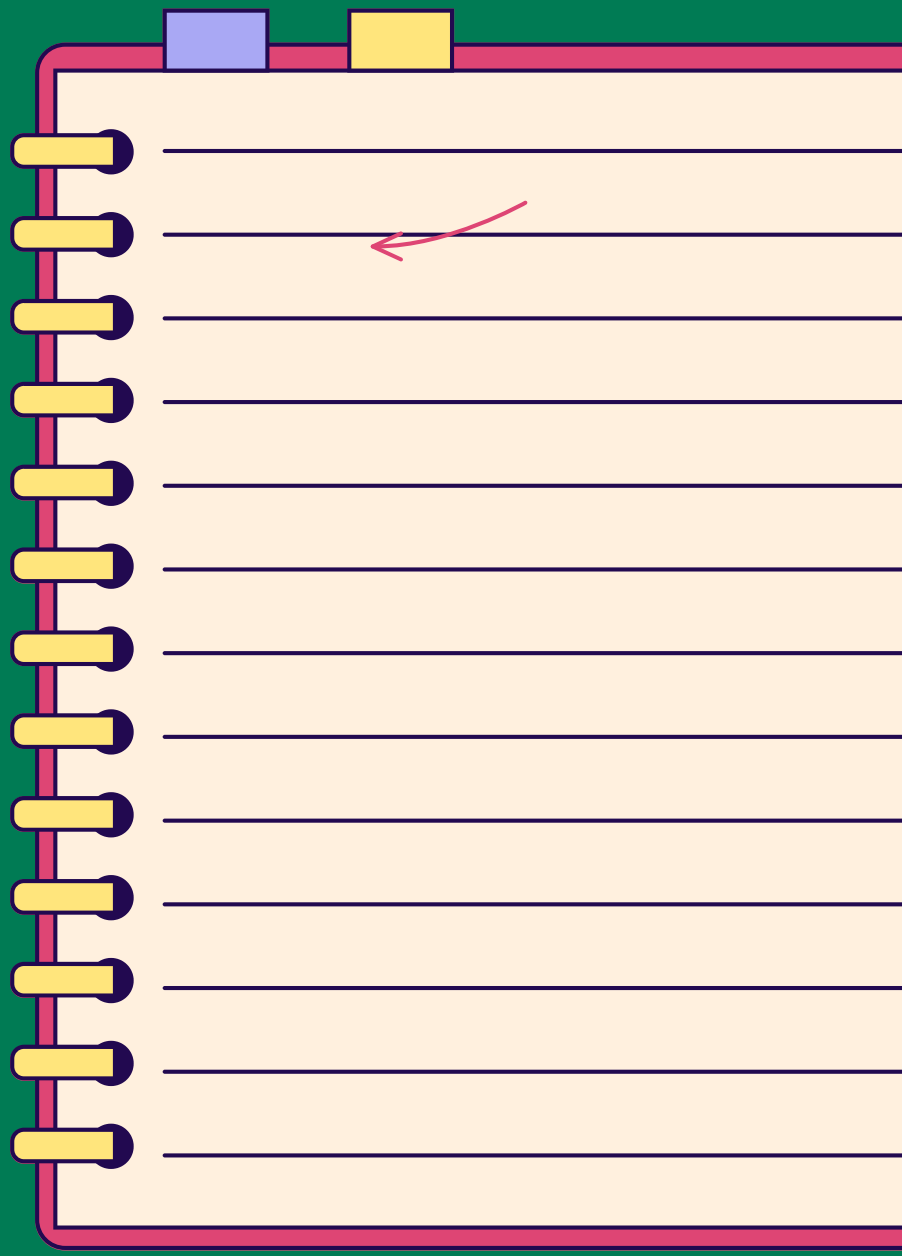
MODULE 12 - ONLINE SCAMS

# CHAPTER 3

## HOW TO REACT TO SCAMS

Skills to Connect



# INTRODUCTION

In this chapter, you'll learn how to respond to various online scam situations, whether it's clicking on a fraudulent link, being a victim of spoofing, or purchasing fraud. We'll walk you through the actions you can take immediately to secure your accounts, report the incident, and avoid further negative consequences.
You will also learn about official sites to report scams in different countries and best practices to adopt to protect your personal information in the future.

