



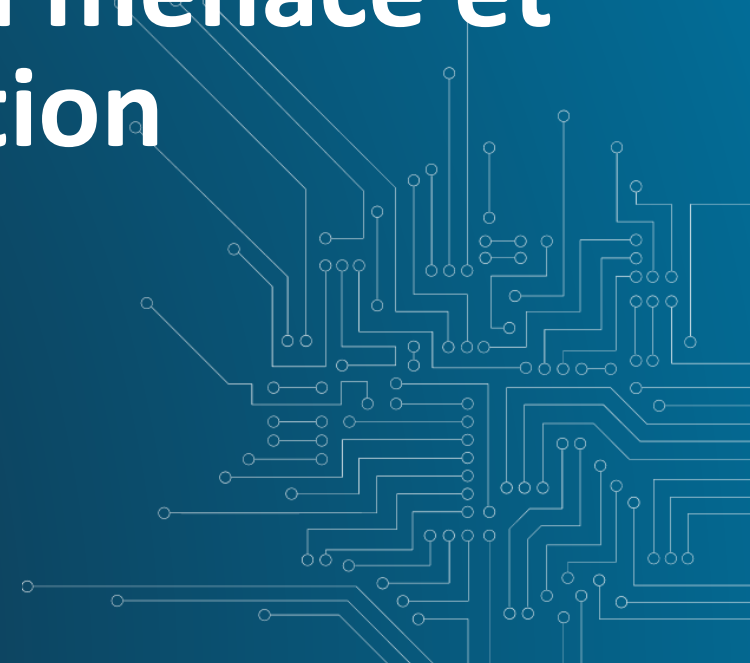
CENTRE FOR
CYBER SECURITY
BELGIUM

Le facteur humain : force ou faiblesse ? Etat de la menace et outils de sensibilisation

Security Forum 24/10/2019

Phédra Clouner

Deputy Director



Legal Basis

- R.D. 10/10/2014

Contribute to build a safer and reliable Internet

Create a national policy and capabilities with existing actors

Belgian policies & Coordination

Legal basis

1. Monitoring, coordinating and supervising **the implementation of Belgian policy** on the subject;
 2. Managing the various projects on the topic of cybersecurity using an **integrated and centralized approach**;
 3. **Ensuring coordination** between the relevant government departments and governments, as well as the public authorities and the private or scientific sectors;
 4. Formulating proposals aimed at **adapting the regulatory framework** in the field of cybersecurity;
 5. **Ensuring crisis management** in case of cyber incidents in cooperation with the government's Coordination and Crisis Centre;
 6. Preparing, disseminating and supervising the **implementation of standards, guidelines and security standards** for the various information systems of the governments and public institutions;
 7. **Coordinating the Belgian representation in international cybersecurity forums**, coordinating the monitoring of international commitments and national proposals on this subject;
 8. Coordinating the **security evaluation** and **certification** of information and communication systems;
 9. **Informing and raising awareness** among users on information and communication systems.
- Integration of the Computer Emergency Response team(Cert.be): new organisation (focus: incident handling- information sharing), more capabilities (24 FTE) – High level technical experts

Cyber Security Coalition Belgium

La « Cyber Security Coalition » réunit des spécialistes en sécurité issus **d'organismes publics, d'entreprises et du monde académique** en vue d'assurer une défense plus efficace des autorités, des entreprises et des citoyens face à la cybercriminalité en Belgique.

La Coalition s'appuie à cette fin sur l'échange d'expériences entre ses membres, ainsi que sur des publications contenant des conseils destinés aux entreprises et des campagnes de **sensibilisation à l'intention du grand public.**



