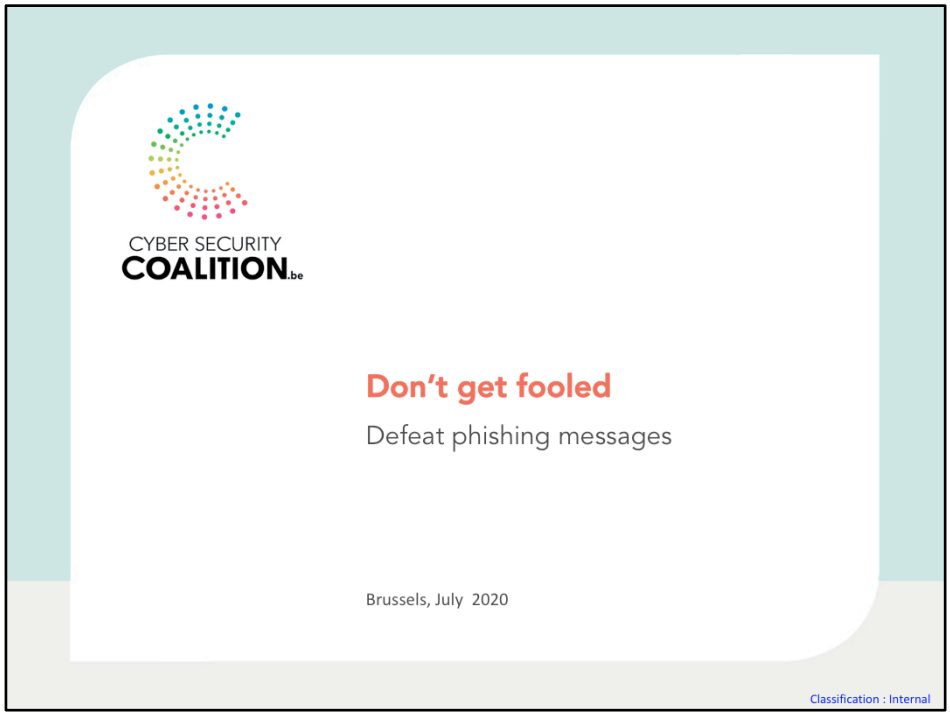
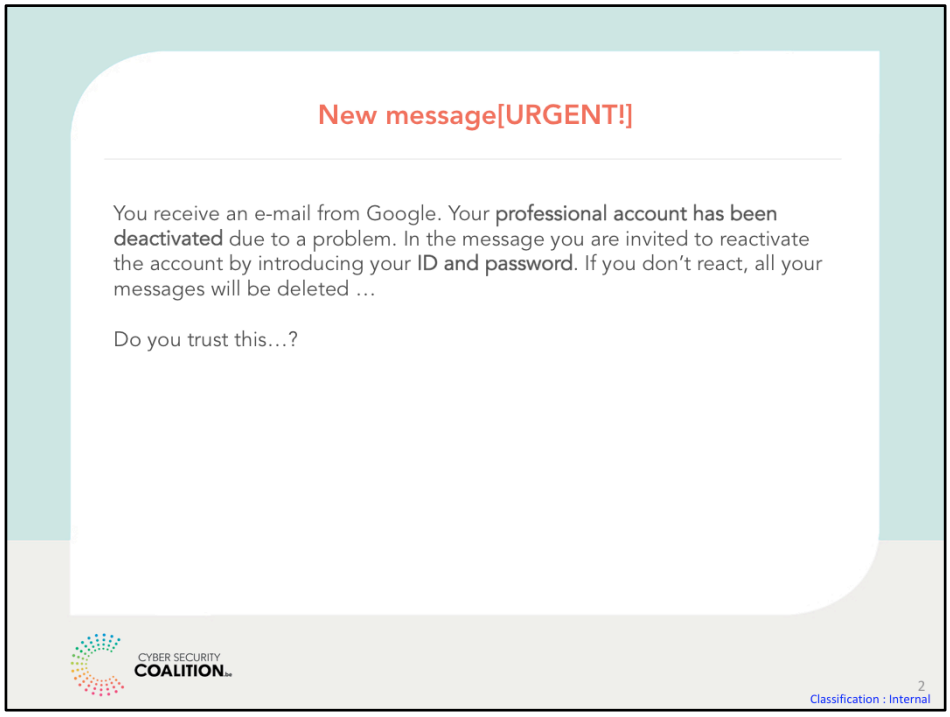
