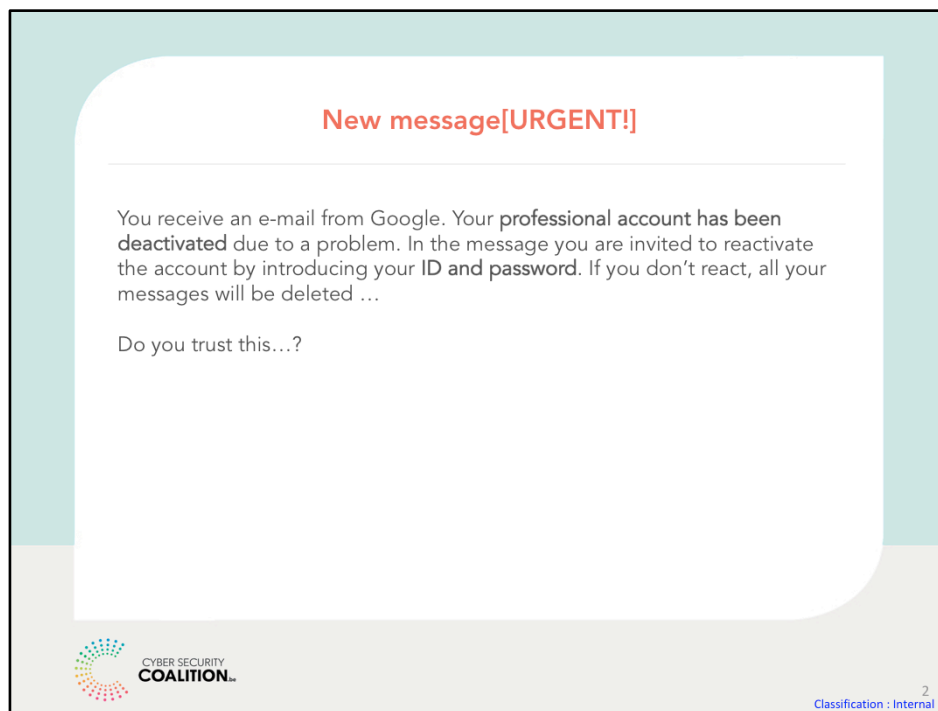


Hello and welcome everybody!



The classic phishing scenario with SME's.

### Case1: University of Maastricht

*On 15 and 16 October 2019, a hacker gained access to the University of Maastricht network because two employees clicked on an attachment in an e-mail. The attacker then compromised several servers from 16 October to 23 December. On 21 November, the attacker managed to acquire full rights within the university's infrastructure via a server that lacked security updates. Then, on 23 December, the attacker placed ransomware (hostage software where the hacker encrypts the data, which can only be decrypted in exchange for payment of a ransom) on 267 Windows servers. After careful analysis – as the leakage of valuable research data and information about commercial operations was at stake – the university decided to pay the requested ransom of USD 220,000 on 30 December.*



3  
Classification : Internal

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:

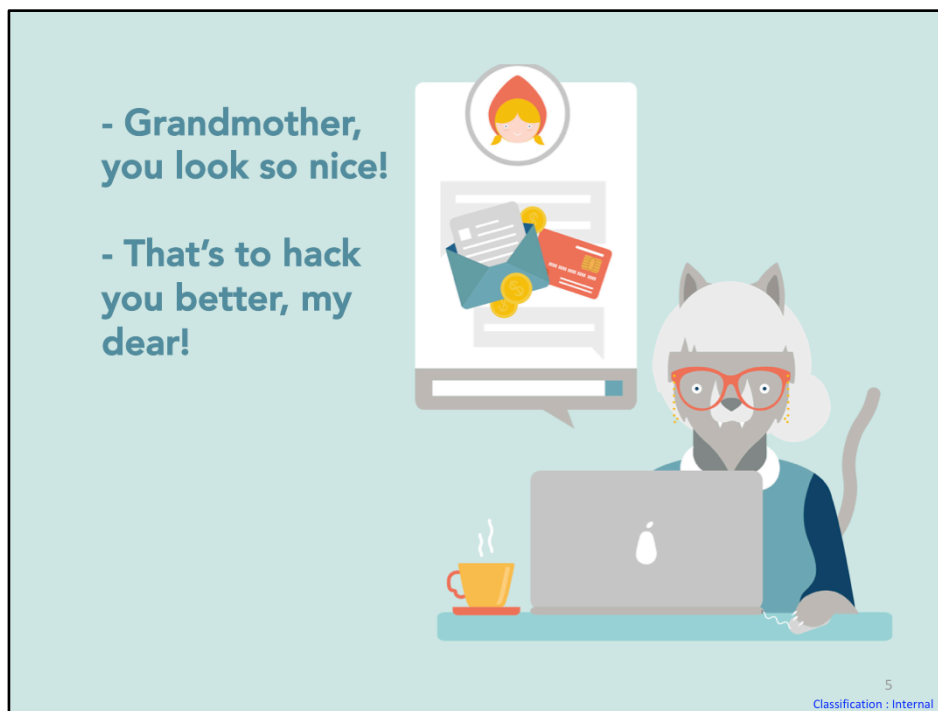
- Improve processes with regard to vulnerability and patch management
- Create more segmentation within the network architecture and user rights
- Implement or improve network and log monitoring
- Practise the different crisis scenarios regularly and improve the prepared plans where necessary