CYBER SECURITY
COALITION.be

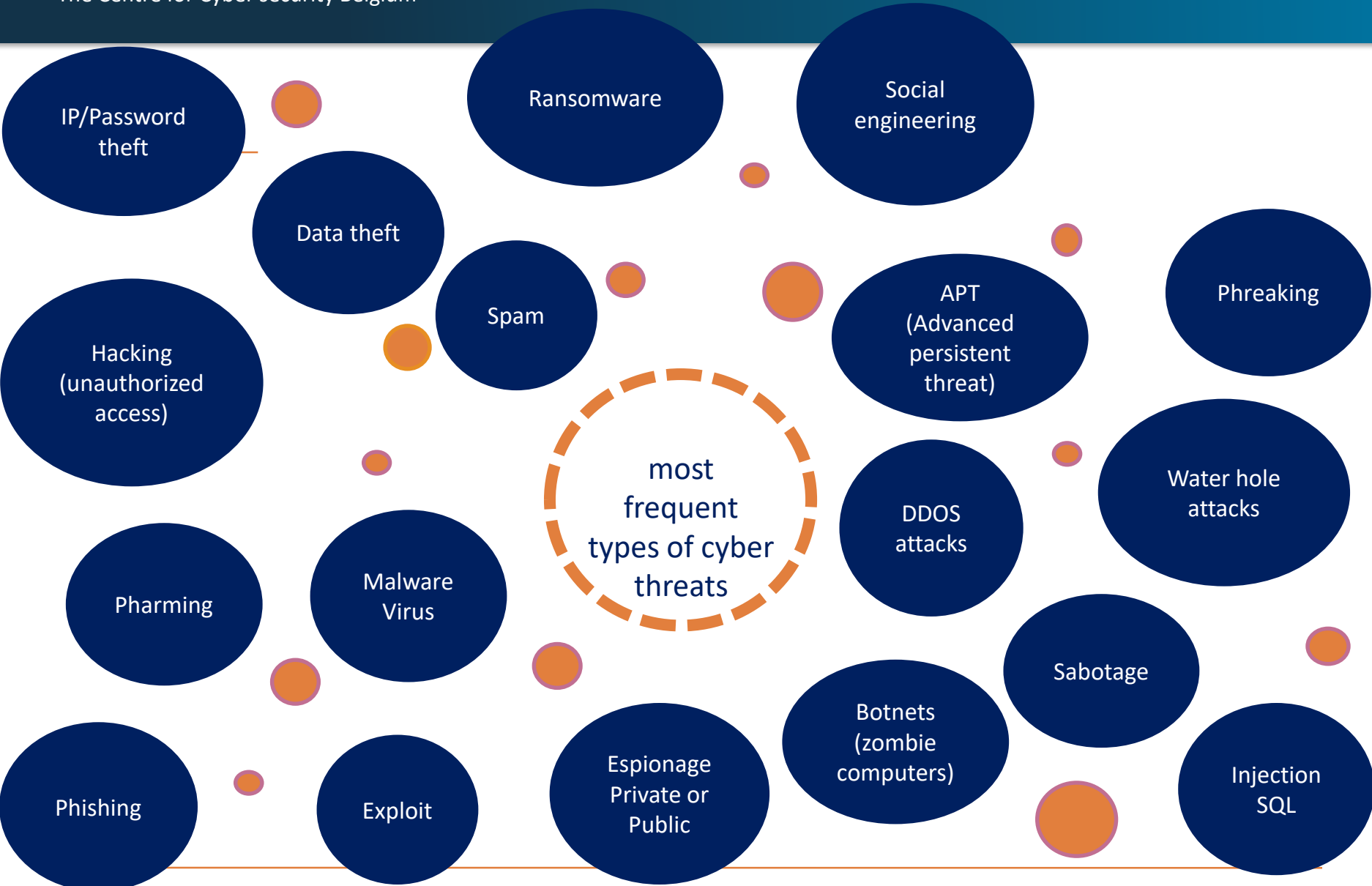
01













































What kind of Cyberthreat?



