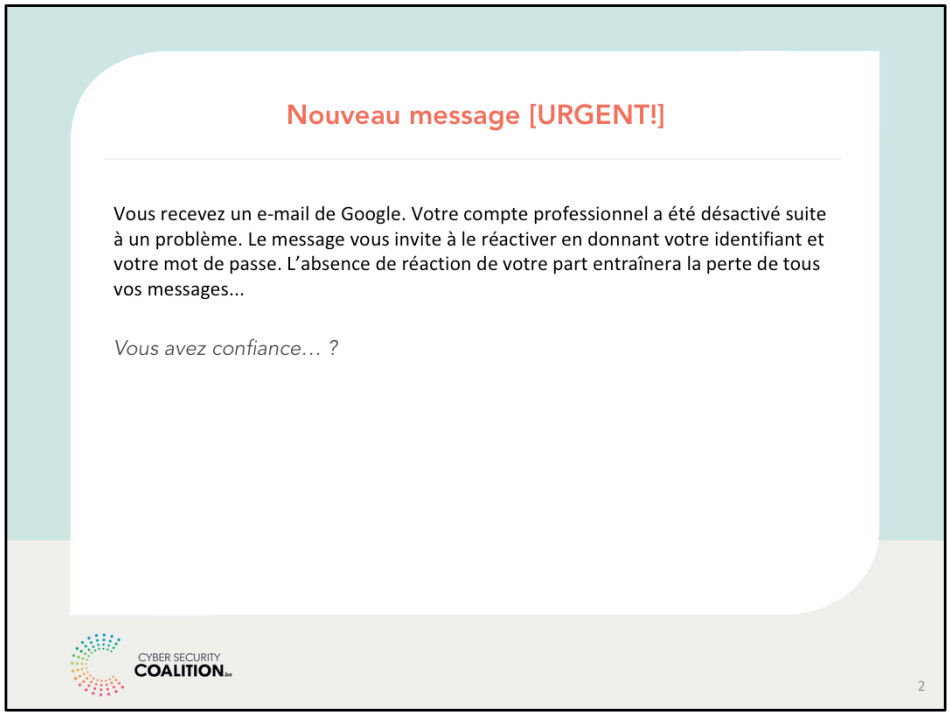
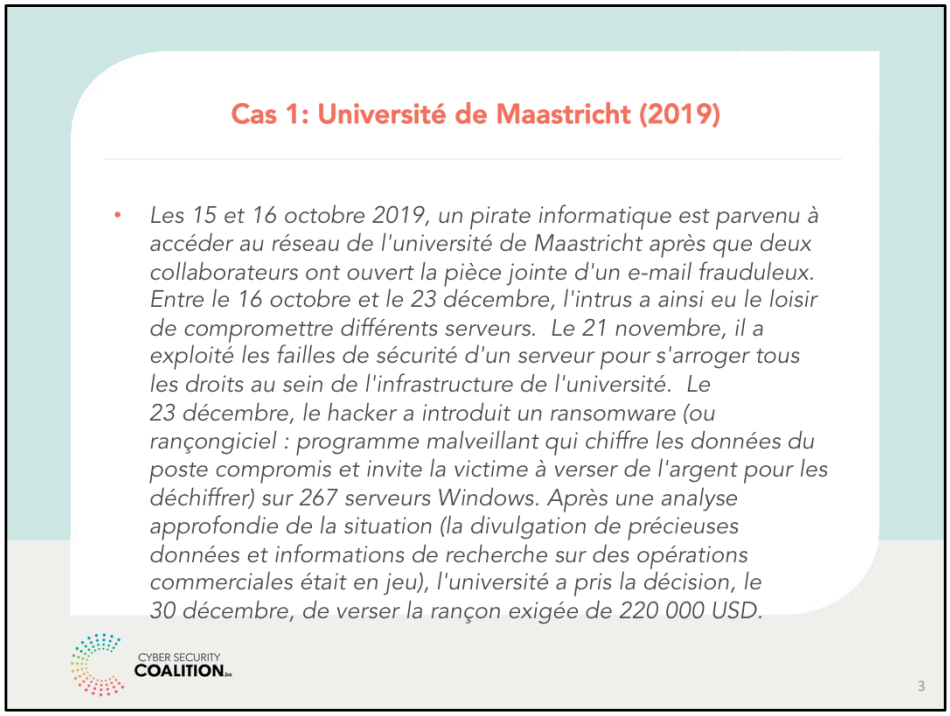
Bonjour et bienvenue à tous !



