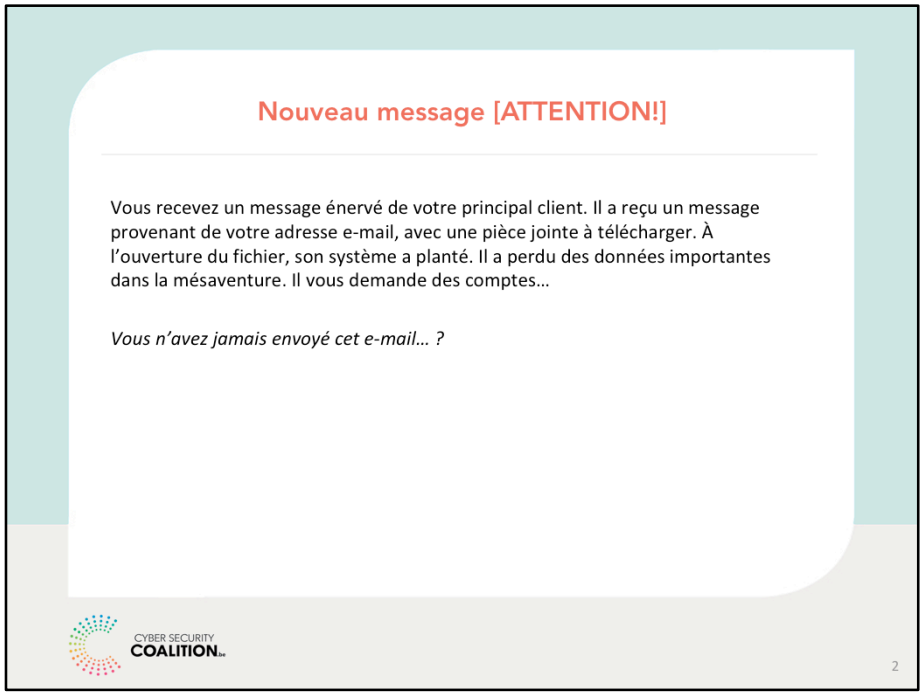
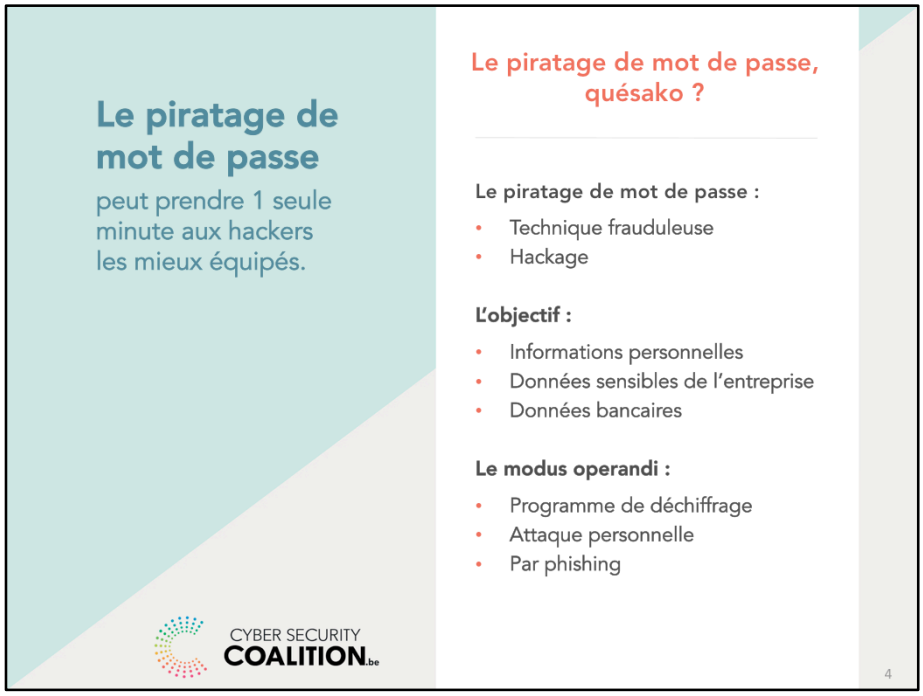
Bonjour et bienvenue à tous !