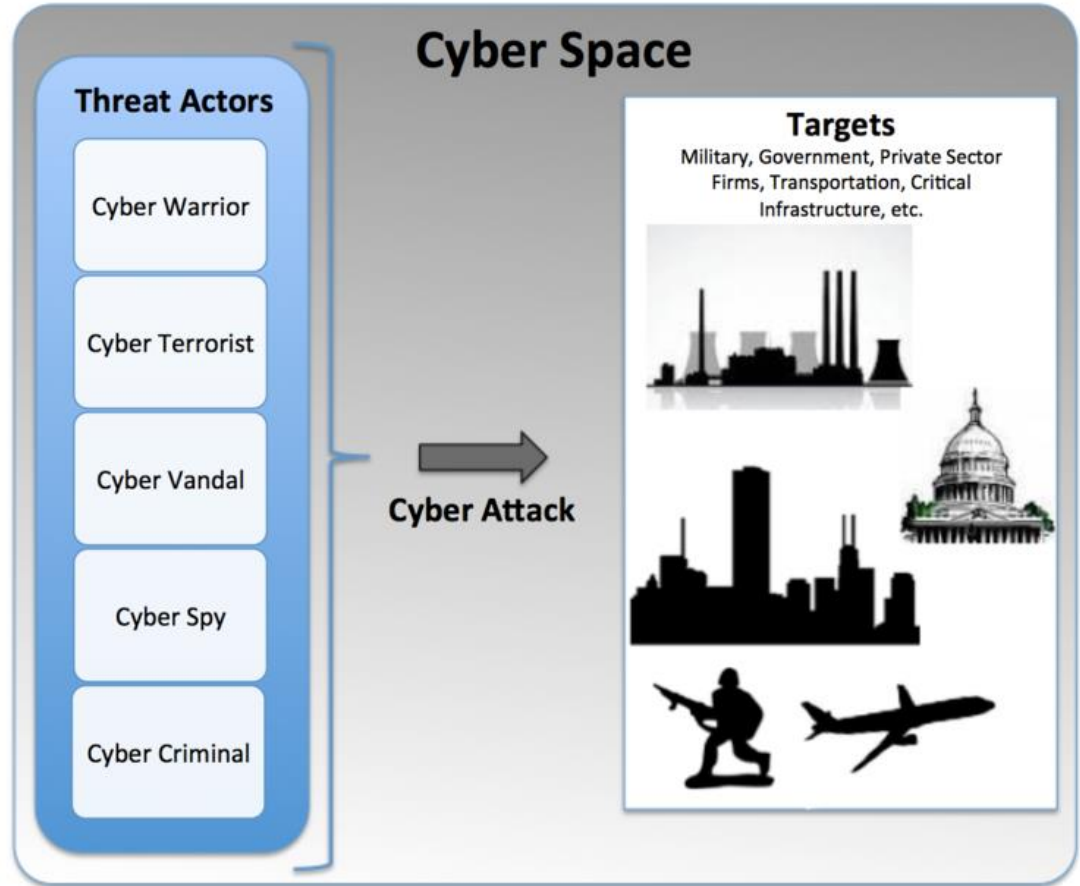
There are only two
types of companies,
those who got hacked
and those who will be.

Robert Mueller



Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware		1. Malware		
2. Web Based Attacks		2. Web Based Attacks		
3. Web Application Attacks		3. Web Application Attacks		
4. Phishing		4. Phishing		
5. Spam		5. Denial of Service		
6. Denial of Service		6. Spam		
7. Ransomware		7. Botnets		
8. Botnets		8. Data Breaches		
9. Insider threat		9. Insider Threat		
10. Physical manipulation/ damage/ theft/loss		10. Physical manipulation/ damage/ theft/loss		
11. Data Breaches		11. Information Leakage		
12. Identity Theft		12. Identity Theft		
13. Information Leakage		13. Cryptojacking		NEW
14. Exploit Kits		14. Ransomware		
15. Cyber Espionage		15. Cyber Espionage		

THREAT ACTORS



Threat Actors (2)

- Nation-State & Next to Nation-State
 - A lot of players: US, Russia, China, UK, Israel, Turkey, Iran, North Korea, Lebanon, Syria, Palestine, Vietnam, Pakistan....
 - Cyber Arms proliferation
 - Poor containment → Uncontrolled spreading
 - Reverse engineering → “easy” re-use
 - Espionage, disinformation, OSINT – Doxing, SCADA control ...
 - Extremely well hidden & using standard services (Gmail, Dropbox etc)
 - APT

Threats for companies

- Industrial Spying
- Theft €
 - CEO Fraude
- Extortion
 - DDOS
 - Ransomware
 - *Informatie theft*
- Disturbance



