MEMORY SHEET
Online scams

INTRODUCTION

Online scams: spot, avoid, act

Online scams are becoming more and more sophisticated and difficult to spot

- Learn how to recognize the most common scams, how to spot them using distinctive signs, and adopt best practices for browsing safely.

SUMMARY

1) Recognize the main scams
2) Signs to look out for
3) Protect yourself
4) Stay safe while online shopping
5) How to react to a scam?

Skills to Connect

1 Recognize the main scams

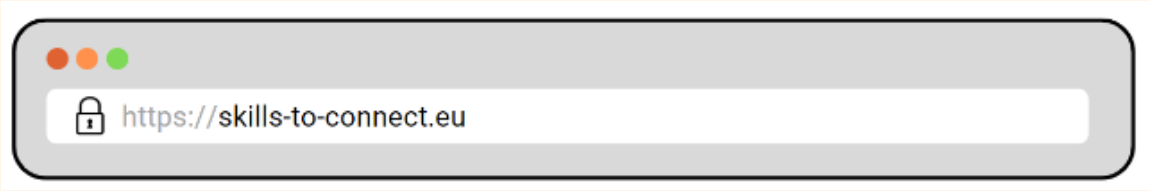
Here are the most common scams:

- **Phishing:** a fake email or SMS tricks you into clicking on a link to steal your information (password, card number, etc.).
- **Spoofing (identity theft):** a fake bank advisor or police officer calls or writes to you.
- **Purchase fraud:** you order an item from a site that will never ship anything.
- **Triangular fraud:** you buy a stolen product without knowing it.

2 Signs to look out for

- **Always check:**

1.
   - The website address must always start with :
   - the designation: https://
   - A lock 
   - ✅ **Secure site:**



   - 🚫 **Unsecured site**

2.
   - The appearance of the message

3.
   - Sender's email address or number:

Do you know this email address or the sender?

2 Signs to look out for

- Here are the signs of a fraudulent message:

Be wary if:

- You are put under pressure: “Your account will be blocked within 24 hours!”
- You are given a gift or a big unexpected discount
- You are asked for your codes, password or card number
- The message is written strangely:

Use of two languages

Using special characters

Spelling or syntax errors

🚫 Additional signs to look out for :

Fake logos like this :

The real Google logo looks like this:

Google

Emergency message:

Plays on emotions, stress and a sense of urgency to push you into **action without thinking**

GOOGLE MAIL NOTICE

This is a reminder that your email account will be locked out in 24hours

Due to not being able to increase your Email storage Quota

Go to the INSTANT INCREASE to increase your Email storage automatically INSTANT INCREASE

==========

Sincerely Gmail Team,

Copyright ©2014 Gmail. All rights reserved.

A fraudulent link is hidden behind the button

3 Protect yourself

Some reflexes to have:

- **Protect your devices:** Install antivirus software on your devices (computers and tablets). Update your devices.

- **Protect your accounts:** use strong and different passwords, activate two-factor authentication.

- **Limit the information shared:**

Do not give your personal data on any site and make sure that the site is secure and reliable (see points 4 and 5).

Never send your card number, PIN or any other banking information to anyone by email.

4 Safe online shopping

- Four tips:

1. **Buy from trusted sources:** Choose brands and stores you're familiar with or have shopped at before, and check private sellers' ratings on sites like Amazon or eBay.

2. **If you buy something online from an individual on a resale site** (Facebook Marketplace, Ebay, gumtree, etc.): Do not send the money directly to the seller: offer to give it in person or ask to receive the item before paying.

3. **Don't send money to someone you don't know:** If someone approaches you online and asks for money, ask yourself if you would give the same thing to a stranger on the street.

4. **Avoid using online shopping sites that do not require full authentication and always save documents related to your online purchases:** They can be used as proof if you do not receive the goods you paid for

5 What should I do if I am the victim of a scam or attempted scam?

📌 **When in doubt:** “I received a suspicious email asking me to click on a link and send my details or call them.”

If I receive a suspicious message:

1. Do not click on the link
2. Do not reply to the message
3. Do not forward the message to other people
4. Do not call the number indicated
5. Block the email in question and delete the message

📌I am the victim of a scam:

1. **Change your passwords immediately.**
2. **Contact your bank** if banking information has been shared.
3. **Report the scam:**

- In Belgium: www.safeonweb.be
- In France: www.internet-signalement.gouv.fr
- In Europe: EU Victims Site

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.

💡 Good to know

A bank advisor will never ask you for your password, PIN, or credit card number over the phone or via email. If someone asks for them, it's most likely a scam.

To access your taxes, pension, or other public services online in Belgium, you must always use the secure CSAM platform or the ITSME application. You will never receive an email asking you to click on a link to view your tax return. If you receive this type of message, do not click: it is an attempt at fraud.