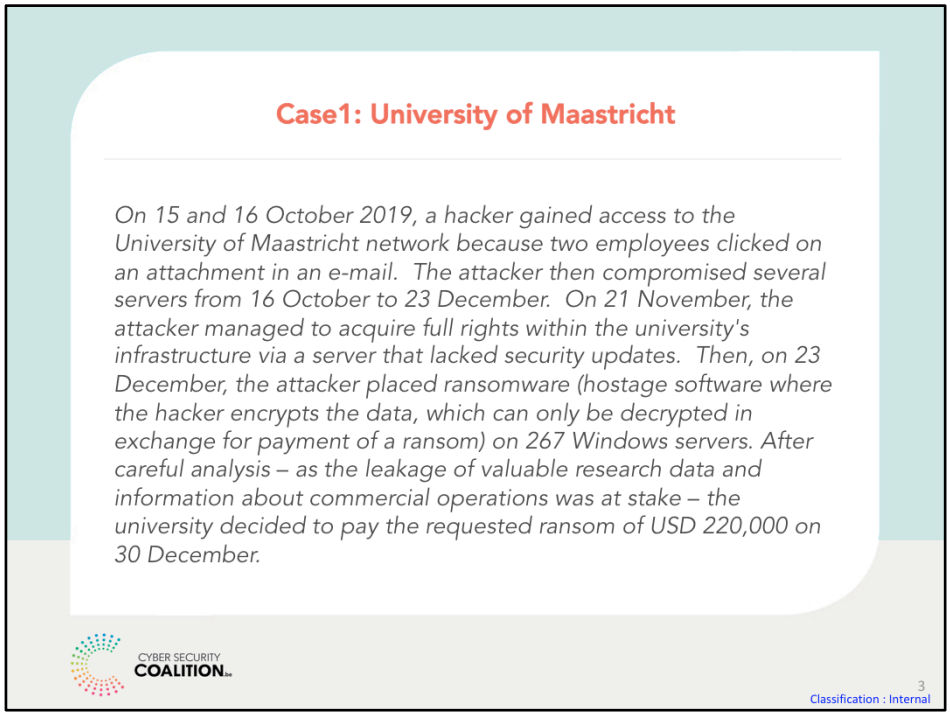