Risk Analysis

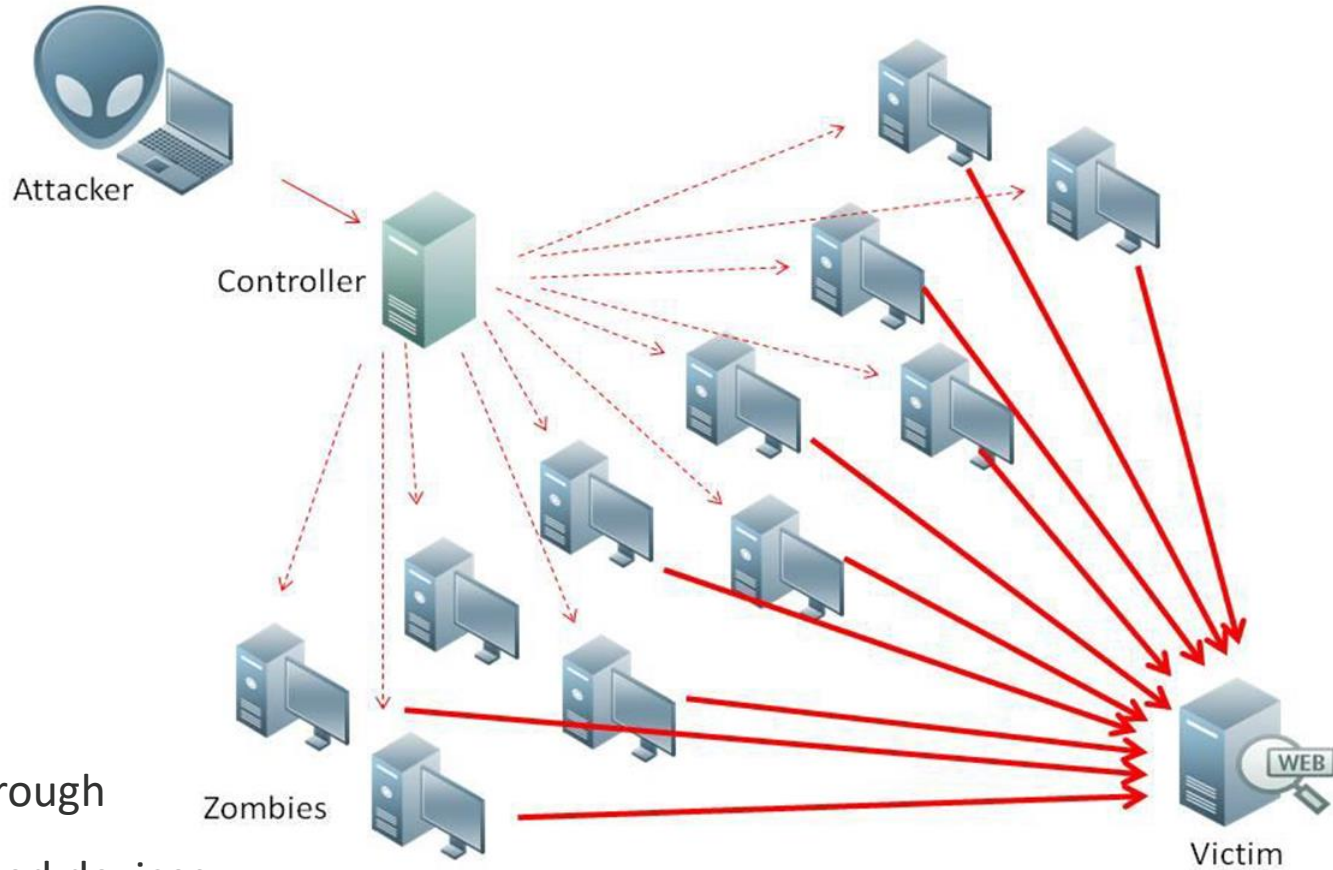
- Outsider threat
- Insider threat: rogue employee
- Insider threat: negligence
- Technical failure
- Calamities

Protect



DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)

BOTNETS



Strong increase volumes through botnets of internet-connected devices

The Internet of Things (IoT)

Threat @ home

Social
engineering

Phishing

Ransomware

Information
Theft



Ransomware – Cryptoware (Remember the WannaCry — Ransomware 12-15/5/2017)

CryptoLocker

Your Personal files are encrypted!