Un scénario classique de piratage de mot de passe dans les entreprises et PME.

Alerte piratage !
Une personne mal intentionnée a piraté votre mot de passe.

Elle a maintenant les clés de chez vous. Elle peut vous voler des données confidentielles, envoyer des messages à votre réseau de contacts, vos collègues, vos clients. Se connecter à votre profil sur les réseaux sociaux, faire des achats sur vos sites préférés.



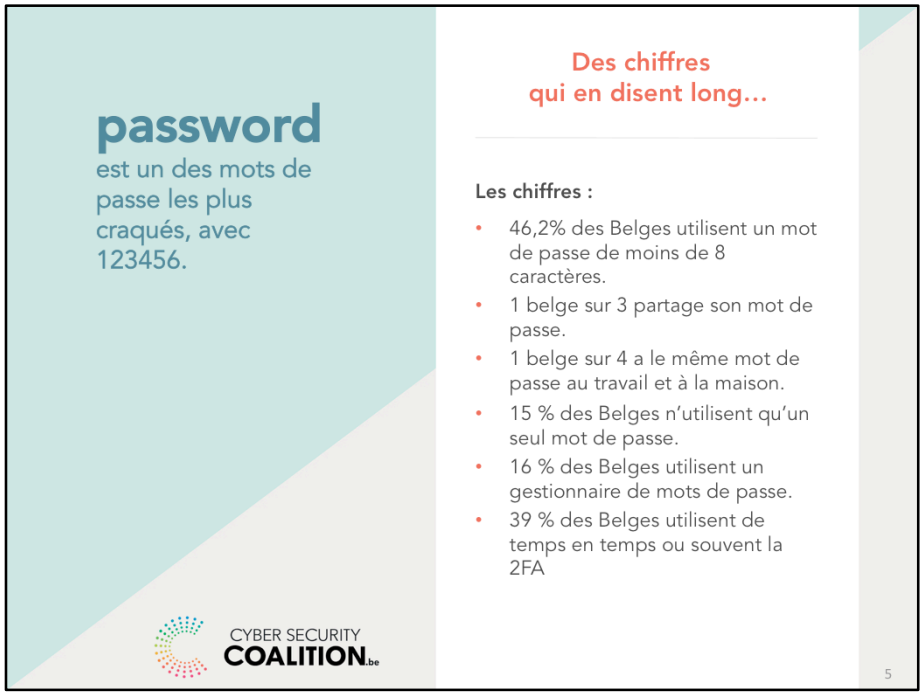
Le piratage de mot de passe est une technique frauduleuse qui consiste à **hacker un mot de passe pour accéder** à **vos comptes professionnels ou privés**.

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.
- Vous **soutirer de l'argent** en accédant à vos données bancaires.

Comment ?

- Un hacker qui utilise un **programme de déchiffrage** de mot de passe
- Une attaque personnelle, un proche ou un tiers ayant eu un accès direct à votre mot de passe
- Un **e-mail de phishing** qui vous a soutiré l'information de manière frauduleuse



Près de la moitié des Belges utilisent un mot de passe faible de **moins de 8 caractères**.

Inquiétant ! **1 belge sur 3 partage son mot de passe** avec une tierce personne, proche ou non.

Autre chiffre alarmant pour les entreprises et les PME : **1 belge sur 4 a le même mot de passe** pour ses comptes privés et professionnels.

15 % des Belges n'utilisent qu'un seul mot de passe. (Safeonweb, Indice de santé digitale 2018)

Il n'est pas si simple de retenir des mots de passe. Pour vous faciliter la tâche, vous pouvez utiliser un gestionnaire de mots de passe en ligne ou « password manager ». Il y en a de toutes sortes, gratuits et payants. **Seuls 16 % des Belges utilisent un gestionnaire de mots de passe**. (Safeonweb, Indice de santé digitale 2018) Les gestionnaires de mots de passe retiennent tous vos mots de passe et doivent être sécurisés à l'aide d'un mot de passe fort, qui est alors le seul que vous avez à retenir.