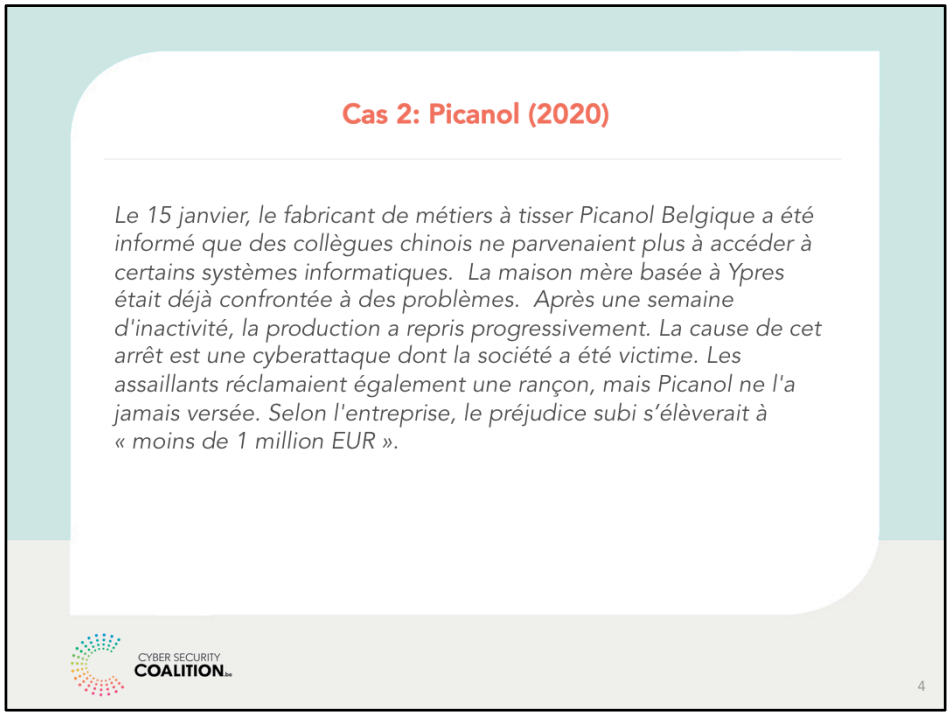
Le scénario classique du phishing dans les entreprises et PME.



Le cas de l'université de Maastricht (source : FOX IT – NCC Group) nous apprend que les pirates informatiques prennent le temps nécessaire pour mettre au point leur attaque en toute discrétion.

À la suite de cet incident, les conseillers en sécurité concernés ont émis les recommandations suivantes :

- Optimiser les processus existants en matière de vulnerability & patch management
- Accroître la segmentation entre l'architecture du réseau et les droits des utilisateurs
- Implémenter ou améliorer le suivi des activités et des connexions
- Procéder à un examen méthodique de divers scénarios de crise et y apporter les ajustements nécessaires



Source: VRT Journal

Attention, phishing !
Une personne mal intentionnée veut partir à la pêche aux informations.

Dans votre boîte e-mail professionnelle, vos dossiers confidentiels, vos comptes en ligne... Souvent, elle ne s'arrête pas là : elle peut aussi faire une belle prise dans votre profil sur les réseaux sociaux et même effectuer des achats sur vos sites préférés.