Your personal files **encryption** produced on this computer: photos, videos, documents, etc. Encryption was produced using a **unique** public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **1.00 bitcoin** (~291 USD).

You can easily delete this software, but know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click "Pay with Bitcoin"
To open a list of encoded files, click "Show files"

Do not delete this list, it will be used for decryption. And do not move your files.

Private key will be destroyed on
1/6/2015 1:11:47 PM

Time left
71:52:21

Checking wallet..
Received: **0.00 BTC**

[Show files](#) [Pay with Bitcoin](#)

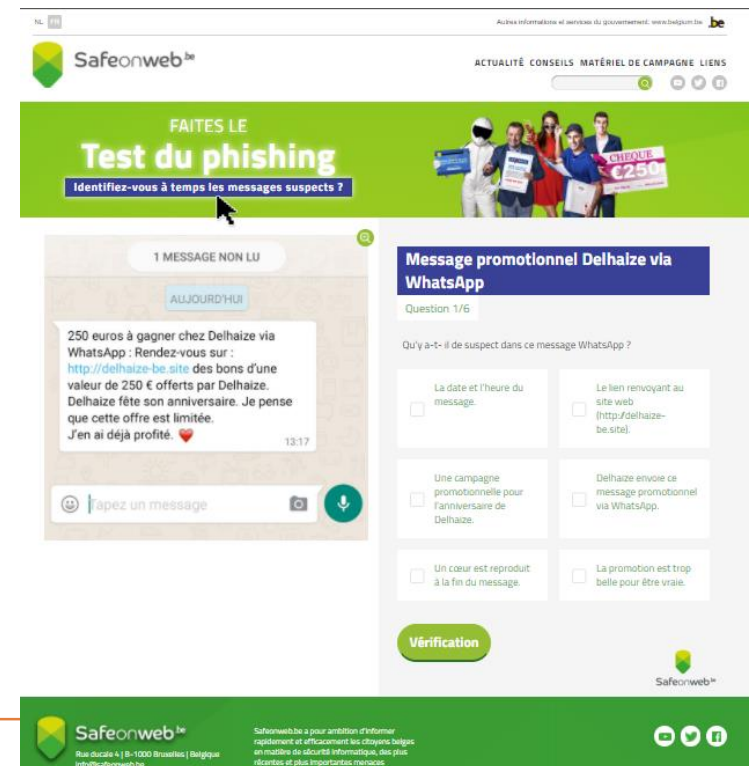
02

How to protect and what's the place of the human factor?



SafeOnWeb (<http://www.safeonweb.be/>) Recommendations for citizens

1. Scan your computer and use an antivirus software
2. Keep your program's up-to-date
3. Make back-ups (cloud)
4. Recognise phishing
5. Use strong password



CCB.BELGIUM.BE

NL FR DE **EN**

Other official information and services: www.belgium.be **.be**



[Home](#) [News](#) [Organisation](#) [Sectors](#) [Vacancies](#) [Contact](#)



At Home

Safeonweb.be informs and advises about cybersecurity and main actual digital threats.



At Work

For more information, advice, and useful links on how to protect computers and networks at work.



At School

More information about cyber education and internet safety in schools.



At government

Guidelines for the various information systems of public institutions. Training for federal public officials.



Vital Sectors

Various projects protecting Belgium's Vital Industries against cyber-attacks.

HIGHLIGHTS



WWW.CERT.BE

NL FR DE **EN**

Other official information and services: www.belgium.be **be**



[About us](#) [Report an incident](#) [Advisories](#) [News](#) [Vacancies](#) [Contact](#)



Welcome to CERT.be

The federal Computer Emergency Response Team, or CERT.be for short, is the operational service of the Centre for Cyber Security Belgium (CCB). The task of CERT.be is to detect, observe and analyse online security problems, and to inform various target groups accordingly.

RECENT ADVICE AND WARNINGS



REMOTE ROOT CODE EXECUTION VULNERABILITY IN EXIM MTA

2019-09-06 16:30

CERT.be recommends to system administrators to patch your systems immediately if they are running Exim.