# 1 HOW TO REACT TO SCAMS

## WHAT TO DO WHEN YOU CLICK ON A FRAUDULENT LINK

### YOU CLICKED ON A FRAUDULENT LINK AFTER A PHISHING ATTEMPT: WHAT TO DO NEXT?

#### 1 - DO NOT ENTER ANY DATA

- If you enter your credentials on a fake site, you give the cybercriminal direct access to your real account. Once logged in, he or she can use your account for malicious purposes. **The situation becomes even more serious if you reuse the same password on multiple accounts, as this will allow him or her to access those other accounts as well.**

#### 2 - DON'T CLICK ON ANYTHING

- If you land on a suspicious site, do not click on any links, as they may contain viruses waiting to be activated. Also avoid clicking on advertisements: they may contain malware, a phenomenon called “malvertising”. Even a simple click can trigger the installation of a harmful program on your device.

#### 3 - DISCONNECT FROM THE INTERNET & CHANGE YOUR PASSWORDS

- Cutting off your internet connection can help block the cybercriminal from remotely accessing your device. It also limits the spread of malware to other devices connected to your Wi-Fi network. Disconnecting your device quickly can significantly reduce the risk of damage.
- Once your device is disconnected, use another trusted device (like another computer, tablet, or smartphone) to change your passwords
  - Connect to a secure network: Avoid public Wi-Fi networks. Use your home network or share a smartphone's Internet connection ("tethering" or "mobile hotspot" mode).
  - Access important sites like your email, bank accounts, or social networks.
  - Click on "Forgot your password?" if you have difficulty logging in. This will allow you to reset your password by following the instructions sent by email or SMS.

# 1 HOW TO REACT TO SCAMS

## WHAT TO DO WHEN YOU CLICK ON A FRAUDULENT LINK

### 4 - PERFORM A FULL SCAN WITH AN ANTIVIRUS:

- Once disconnected, it is important to scan your device with antivirus software. If you do not already have one installed, do so immediately. The antivirus will scan your device to detect and remove viruses or malware before they cause significant damage. To do this:
  - Open your antivirus installed on your device.
  - Choose the "Full Scan" or "Complete Scan" option. This allows the antivirus to examine all files on your computer, including sensitive areas where viruses often hide.
  - Once the scan is complete, follow the antivirus recommendations: delete or quarantine the detected threats.
  - After scanning, reconnect only if your device is clean (no threats detected).
  - Once online, update your antivirus so that it has the latest protections against new threats. Then, run a new scan to verify that everything is secure.

### 5 - MONITOR YOUR ACCOUNTS:

- Even after taking these precautions, stay vigilant by regularly monitoring your accounts to identify suspicious activity. The cybercriminal may have had time to retrieve sensitive information. Check your bank statements carefully for transactions you didn’t make, as well as unusual logins or unauthorized changes to your online accounts.

# 2 HOW TO REACT TO SCAMS

## WHAT TO DO WHEN YOU ARE A VICTIM OF SPOOFING

### SOMEONE PRETENDED TO BE YOUR BANKER AND STOLE YOUR MONEY: WHAT TO DO NEXT?

#### 1 - CONTACT YOUR BANK IMMEDIATELY

- Call your bank using the official number (the one on your bank card or on the official website). Explain what happened and ask:
  - Block your bank cards if you have given your numbers,
  - Check your accounts to block any suspicious transactions,
  - Change access to your online accounts to prevent the scammer from logging in.

#### 2 - CHANGE YOUR PASSWORDS

- Immediately change your passwords for all your sensitive accounts, especially:
  - Your online banking accounts,
  - Your email box (because often used to recover passwords),
  - Your accounts on other services (social networks, shopping sites) if you reuse the same password.

# 2 HOW TO REACT TO SCAMS

## WHAT TO DO WHEN YOU ARE A VICTIM OF SPOOFING

### 3 - MONITOR YOUR BANK ACCOUNTS

- Check your bank statements and online transactions to spot payments or transfers you didn't make.
  - Enable SMS or email notifications to be alerted as soon as a transaction takes place.
  - If you see any suspicious transactions, report them to your bank immediately.