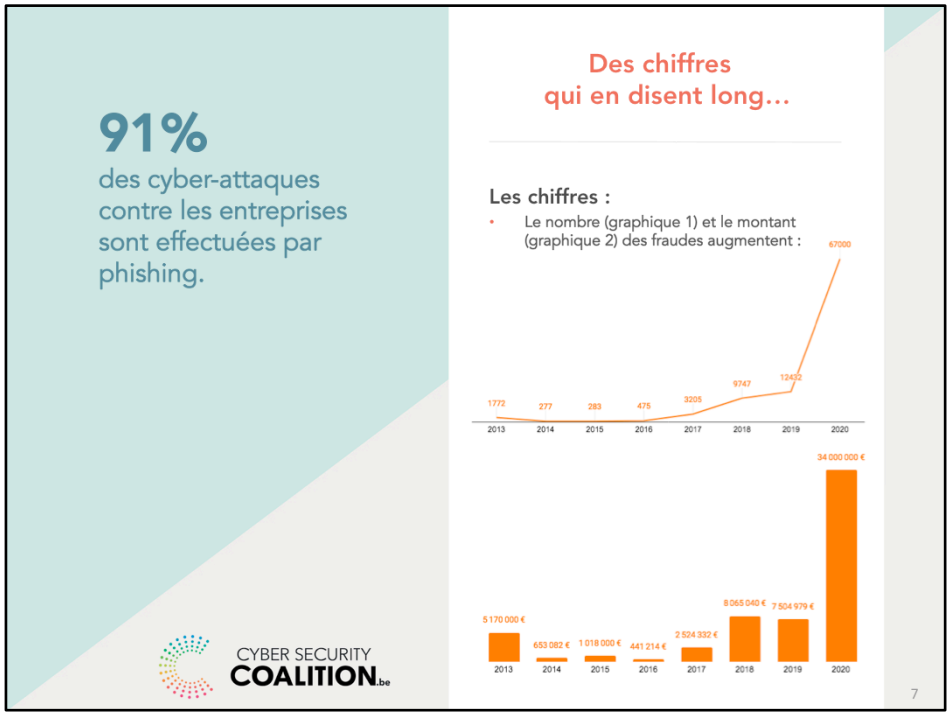
Le phishing, ou **hameçonnage**, est une technique frauduleuse qui consiste à **usurper l'identité d'une personne ou d'une institution.**

Le fraudeur fait croire à la victime qu'elle s'adresse à un **tiers de confiance** — banque, administration, contact personnel, etc. — afin de lui soutirer des **renseignements personnels ou professionnels**.

Le plus souvent, il s'agit d'un **e-mail,** SMS (Smishing), message WhatsApp, Messenger, … Aussi via téléphone (Vishing, V=Voice/Voix)

Son but ?
- Récupérer des **informations personnelles** (identifiant, mot de passe, numéro de carte de crédit).
- Accéder à des **données sensibles** au sein de l'entreprise.
- Obtenir un **transfert d'argent**.
- **Sabotage** industriel

Comment ?
- Une **pièce jointe infectée** qui installe un virus.
- Un lien qui redirige vers un **site malicieux**.
- Un faux système de **paiement**.



Le phishing représente aujourd'hui **91% des cyber-attaques** contre les entreprises et les PME (Cert – 2015)

Selon une étude d'UNIZO, **une entreprise sur cinq** a déjà été victime de ce genre de fraude en Belgique.

Nombre de cas de fraude et pertes financières dans le secteur financier en Belgique (source : Febelfin – mars 2020) : le nombre de cas de fraude recourant au phishing est reparti à la hausse en 2019 pour s'établir à 12 432, soit un bond de 27,5 % par rapport à 2018 (9 747). Le coût que représentent ces cas de fraude pour les institutions financières belges semble s'être stabilisé en 2019 (7,5 millions EUR) par rapport à 2018 (8 millions EUR). Un simple calcul permet de constater que les cybercriminels sont arrivés à extorquer en moyenne 604 euros par victime en 2019. Dans l'immense majorité des cas, il s'agit de petits montants, mais il arrive parfois que les pirates s'emparent d'un butin nettement plus important. Malheureusement, les chiffres de début 2020 (sur fonds de COVID-19) s'envolent à nouveau.

Grâce à la vaste contribution de la population belge, le Centre pour la Cybersécurité Belgique (CCB) est parvenu, en 2018, à bloquer en moyenne **quatre sites Web frauduleux par jour**. Au total, **1 478 sites de phishing ont ainsi été bloqués**.

En 2018, les Belges ont envoyé **648 522 e-mails** à l'adresse suspect@safeonweb.be. Les e-mails transférés sont automatiquement scannés par le logiciel BeFish. Dans un premier temps, les messages contenant des adresses URL sont identifiés. Ensuite, les liens suspects présents dans ces e-mails sont détectés et transmis à l'organisation *EU Phishing Initiative*, qui peut les bloquer grâce à la collaboration de quatre navigateurs : Google Chrome, Mozilla Firefox, Safari et Internet Explorer.

Rendez-vous sur : https://www.safeonweb.be/fr/quiz/test-du-phishing

Dans ce **test (anonyme)**, vous verrez **10 e-mails** envoyés chaque jour par de véritables entreprises et organisations et par des escrocs.