VULNERABILITY IN PULSE SECURE: PULSE CONNECT SECURE (PCS)

2019-08-27 12:56

CERT.be recommends all System administrators to upgrade their vulnerable Pulse Secure instances to version 9.1R1 and above.



BLUEKEEP: WINDOWS RDP REMOTE CODE EXECUTION VULNERABILITY V2

2019-08-14 10:33

CERT.be recommends administrators to update their Microsoft Windows systems with the latest available patches as soon as possible:

How to avoid cyber incidents?

- Bad news... you can't!
- Maybe... you can use technology ...
- But please take care of your employees...
 - Sometimes they can make mistakes because
THEY ARE NOT INFORMED OR TRAINED!!!!!!!!!!

Human factor is at the origin of 80% (or 70 or 65 (bref... a lot) of Incidents!

- What are the main problems
 - Most of cyber attacks take advantages of human error
 - Inappropriate sharing of data via mobiles devices
 - Physical loss of mobile devices
 - Use of personal devices
 - Inappropriate IT resource use by employees
 - Insider threat (rogue employee)
 - ...
 - **AND... PHISHING!!!!!!!!!!!!!!!!!!!!**

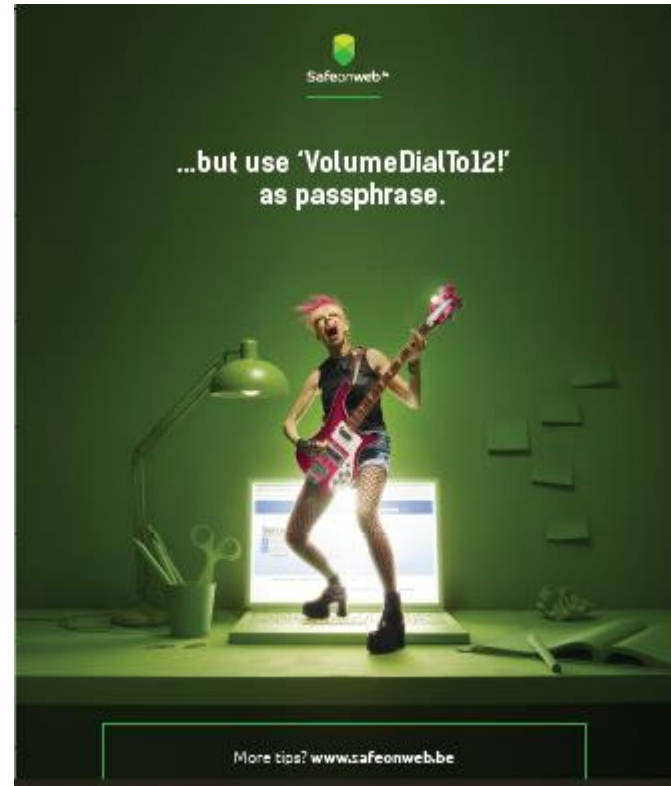
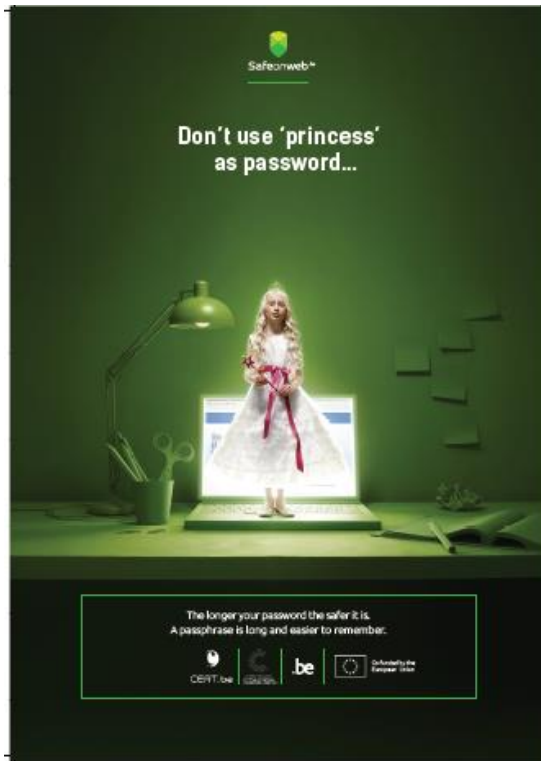
Source : <https://www.kaspersky.com/blog/the-human-factor-in-it-security/> (2018)