### 4 - FILE A COMPLAINT

- Go to the police station to file a complaint. Bring all possible evidence: the number that contacted you, messages, emails or screenshots related to the scam.
- You can also report the scam online on dedicated platforms:
  - In France: report it via the Pharos platform
  - In Belgium: report a problem on Safeonweb.be
  - In Portugal: file a complaint with the Public Security Police (https://www.policiajudiciaria.pt/queixa-eletronica/) or the Office for Combating Cybercrime (https://cibercrime.ministeriopublico.pt/pagina/denuncia-0)

see chapter 4

# 3 HOW TO REACT TO SCAMS

## WHAT TO DO IF YOU ARE A VICTIM OF PURCHASING FRAUD

### YOU MADE A PURCHASE ON A FRAUDULENT SITE: WHAT TO DO NEXT?

#### 1 - CONTACT YOUR BANK OR CARD PROVIDER IMMEDIATELY

- If you paid by credit card or other payment method, contact your bank or card provider immediately. Explain the situation and ask:
  - Cancel the transaction if possible,
  - Block your card to avoid further fraudulent payments,
  - Check other recent transactions for unauthorized payments.

#### 2. CHANGE YOUR PASSWORDS

- If you entered sensitive information (such as your password or banking details) on the fraudulent site, change the passwords for your online banking accounts, email, and any other accounts used with that password.

# 3 HOW TO REACT TO SCAMS

## WHAT TO DO IF YOU ARE A VICTIM OF PURCHASING FRAUD

### 3 - MONITOR YOUR ACCOUNTS

- Check your bank statements and watch for any suspicious activity, especially if unauthorized transactions are taking place.
- Activate SMS or email alerts from your bank to be informed in real time of any activity on your accounts.
- Also check your online accounts (Amazon, PayPal, etc.) to ensure no information has been used fraudulently.

### 4 - REPORT THE FRAUDULENT SITE

- File a complaint with your local police or online.
- You can also report the scam online on dedicated platforms:
  - In France: report it via the Pharos platform
  - In Belgium: report a problem on Safeonweb.be
  - In Portugal: report on https://queixaselectronicas.mai.gov.pt/

see chapter 4

You can also report the fraudulent site to consumer organizations

- Trustpilot
- Signal-Scams
- ScamDoc

see chapter 1

# 4 WHAT TO DO IF YOU SPOT A SCAM?

## REPORTING AND PREVENTION PLATFORMS

### BELGIUM

- Cybersimple.be: This platform offers advice on preventing online scams, provides information on common types of fraud and reports cybersecurity incidents.
- Safe On Web: Official platform for reporting scams and cybersecurity incidents. It also provides recommendations for protecting yourself from digital risks.

### FRANCE

- Thesee: Official platform of the Ministry of the Interior for reporting online scams (phishing, bank fraud, etc.). It also allows you to file complaints.
- Cybermalveillance: Platform for reporting cyberattacks and getting help with cybersecurity incidents. This site offers advice and resources for victims.
- Pharos: Official platform for reporting illegal online content (scams, phishing, cybercrime). It allows you to report online fraud to the relevant authorities.

# 4 WHAT TO DO IF YOU SPOT A SCAM?

## REPORTING AND PREVENTION PLATFORMS

### PORTUGAL

- Seguranet: Portuguese government website providing information on reporting online fraud and tips on protecting yourself against cyberattacks and phishing.
- Violencia: A site to report criminal behavior online, including scams, abuse, and fraud. It also provides safety tips.

### EUROPEAN UNION

- EU Site - Victims' Rights: This European site provides information on the rights of victims of crime across the EU, including how to report fraud and cross-border crime.

# TO REMEMBER

If you fall victim to an online scam, act quickly by changing your passwords, contacting your bank, and reporting the incident to the appropriate authorities. It’s crucial to not click on new links and disconnect your device from the wifi to prevent the spread of malware. By regularly monitoring your accounts and using security tools like antivirus and two-factor authentication, you can limitate your risks and protect your personal information. Finally, stay vigilant against future scam attempts by learning to recognize the signs of a scam.