- Saurez-vous **démasquer** les e-mails de phishing ?
- Défiez vos collègues : qui a le **meilleur score** ?

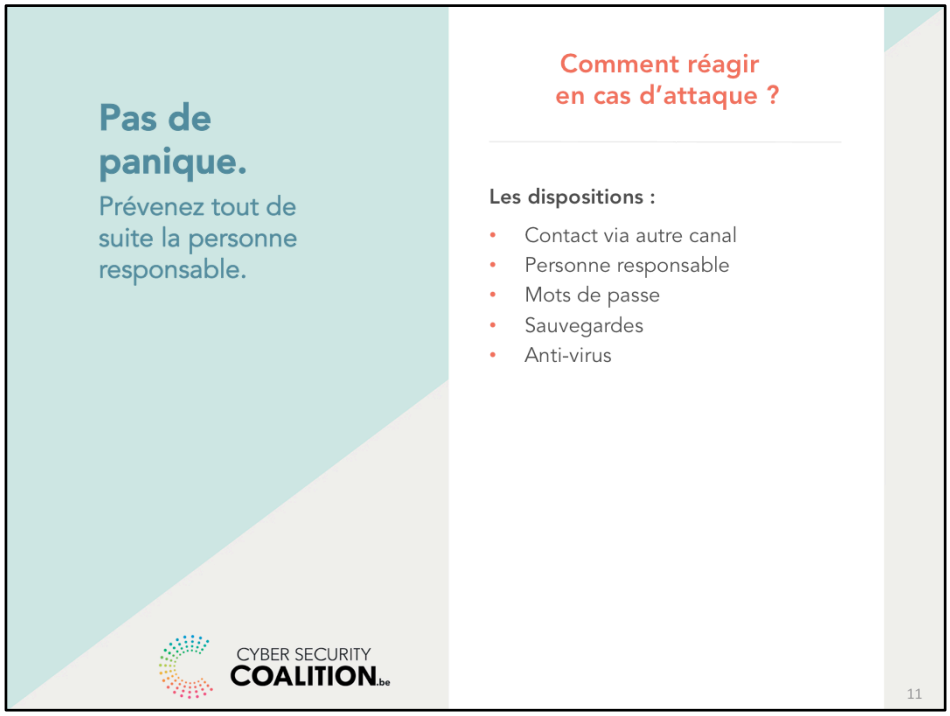
Vous verrez que ce n'est **pas toujours facile**. Mais pas de panique, c'est en forgeant qu'on devient forgeron….

Démasquez un e-mail de phishing

- Il n'y a **aucune raison** que vous receviez ce message.
- L'objet de l'e-mail est **vague**, vous n'identifiez pas le contexte.
- Il est arrivé dans vos **spams**.
- Le ton est **alarmiste**, menaçant ou intriguant.

Adoptez les bons réflexes contre le phishing

- Ne **répondez pas** à l'e-mail !
- Vérifiez la conformité de l'**adresse expéditeur** (survolez, ainsi vous verrez l'adresse email réelle)
    - Les deux derniers mots après le @ et juste avant le premier '/' sont le nom du domaine de l'organisation. Contrôlez si ce nom est le nom du domaine officiel de l'organisation.
- Survolez les liens pour contrôler la **fiabilité de la cible** (survolez, ainsi vous verrez l'adresse réelle du website concerné)
    - Les 2 derniers mots juste devant la première seule barre oblique sont le nom du domaine de l'organisation. Contrôlez si ce nom est le nom du domaine officiel de l'organisation (sur leur site).
- Méfiez-vous des **pièces jointes**, fichiers et images.
- N'effectuez **aucune transaction** via un système inconnu.



Réagissez en cas d'attaque par phishing

- Contactez **via un autre canal** la personne ou l'organisation usurpée.
- Prévenez la **personne responsable** au sein de votre entreprise.
- Changez vos **mots de passe**, professionnels et privés.
- Mettez vos **données à l'abri** et faites des sauvegardes.
- Faites un check **anti-virus** sur votre ordinateur.

Qu'en pensez-vous ?
Avez-vous des remarques ?
Qu'avez-vous retenu ?
Quelle sera votre première action suite à cette présentation ?

Merci de votre attention !