SIEM/UEBA
EDR, NTA
Firewalls
Encryption
IDS/IPS
CSOC
End Point Protection
Antivirus/Antimalware
Vulnerability Management
ERM
Soar
Threat Intelligence Platform
Artificial Intelligence
DNS sec
TLS
Exploit Protection
Multi-factor Authentication
DMARC
Machine Learning
IAM
Privileged Access
Management (PAM)
Data loss prevention
WAF
Spam filter
anti-phishing
CSPM and CASB
Pen Testing
Sandboxing
Code Signing
Data Backup
Network Segmentation
SSL Inspection
blablabla Page 20

Human factor: the weakest link? We are not agree! It could be the most efficient firewall... but you have to invest!



Campaign 2015



Campaign 2016



**RÉCUPÉRONS
INTERNET**

6,491,641
BELGES AIDENT LES CYBERCRIMINELS

Ensemble, faisons baisser le compteur.
Faites le test sur safeonweb.be

Faites le test sur safeonweb.be, nettoyez votre ordinateur, smartphone ou tablette et apprenez à tenir compte des risques en ligne. Afin de rendre tous ensemble Internet plus sûr et plus fun.

   Safeonweb^{be}

Campaign 2018



Campaign 2017: Recognise phishing

- Unsubscribed/ unknown email address or not from a known organization (by ex: Anne58632@gmail.com)
- You get scared and have to take action quickly
 - Something wrong with your bank account
 - An expensive order that you never placed
- Your name is not used in the message
- The message contains writing errors or an unnatural language
- You will be asked to submit online personal information
- Attachment or link
- Link does not match what can be expected.
- Your system requests unexpected permission to install a program.



→ AWARENESS IS ONE OF THE KEY!

2019: oops we dit it again!

• WHY?

- Because phishing stays the main vector to spread cyber attacks!
- The cybercriminals are more and more creatives!
- In 2019 'Email is still your worst friend/ your best enemy (Security and risk management summit Gartner)
- Email delivery is involved in 94% of malware detection
- Phishing present in 78% of cyberespionage incidents
- Losses of over 1,2B dollar from business email compromise in 2018

"Relax, réfléchissez à deux fois avant de cliquer sur un lien"

Vous avez dit phishing ?

Le phishing est une escroquerie en ligne au moyen de faux emails, sites internet ou messages. Les cybercriminels exploitent la confiance que vous avez, par exemple, en une personne ou en une société. Ils essaient aussi de vous faire peur. Ne tombez pas dans le panneau !

Comment identifier les messages suspects ?

Les messages de phishing :

- arrivent généralement **de façon inattendue** et sans raison
- sont insistants ou tentent d'éveiller votre curiosité
- contiennent des fautes ou utilisent des formulations bizarres
- s'adressent à vous avec un **titre vague** ou utilisent votre adresse email au lieu de votre nom ou prénom
- **proviennent d'un expéditeur inconnu**
- ont un lien qui ne mène pas à un site internet sécurisé

Les faux messages ne sont pas toujours des emails. De plus en plus, les escrocs envoient de faux sms – on parle alors de **Smishing**. Vous pouvez aussi recevoir des messages de phishing via les médias sociaux, comme Facebook ou WhatsApp.

Phishing

- Call the population to participate (it works!)
 - Forward suspicious e-mails
 - suspicious@safeonweb.be
 - verdacht@safeonweb.be
 - suspect@safeonweb.be

In 2018

648.522	received mails
410.315	contained URLs
1.478	blocked phishing sites

In 2019/Jan-Aug

970.000	received mails
833.000	contained URLs
864	blocked phishing sites

Herken jij verdachte berichten op tijd?