Hello and welcome everybody!



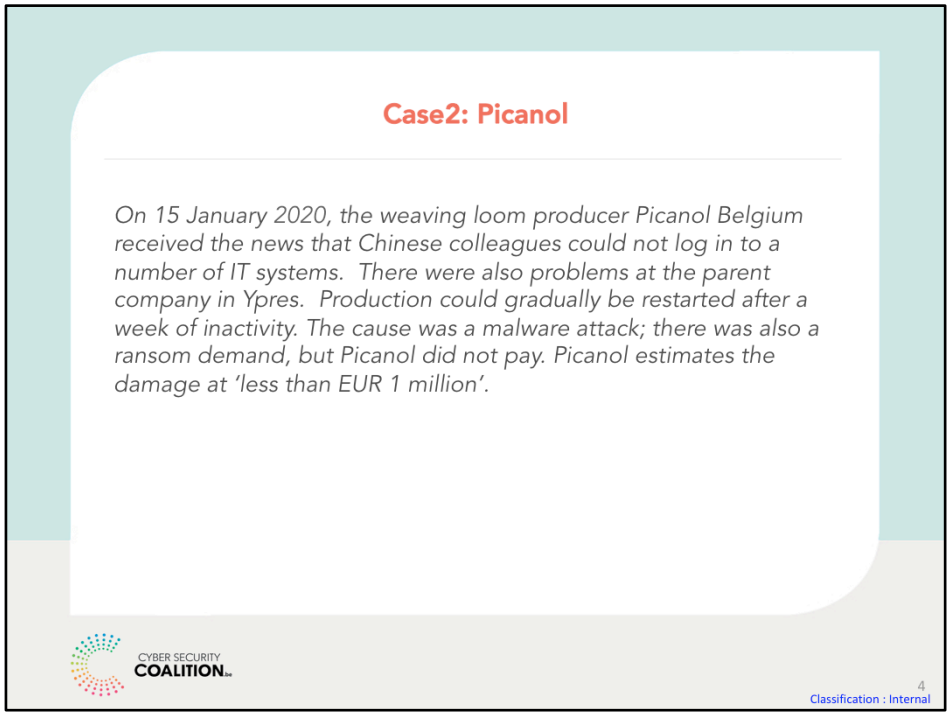

The classic phishing scenario with SME's.




The University of Maastricht case (source: FOX IT – NCC Group) shows that hackers have time, work thoroughly, and are able to stay under the radar.

This incident led to the following recommendations from the security consultants involved:

- Improve processes with regard to vulnerability and patch management
- Create more segmentation within the network architecture and user rights
- Implement or improve network and log monitoring
- Practise the different crisis scenarios regularly and improve the prepared plans where necessary




Source: VRT News (January 2020)


**Attention: phishing!**

A person with bad intentions wants to obtain information from your professional **inbox,** your confidential **files,** your **online accounts**,... Often it does not stop there and the hacker also steals information from your **social network** profile and **buys** stuff on your favourite sites.


Phishing is a fraudulous technique where the **identity of a person or organisation is stolen.**

The fraudster makes his victim believe that he / she is a **trustworthy party** – a bank, an administration, a personal contact person – to obtain **personal or professional information.**

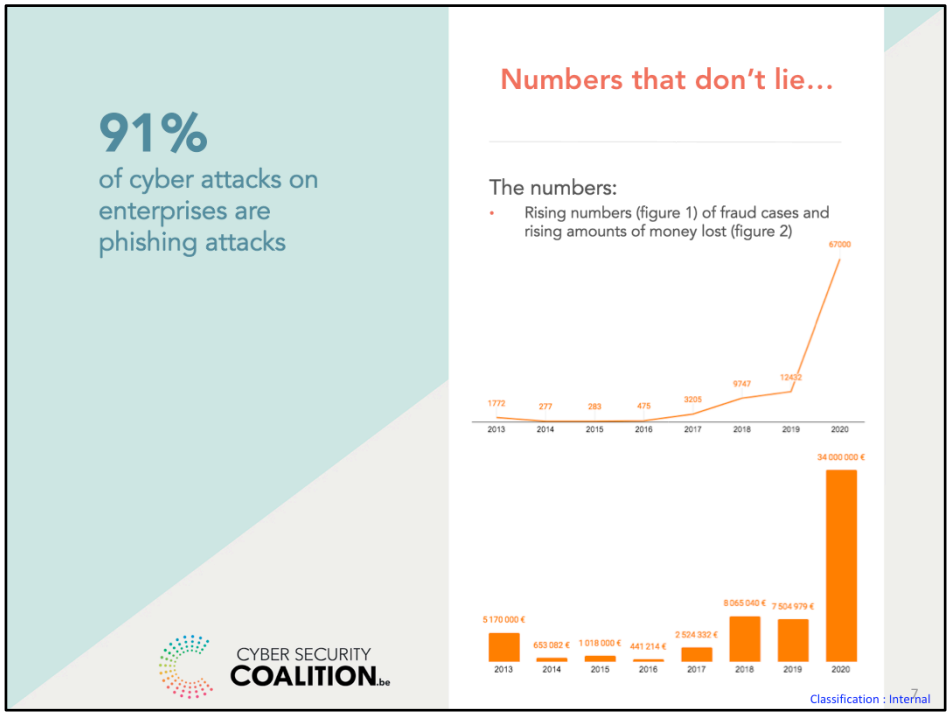
This usually happens via **e-mail, SMS (Smishing), WhatsApp, Messenger. Also via phone (Vishing, V=voice)**

**What's the purpose?**

- Collect **personal information** (ID, password, credit card number).
- Get access to **sensitive data in the enterprise**.
- Obtain a **money transfer**.
- Industrial **sabotage.**

**How?**

- An **infected attachment** which installs a virus.
- A link which forwards you to a **false website**.
- A **false payment system**.