## Case2: Picanol

*On 15 January 2020, the weaving loom producer Picanol Belgium received the news that Chinese colleagues could not log in to a number of IT systems. There were also problems at the parent company in Ypres. Production could gradually be restarted after a week of inactivity. The cause was a malware attack; there was also a ransom demand, but Picanol did not pay. Picanol estimates the damage at 'less than EUR 1 million'.*



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 widely used technique which is increasingly sophisticated



### Phishing... what's that?

**Phishing:**

- 'Angling'
- Steal identity
- Abuse of trust
- E-mail, SMS (Smishing), WhatsApp, Messenger, ...
- Phishing via phone (Vishing)

**Purpose:**

- Personal information
- Sensitive data of the enterprise
- Money transfer
- Industrial sabotage

**How?**

- Infected appendix
- Link to false website
- False payment system

Classification : Internal

Phishing is a fraudulent 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**.

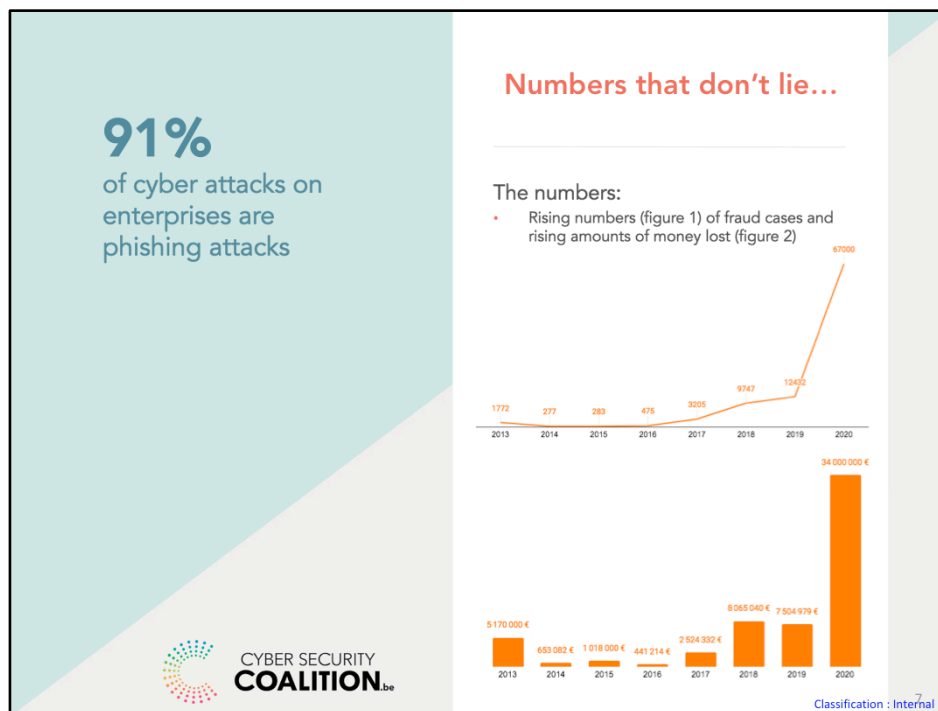
This usually happens via **e-mail, SMS (Smishing), WhatsApp, Messenger**. Also via **phone (Vishing, V=voice)**