DOE DE PHISHINGTEST OP SAFEONWEB.BE

Een initiatief van:





DISTRIBUTEURS DE BILLETS



**Crier votre code PIN,
vous le feriez, là ?**

En ligne aussi, réfléchissez
à deux fois avant de
cliquer sur un **lien**

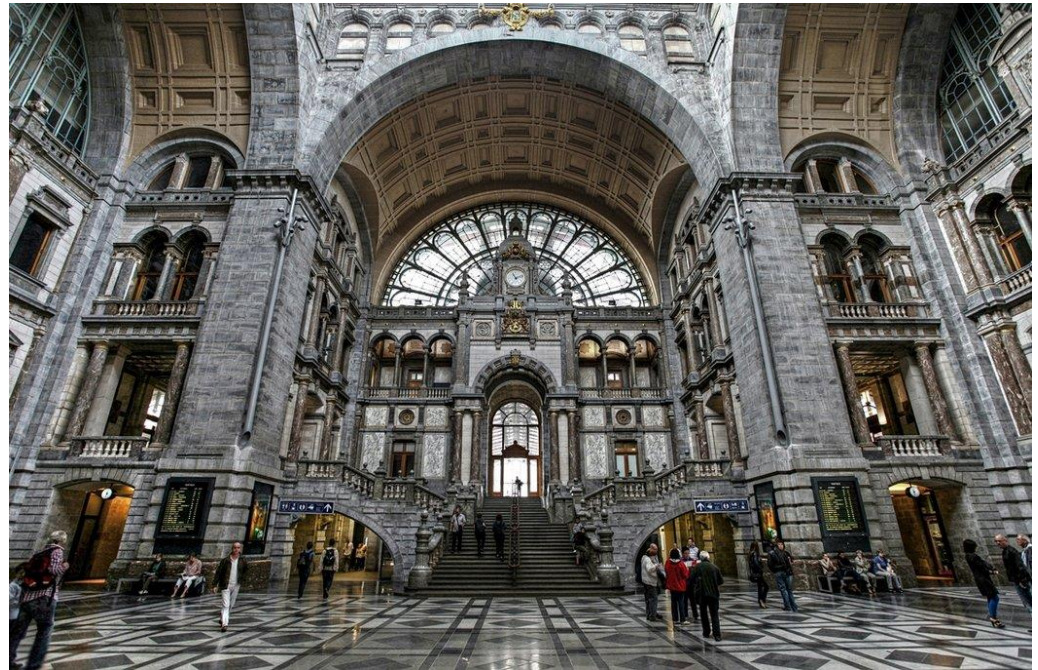
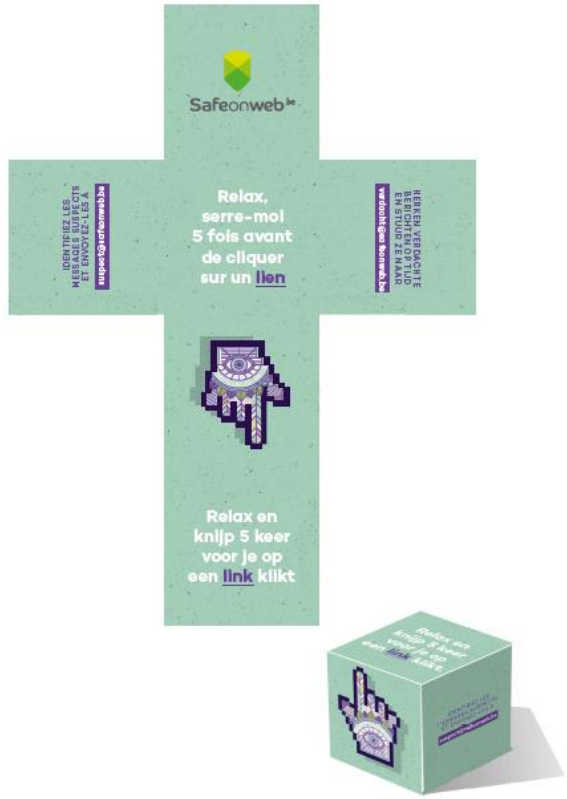
**Découvrez comment identifier
les messages suspects sur
safeonweb.be**

   **.be**

BUS STIB



METRO 5 GARES



FEDERAL TRUCK



Questions ?

Info@ccb.belgium.be