39 % des Belges utilisent de temps en temps ou souvent la 2FA (authentification à 2 facteurs : voir slide 8). (Safeonweb, Indice de santé digitale 2018)

123456, azerty, Star Wars ou une combinaison « nom et année de naissance » (comme MonNom1985) sont les mots de
passe les plus utilisés. Ce n'est pas une bonne idée, car il existe des programmes qui cassent automatiquement ces mots de passe ou qui testent toutes les combinaisons de caractères possibles à la vitesse de l'éclair.

Rendez-vous sur : https://www.grc.com/haystack.htm

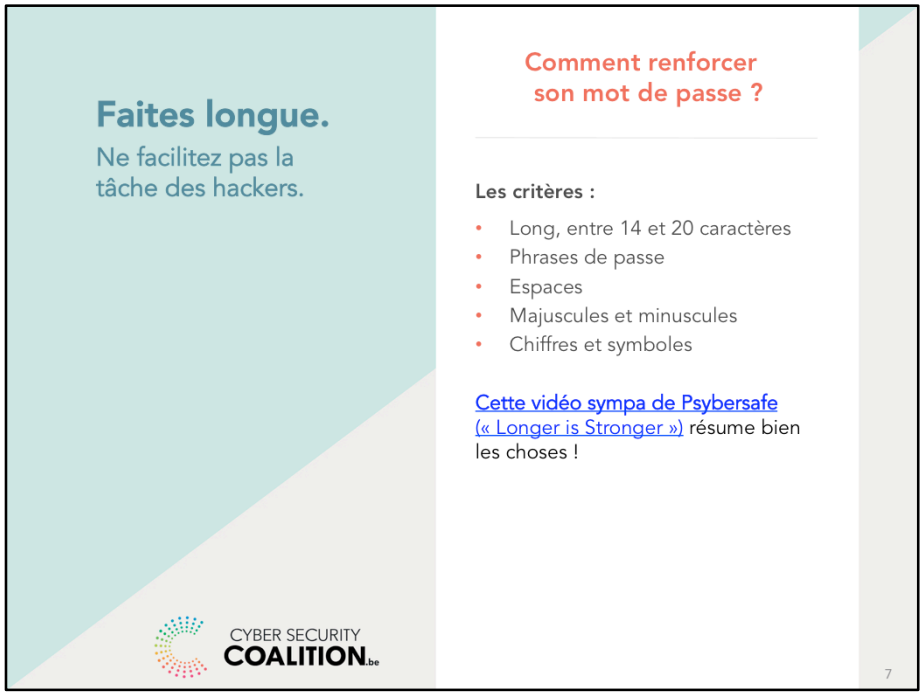
Dans ce **test (anonyme)**, vous ne devez pas communiquer votre mot de passe, évidemment !

Mais en répondant à **quelques questions**, vous saurez en combien de temps un hacker peut pirater votre mot de passe.

- Alors, en combien de temps ?
- Défiez vos collègues : qui a le **mot de passe le plus compliqué** ?

Vous verrez qu'il n'est peut-être **pas si fort** que vous le pensez. Mais pas de panique, il est encore temps d'en changer…

Et bien entendu, ne communiquez JAMAIS vos mots de passe.



Renforcez votre mot de passe

- Composez un mot de passe long, entre **14 et 20 caractères**.
- Préférez des **phrases de passe**, faciles à retenir et plus sûres.
- Conservez les **espaces** pour simplifier la frappe.
- Utilisez des **majuscules et minuscules**.
- Ajoutez des **chiffres et symboles**.

