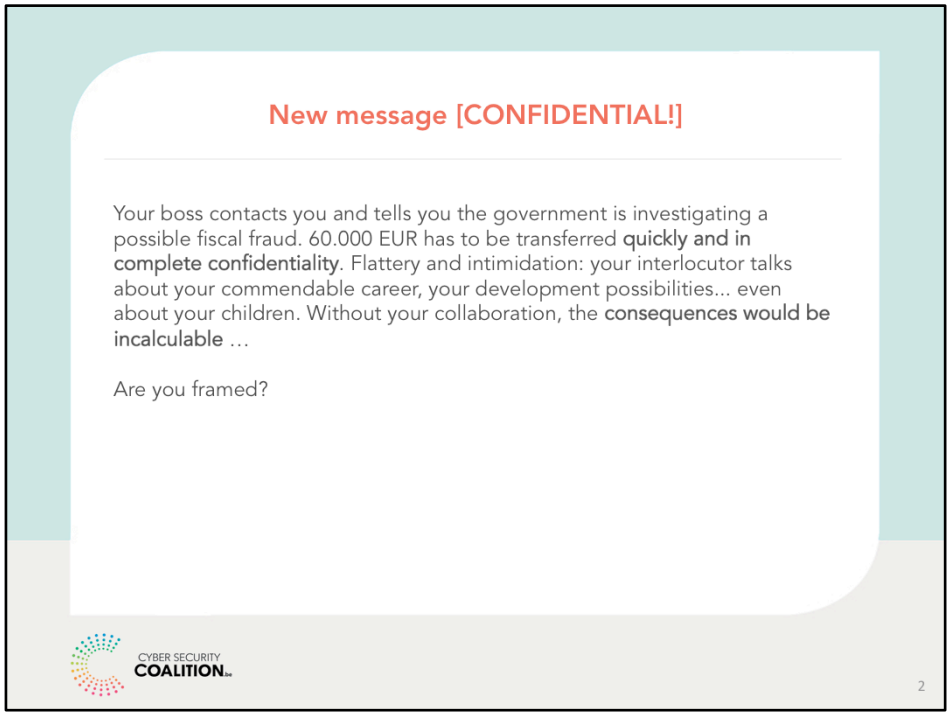
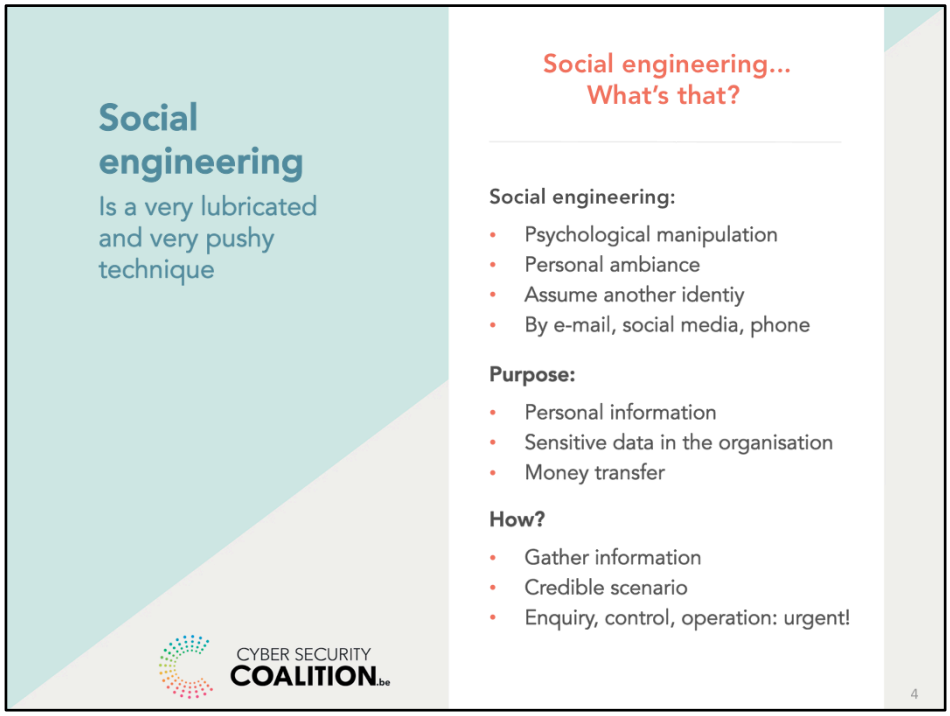
Hello and welcome everyone!



A classic scenario for social engineering with SME

Attention!