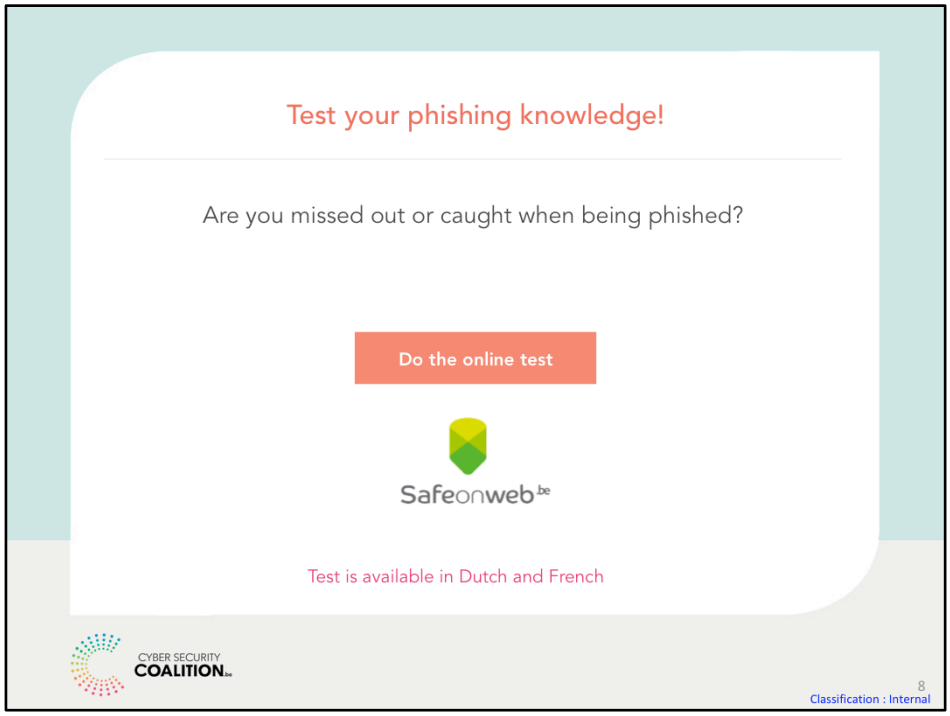

Phishing represents nowadays **91% of all cyber attacks** against enterprises and SME (Cert – 2015)

Unizo (**Uni**e **Z**elfstandige **O**ndernemers in Flanders) states (2016) that 1 enterprise on 5 has been victim of this type of fraude in Belgium.

Number of cases of fraud and financial losses in the financial sector in Belgium (source: Febelfin – March 2020): the number of successful fraud cases via phishing increased by 27.5% in 2019 (12,432) compared to 2018 (9,747). The cost of these fraud cases for Belgian financial institutions appears to have stabilised in 2019 (EUR 7.5 million) compared to 2018 (EUR 8 million). A calculation shows that cyber criminals obtained an average of EUR 604 per victim in 2019. Only small amounts are involved in the vast majority of cases, but large sums of money are also sometimes taken. Unfortunately, the figures increased significantly again in early 2020 (Covid-19).

Thanks to significant amounts of help from the Belgian population, the Centre for Cybersecurity Belgium (CCB) was able to block an average of **four fraudulent websites a day** in 2018. A total of **1,478 fake websites were blocked**.