#### 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**.



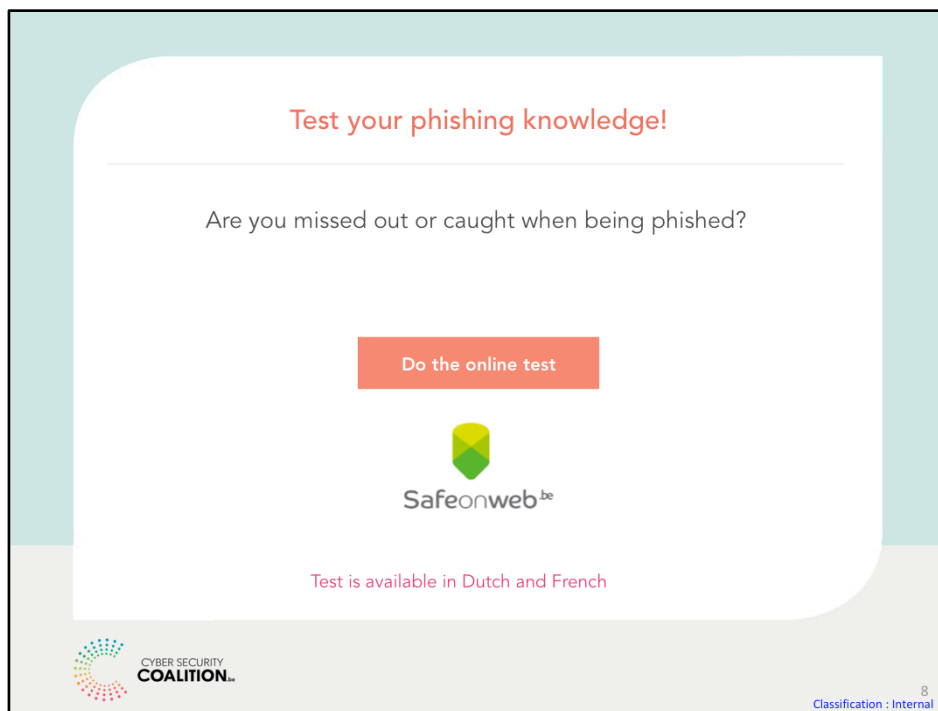
Phishing represents nowadays **91% of all cyber attacks** against enterprises and SME (Cert – 2015)

Unizo (**Unie** Zelfstandige **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](mailto: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 will 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!




The infographic is divided into two main sections. The left section has a light blue background and contains the text 'Be vigilant' in bold, followed by 'Use your common sense and be careful!'. The right section has a white background and contains the title 'How to demask a phishing e-mail?' in red, followed by a horizontal line and the heading 'The signals:'. Below this heading is a bulleted list of four items: 'Strange message', 'Vague subject', 'Spam', and 'Alarming tone'. At the bottom left of the infographic is the 'CYBER SECURITY COALITION.be' logo, which consists of a colorful circular pattern of dots. At the bottom right, there is a small text label 'Classification : Internal'.

**Be vigilant**  
Use your common sense and be careful!

**How to demask a phishing e-mail?**

**The signals:**

- Strange message
- Vague subject
- Spam
- Alarming tone

 CYBER SECURITY COALITION.be


Classification : Internal

### 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.

## 2 know more than 1

If you hesitate, talk to others



### What to do when being 'phished'?

**Good reactions:**

- Don't answer
- Check the address of the sender (hover over so that you see the real e-mail address)
- Check if you can trust the links (hover over so that you can see the real web address)
- Mind the appendices
- Don't use payment systems you don't know

Classification : Internal

#### 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!).

**No panic**  
Immediately warn the responsible

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

**The means:**

- Contact sender via another channel
- Warn responsible
- Change passwords
- Take back-ups
- Do antivirus control

 CYBER SECURITY COALITION<sub>be</sub>

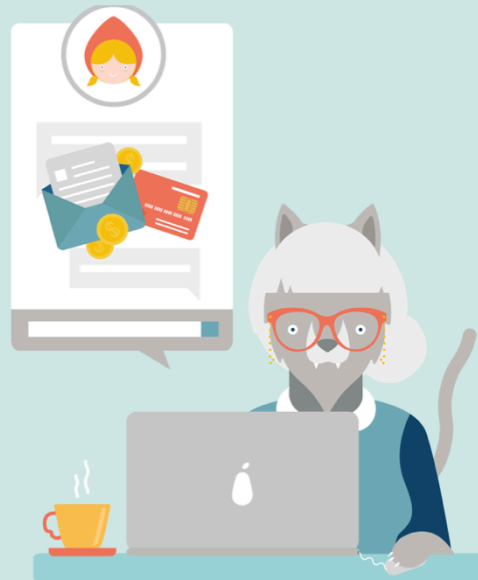
Classification : Internal<sup>11</sup>

#### 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.

**Phishing:  
discuss it! (not  
only with your  
grandma)**

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



12

Classification : Internal

What is your opinion?

Do you have remarks?

What do you remember?

What will be your first action after this presentation?



**CYBER SECURITY  
COALITION**.be

**An initiative from  
the Cyber Security Coalition**

Its objective? Increase the IT-security in Belgium. The Coalition brings together experts from the academic world, the government and the enterprises to better combat cyber-crime.

[www.cybersecuritycoalition.be](http://www.cybersecuritycoalition.be)



All rights reserved © 2020 Cyber Security Coalition

Classification : Internal

Thank you for your attention!