Safeonweb.be

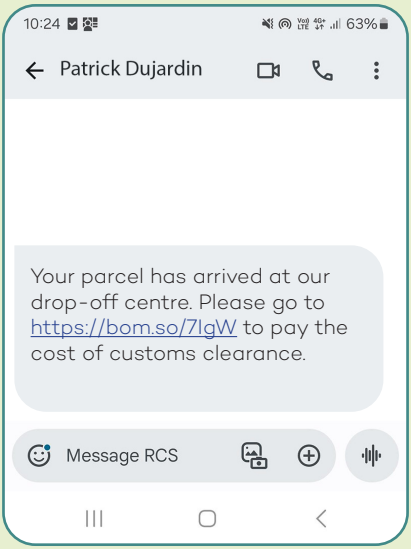
# ONLINE SCAMS: HOW TO SPOT THEM, HOW TO PREVENT THEM AND HOW TO RESPOND ?

**Visit safeonweb.be/en for more information and other scams**

CENTRE FOR CYBERSECURITY BELGIUM

.be

## Phishing



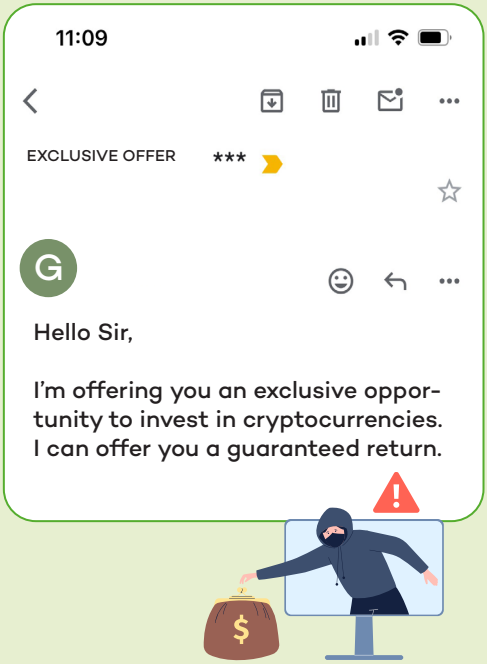

**Phishing is a form of online fraud that uses fake e-mails, websites, mobile phone text (SMS) messages, QR codes and so on to obtain your personal information.**

- Think before you click, offers can be misleading.
- Never disclose any passwords, bank card codes or Digipass (card reader) response codes in an e-mail, phone call or text message or on social media.
- Check the sender's address and the URLs of the links you are being referred to.
- Learn how to identify suspicious messages at surfwithoutworries.safeonweb.be.

## Investment fraud

**You may be contacted by phone or e-mail (or via a friend's hacked account) by a so-called investment company offering to buy shares or other financial products. Or you may see a fake advertisement with a celebrity endorsing these investments.**

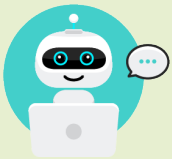
- Be wary of unsolicited financial proposals and be critical of offers.
- Check the identity of the service provider, even if it appears to be a reliable company: name, registered office, contact details.



## PC problems (tech scams)

- Beware of phone calls from companies asking you to perform a series of actions on your computer.

> I'm Mark from the Microsoft helpdesk. Your computer has a security problem. I'll help you by taking control of your computer.



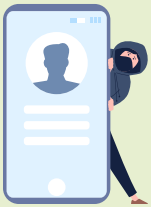
- If a pop-up appears saying that your computer is locked, don't call the number given. Run a virus scan.
- Never install any apps or software suggested by the 'helpdesk'. It could take control of your device.

## Identity theft/ account hacking

> "Strange things are happening to my account: I seem to have sent messages to my friends without my knowledge, and messages and photos are appearing on my page even though I haven't posted anything."

**Your account has probably been hacked.**

- Do you still have access to the account? If so, change the password on that account and all your other accounts immediately and notify your contacts.
- You don't have access to your account anymore? Use the account recovery options ('Forgotten your password?' option) to regain access and then change all your passwords.
- Enable two-factor authentication. The first step is to log in to your account with your password. In the second step, the account sends a code to your mobile phone that you need to enter to access to your account.
- Use a different (strong) password for each account and store the passwords in a password manager. It's an online safe where you can store your passwords by account, protected by a password.