The Belgian population forwarded **648,522 e-mails** to verdacht@safeonweb.be in 2018. The forwarded e-mails are automatically scanned by the BeFish software. In a first phase, the messages with URLs are identified. The anti-virus technology then detects any suspicious links in these e-mails, which are forwarded to the *EU Phishing Initiative*. The latter can then block phishing websites through a collaboration with four browsers: Google Chrome, Mozilla Firefox, Safari and




Link to the test: https://www.safeonweb.be/en/quiz/phishing-test
(Dutch or French)

In this **(anonymous) test** you wil see **10 e-mails** which are sent by real enterprises and organisations and by fraudsters.

- Can you **unmask** the phishing-e-mails?
- Challenge your colleagues: who gets the **best score**?

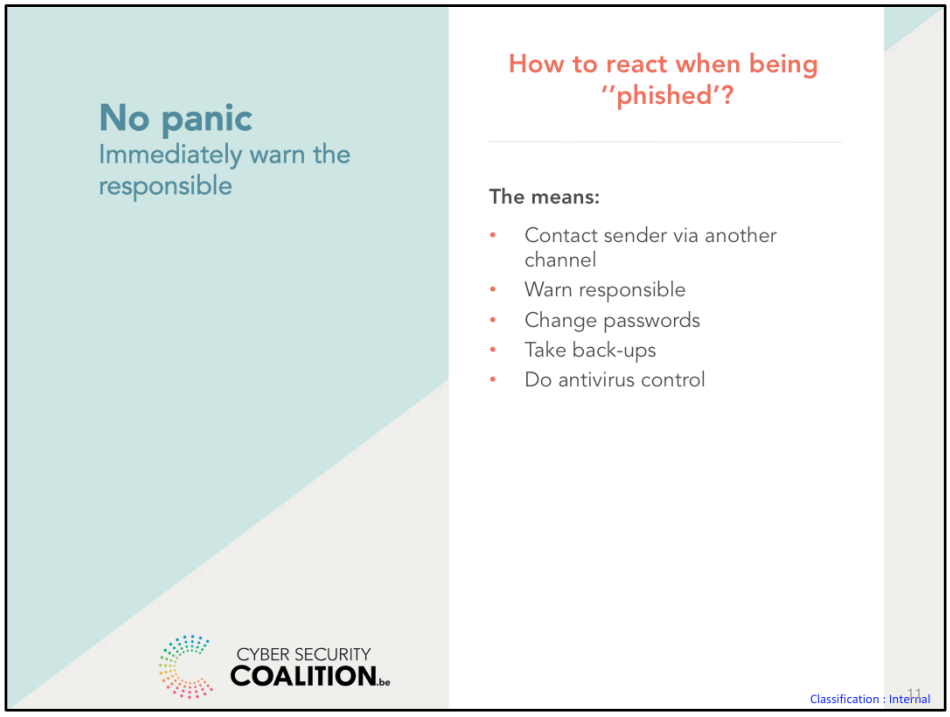
You will see that it is **not always easy**… . But no panic, practice makes perfect!


**Demask a phishing e-mail**

- There is **no reason** why you should receive this message.
- The subject of the e-mail is **vague**, you don't get the context.
- Got into your **spam** folder.
- The tone is **alarming,** threatening or intriguing.


**Good reactions when being phished:**

- **Don't answer** the e-mail!
- Check the **address of the sender** (hover over so that you see the real e-mail address)
    - The two last words after the @ and just before the first '/' are the domain name of the organisation. Check if this is the official domain name of the organisation.
- Check if you can trust the **links** (hover over so that you can see the real web address)
    - The 2 last words before the first single slash are the domain name of the organisation. Check if this is the official domain name of the organisation.
- Distrust attachments, files, images.
- **Don't do transactions** with an **unknown or other than usual payment system**, or via a **changed account number** (check!).




**How to react when being 'phished'?**

- **Contact** sender (person/organisation) **via another channel**.
- **Warn** the **responsible** in your enterprise.
- **Change** professional and private **passwords**.
- Keep your **data on a safe place** and take a **back-up**.
- Do an **antivirus control** on your computer.


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!