Ransomware

Your computer, mobile devices or digital files have been locked and you have to pay a ransom to get them back.

What to do?

- Disconnect the device from the Internet (Wi-Fi orinternet cable).
- Immediately disconnect all other accessories, such as an external hard drives or a USB drives.
- If your device is completely blocked and you have to pay a ransom, check www. nomoreransom. org to see whether the key to this ransomware is available.
- Perform a clean install of your device and use a backup or copy to restore your data afterwards.
- Do not pay: you have no guarantee that you will actually get your data back safely.

How to prevent this?

- Use anti-ransomware software.
- Perform updates regularly.
- Scan your computer regularly with anti-virus software.
- Learn to recognise fake messages (phishing).

Help fraud and friendship fraud

Someone you know or someone you met online is asking for money.

What to do?

- Contact the family member or acquaintance via a different channel to find out if the request for help is really coming from them.
- Do not transfer money to people you have met online or family members who 'suddenly' have a different account number.
- Break off all contact with the fraudster.

How to prevent this?

- Ignore friendship requests from strangers.
- Do not share sexually explicit photos or videos.

Phishing

Phishing is online fraud using fake e-mails, websites or messages. Cybercriminals will try to gain your trust and abuse it. They will try to use your emotions, such as desire and fear, against you.

What to do?

- If you have given them a password that you also use elsewhere, change this password immediately.
- If you have clicked on a link that directs to a website where you have to submit your bank details, first check that this your bank's actual website. If there is the slightest doubt, do not proceed with the payment.
- If you have downloaded something, delete it and run an anti-virus scan.

How to prevent this?

- Learn to recognise suspicious messages.
- Think twice before clicking
- Only download applications from an official app store

Hacked accounts

Accounts are hacked when hackers have gained access to the login credentials to an online account. The hacker can post messages in your name or contact your contacts.

What to do?

- Do you still have access to your account? Change your password (also in other accounts where you use the same password) and notify your contacts.
- You no longer have access? Use the recovery options to regain access and then change all your passwords.

How to prevent this?

- Activate two-step verification.
- Use a different (strong) password for each account and store it in a password manager.
- Never share your passwords with others.

Tech Scam

You get a call on your landline from someone who pretends to be an employee of an IT company (usually Microsoft, Apple or your company's IT department). The scammer will say there is a security problem with your computer and will offer to help.

How to prevent this?

- Always distrust telephone calls from companies that ask you to do something on your computer.
- Never let someone you don't know take over your computer.
- Do not make payments while an unknown person has taken over the computer.

CEO fraud

CEO fraud is a type of scam where cybercriminals contact a company and ask it to make a payment. The cybercriminals take on the identity of the CEO, CFO or a trusted person and ask someone from finance or accounting to make an urgent payment.

How to prevent this?

- Inform employees properly and warn them about this practice.
- The accounting department should use clear procedures and agreements for payments.

Sextortion scam

You get an e-mail from scammers claiming that they have hacked into your computer and have taken intimate pictures of you. The blackmailers threaten to put the images online unless you pay them.

What to do?

- Do not respond to the request to pay a sum of money.
- Delete the message.
- Mark the message as spam or unwanted.
- Block the sender.

Who to contact after a cyber-attack or online scam?

Police

If you have lost money or are being extorted, we recommend reporting this to the police. You can file a report with the local police where you live.

It is important to bring along as much information as possible when going to the police station. Below is a list of the information you should collect in advance:

- Has money disappeared from your account? Take the bank statements with you.
- Have you been in contact with anyone on social media? Include a screen shot of the suspect's profile and some screen shots of conversations that have taken place.
- Have you opened a fake website similar to that of your bank or other institution, for example? Make a screen print and take it with you when you go in to make your statement.
- Have you been scammed via an online sales site? Take a screenshot of the ad or offer you responded to, and a screenshot of the scammer's profile.
- Have you received an e-mail from the scammer? Save and print the message.

Your bank and Cardstop

Contact your bank and call Cardstop on 070 344 344 if you have passed on bank details, money has disappeared from your bank account or if you have transferred money to a scammer.

This allows for fraudulent transactions to be blocked.
If you want to report fraud, you can contact your bank by calling a special number https://beschermjezelfonline.be/bank-contacteren-for-help

Safeonweb

Have you received a suspicious e-mail or message?

Forward the message to suspicious@safeonweb.be and then delete it.
You will not get a personal reply. The links in the message will be blocked, to make sure less attentive Internet users do not fall victim to the fraud. If you receive a suspicious message at work, you should follow the relevant procedures for phishing, e.g. by forwarding the message to your IT department.

Reporting

Are you a victim of deception, fraud or a scam?

Then report it via https://meldpunt.belgie.be of the FPS Economy.
You will always get a recommendation after submitting your report. The competent services will analyse the report and may launch an investigation.

Centre for Cybersecurity Belgium

If your organisation is facing a cyber-attack or is the victim of a ransomware attack and would like to report it or get advice in complete confidence, you can contact CERT.be, the Federal Cyber Emergency Response Team of the CCB via https://www.cert.be

CENTRE FOR CYBER SECURITY BELGIUM

Safeonweb.be

.be

Cyber-attacks and online scams

What are they, what to do and how to prevent them?

Safeonweb.be