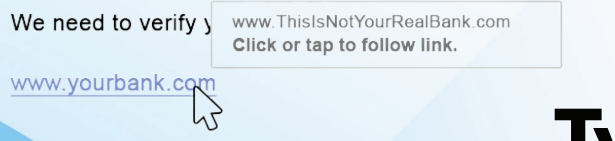
RECOGNIZE

Phishing?

Phishing involves cybercriminals impersonating a trusted source to trick victims into divulging sensitive information.

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!



We need to verify y

www.yourbank.com

www.ThisIsNotYourRealBank.com
Click or tap to follow link.

Typosquatting? Not so healthy!

Typosquatting is the use of misspelled domain names or variations 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.

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	✗

k-force

connected by ict

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

Impersonation and investigation

Attackers increasingly seek 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!

Sign in or pay

Always be extra vigilant when asked for your login credentials. Only log in if you are 100% sure that the website's URL is correct. Exercise additional caution when it comes to payments. Is the account number new, an international one, or does the payment involve a cryptocurrency wallet? This is particularly suspicious!

Received a suspicious message?

suspicious@safeonweb.be

Automated security awareness training and simulations.

↘ **www.k-force.be/en/phishing**

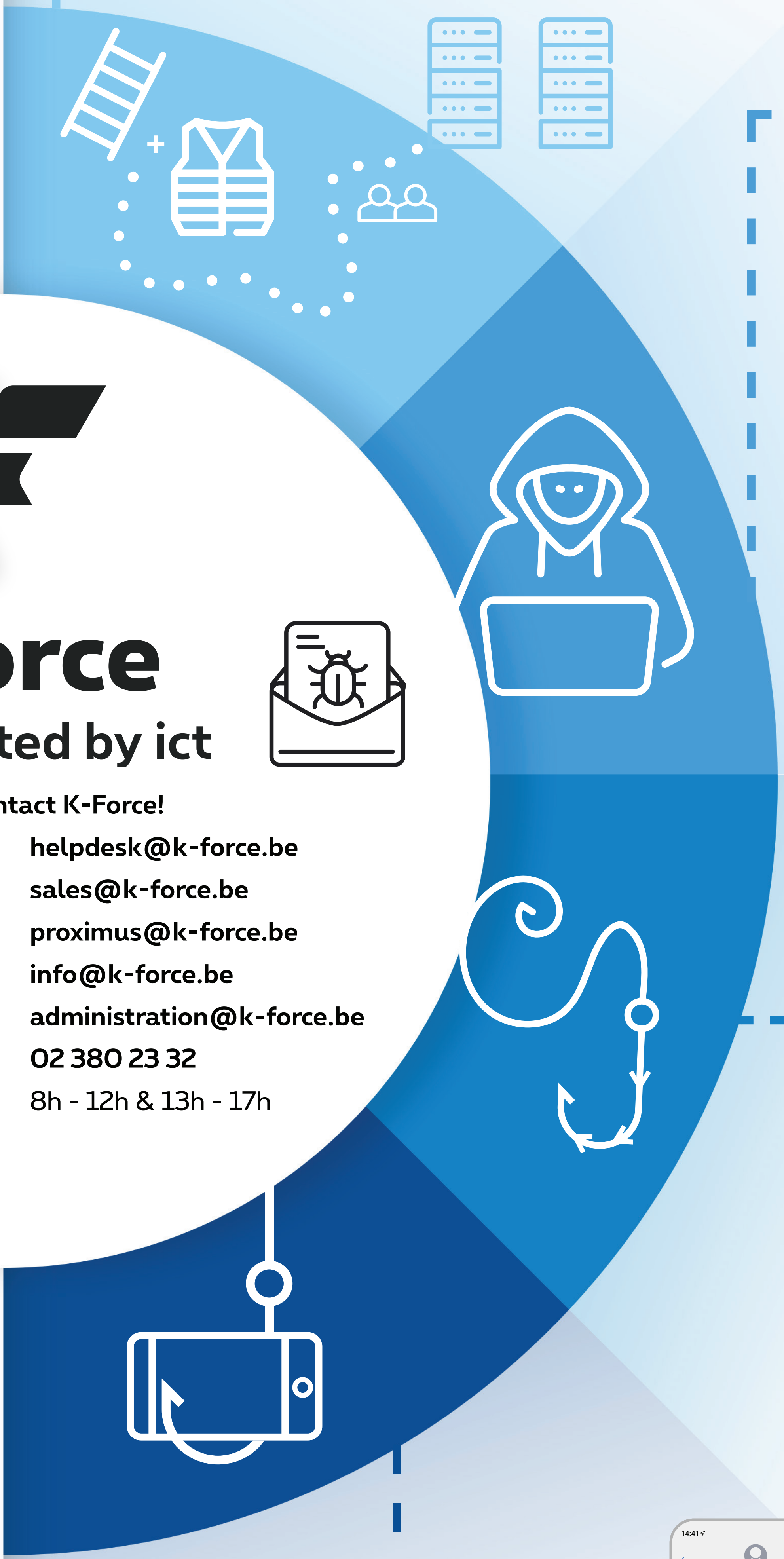
SOCIAL ENGINEERING

Social engineering

Social engineering revolves around influencing people to divulge sensitive information or perform actions that undermine security systems.

Piggybacking

An unauthorized person tries to gain physical access to restricted areas by hitchhiking with an employee. Server rooms are, of course, a highly sought-after target. A good example of this technique is the experiments where individuals, simply by wearing a security vest, can often penetrate deep into a company.



Pretexting & BEC

Pretexting involves inventing a credible story to deceive someone. A classic example is when individuals, claiming to be Microsoft technicians, pretend to ‘assist’ you with a computer problem. In Business Email Compromise (BEC), email systems are hacked to send false payment instructions or other harmful actions. This is often done in the name of authorized individuals (in high positions) within the company, such as general managers, HR, payroll, administration, etc.

Whaling or spear phishing

This term refers to a “big catch”: the aim is to specifically target key individuals within a company, including the CEO, top executives, or finance employees. Typically, these individuals have access to the most critical business information and often hold the highest level of access rights.

Vishing & 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.

On the rise: quishing

Victims are encouraged to scan malicious QR codes. Use secure QR code scanners.

k-force
connected by ict

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