A person with bad intentions wants to abuse your trust. It is such a clean technique that we call it **'social engineering'**: the fraudster knows your profile by studying **information on you** on the web or the social networks. The purpose? Lower your watchfulness by a credible **scenario**, to get tinformation from you or to stimulate you to act.



Social engineering or **social hacking** is a fraudulous technique which consists of abusing people, by exploiting typical traits like curiosity, naivity, fear, trust, greed,…

The fraudster impersonates a **confidential person** and uses the **personal context** of the victim to break into the **network of the enterprise.**

Mostly this is done by an **e-mail, social media** or a **phonecall**.

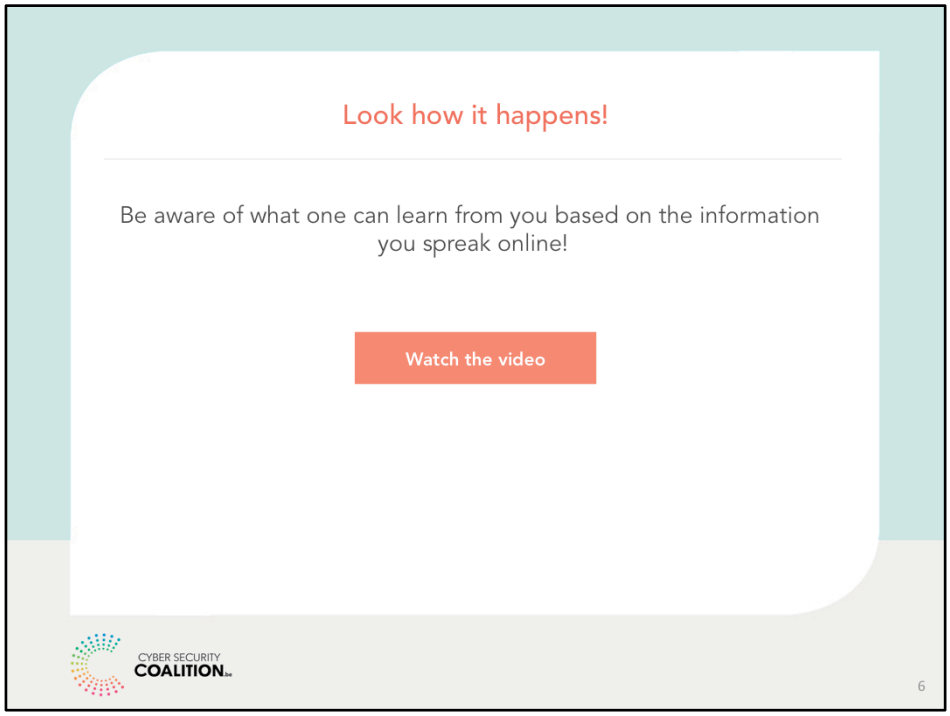
The purpose?
- Looking for **personal information** (ID, passwords, credit card number).
- Access to **sensitive data** in the organisation.
- **Money transfer**.

How?
- Accurately gathering **public and private information** (social networks), sometimes during several months.
- Make a well lubricated and **plausible scenario**.
- An **enquiry, a control, an urgent operation, an opportunity**.

In Belgium **1 in 2 enterprises** are touched by cybercriminality and techniques of social engineering.

Unbelievable! In Q1 2016, a social engineering cost **70 MIO EUR to a Belgian bank**, via so-called CEO fraud. According to Verizon (2019 Data Breach Report: https://www.helpnetsecurity.com/2019/05/09/verizon-2019-data-breach-investigations-report) managers in an organisation are targeted 10 times more then other staff members.

Globally the damage caused by this phenomenon raises up to 10 Billion EUR (Source: FBI - 2018)