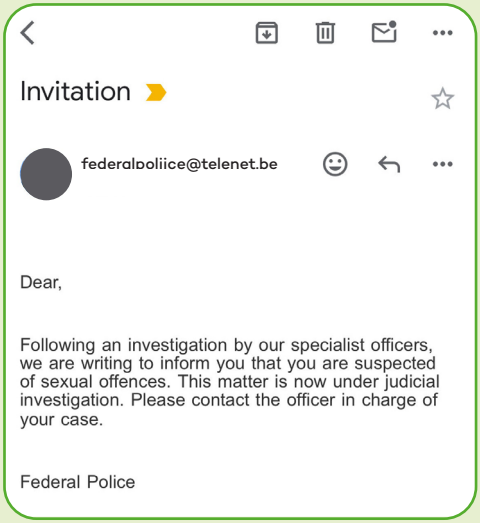
## Scam on an online sales platform

**This type of scam targets buyers or sellers on online sales platforms. It may involve fake buyers or sellers or even fake websites.**

Hello. Is this item still available? I'd like to offer you €500 for your table. I can't come and collect it, so a DPD driver will pick it up. I'll pay you by bank transfer.

- Beware of overly quick responses and bids above the asking price. Check out the profile of the buyer/seller.
- Always continue your conversations with buyers/sellers on the online second-hand platform and not, for example, via text message or on WhatsApp.
- Never pay through a link sent to you by a buyer or seller. These links will take you to a fake website where scammers will ask for your bank details.
- Never enter your personal details on a shipping site using a link provided by the buyer/seller.

## Message supposedly coming from the police




**This is an e-mail scam that focuses on the urgency and seriousness of the alleged crimes.**

- Never respond to a message of this type and don't give in to demands for money.
- Block the sender.
- Look up the contact details of the organisation that is meant to have sent this e-mail to get in touch with them.

## Online security checklist

- Never give out passwords, credit card codes or answer codes by e-mail, phone call, SMS or social media.
- Protect your mailbox and social network accounts with two-factor authentification.
- Install updates as soon as they appear.
- Install antivirus software on your computer, if you have not already done so.
- Back up your files on the cloud or an external hard drive.

## It's too late – you're already been scammed? What should you do?

Have you given your bank details, noticed fraudulent withdrawals from your account or transferred money to a scammer?

- Call Card Stop on 078 170 170 (+32 78 170 170 from abroad) to block access to your accounts.
- Contact your bank. The sooner you notify the bank, the better the chances of recovering your money.
- File a report with the local police. Provide as much information as possible: account statements, screenshots of the fraudulent message or website, profile of and conversations with the suspect, any installed apps, etc.

# TOOLS TO PROTECT YOURSELF

## HAVE YOU RECEIVED A SUSPICIOUS E-MAIL OR MESSAGE?

Forward the message to suspicious@safeonweb.be and then delete it. Suspicious attachments and links will be checked automatically. Any internet user who inadvertently clicks on this link will receive a clear warning advising them not to go to this page.

## INSTALL THE SAFEONWEB BROWSER EXTENSION

The Safeonweb browser extension warns you when you are visiting an unsafe website and when it is dangerous to enter your data. A colour code (in the toolbar) tells you whether a site is trustworthy or not. Watch a video on how to install it at safeonweb.be.

## WATCH OUR 'SURF WITHOUT WORRIES' SERIES OF E-LEARNING VIDEOS

Learn how to spot scams and suspicious messages by watching our e-learning videos at surfwithoutworries.safeonweb.be.

## DOWNLOAD THE SAFEONWEB APP

The Safeonweb app informs you about the current threats in Belgium and gives you advice on how to improve your online security.
It is available free of charge for iOS in the App Store and for Android in the Google Play Store.

## MORE INFORMATION

- safeonweb.be/en
- surfwithoutworries.safeonweb.be/en/modules

**Follow Safeonweb on**