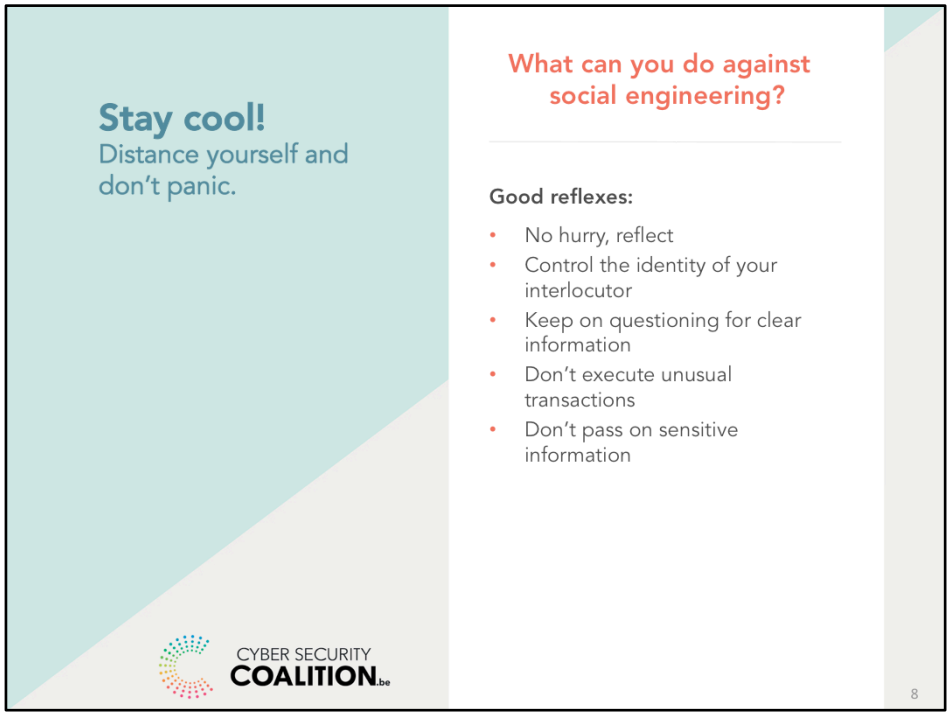
In this **video of Febelfin** (https://www.youtube.com/watch?v=F7pYHN9iC9I) you can see how a genius in social engineering operates to know 'everything' about you…

- What do you spread via social networks?
- What can one learn about you?

You won't look at the internet the way you did before…

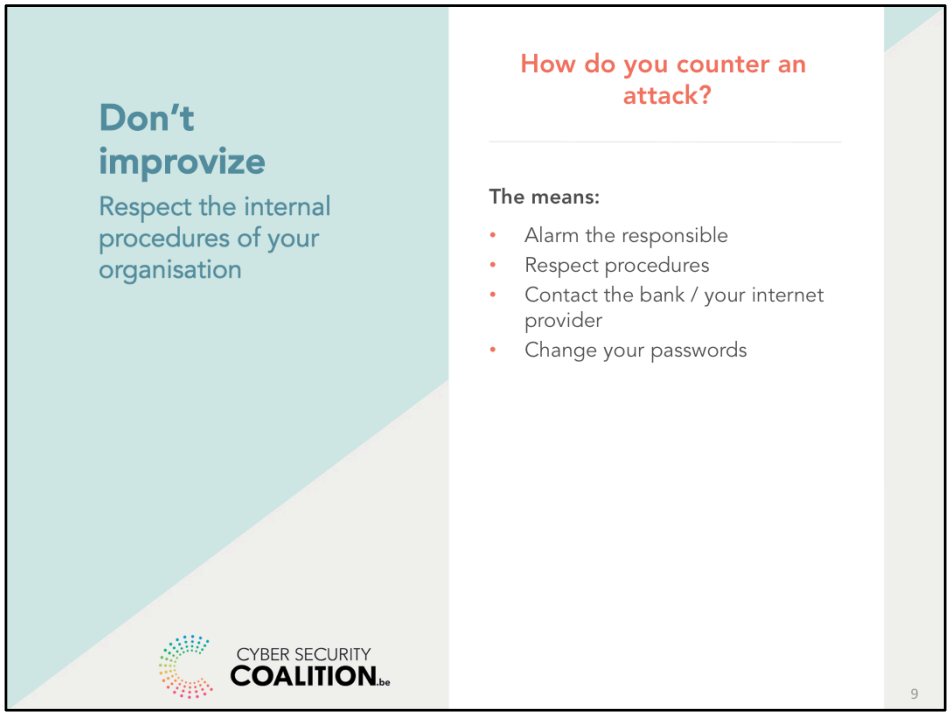
How to unmask a social engineering attack

- You **don't know your internlocutor**.
- The situation is very **critical (cf Covid-19).**
- Urgent, secret: you must **act fast** and it is **confidential**.
- Ubelievable! An offer **too good to be true**…
- The tone is extremely **intimidating or flattering.**



Take good reflexes against social engineering

- Take your **time to reflect,** don't trade in a hurry
- Control the **identy** of your interlocutor.
- Don't be satisfied with a **vague or complex explanation.**
- **Don't execute an unusual transaction** without the agreement of a third person.
- **Don't pass on sensitive or internal information**.



How to react when you are attacked?

- Alarm the **responsible** in your organisation.
- Respect **procedures** that apply in your organisation.
- Contact your **bank** immediately to check whether money has been stolen. Also contact your internet provider.
- Change your professional and private **passwords**.

Social engineering: discuss it!

What is your opinion?
What are your remarks?
What do you remember?
Your first action?

10

What is your opinion?
Do you have remarks?
What do you remember?
What will be your first action after this presentation?

Thank you for your attention!