Un mot de passe fort ne doit pas nécessairement être complexe

Une idée fausse répandue est qu'un mot de passe fort doit être aussi complexe que possible. Ces mots de passe sont difficiles à retenir, difficiles à taper et avec les ordinateurs superpuissants d'aujourd'hui, un assaillant peut facilement les casser. La clé d'un mot de passe fort réside dans sa **longueur** : **plus il y a de caractères, mieux c'est.** Ces mots de passe sont appelés des phrases secrètes (passphrases), car ils consistent en une courte phrase ou en une série de mots aléatoires. Par exemple: « heure de boire un petit café ! » ou « un-escargot-lent-rampe-sur-la-vitre ». Ces deux mots de passe ont plus de douze signes et sont faciles à retenir et simples à taper tout en étant difficiles à casser.

Et si l'on vous demande d'inclure des symboles, des chiffres ou des majuscules dans votre mot de passe, vous pouvez facilement en insérer dans la phrase.

Si vous ne pouvez pas utiliser minimum 14 caractères, suivez toujours « l'ancienne » norme qui recommande au moins une majuscule, une minuscule, un chiffre et un caractère spécial.

Malheureusement, les mots de passe les plus utilisés sont toujours 123456, 123456789, qwerty, password ou 11111 (UK Cybersurvey, 2019).

Adoptez les bon réflexes contre le piratage de mot de passe

- Différenciez vos mots de passe **professionnels et privés**.
- Préférez la **double authentification**, avec un code SMS.
- Veillez à utiliser des **mots de passe différents par application/ compte** : à chaque compte son mot de passe. Souvent, les cybercriminels essaieront un mot de passe volé auprès d'un Les anmaximum de services en ligne différents. Si vous utilisez des mots de passe différents pour chaque compte et que l'un d'entre eux est compromis, vos autres comptes seront encore en sécurité.
- Privilégiez un **système de double contrôle**, par exemple en combinant un mot de passe avec un code par SMS (il s'agit alor d'une **authentification à deux facteurs ou multifacteur** : voir ci-dessous).
- Pour les applications et les comptes importants, rendez votre mot de passe encore plus long/complexe et appliquez une méthode de double vérification (2FA).
- **Changez de mot de passe au moins une fois par an**. Ne réutilisez pas d'anciens mots de passe ou de parties de mots de passe. Par exemple, ne changez pas « Lecavaliermontesurlecheval2016 » en « Lecavaliermontesurlecheval2017 ».
- Ne sauvegardez pas votre mot de passe dans votre **navigateur, un fichier**
- Ne communiquez pas votre **mot de passe à des tiers**.
- Utilisez un **'password manager'** une application qui gère vos mots de passe (il faut juste mémoriser un seul mot de passe, celui qui donne accès au password manager). Exemples: LastPass, OnePass, Dashlane, Keepass

Source : Vrije Universiteit Brussel

L'authentification multifacteur (MFA) est une méthode d'authentification qui impose à l'utilisateur de parcourir au moins deux étapes (facteurs) pour accéder à un compte ou à un service.

Voici les facteurs habituels :

1. Quelque chose que vous savez : c'est le facteur le plus connu, un nom d'utilisateur et un mot de passe.
2. Quelque chose que vous êtes : ce sont toutes les données biométriques, comme une empreinte digitale, la reconnaissance faciale ou un scan rétinien.
3. Quelque chose que vous avez : les cartes d'accès et les jetons physiques sont des exemples typiques. L'appareil que l'utilisateur emploie pour se connecter peut aussi servir de facteur. Dans ce cas, il est uniquement possible de se connecter à partir d'un « appareil de confiance ».
4. L'emplacement : avec ce facteur, l'utilisateur doit se trouver à un certain endroit pour avoir accès aux services. Il peut s'agir d'une limitation géographique ou de réseau.

À la première étape, l'utilisateur introduit son nom d'utilisateur et son mot de passe. À la deuxième étape, l'utilisateur doit exécuter une autre action. Il doit par exemple introduire une deuxième clé, comme un code reçu par SMS ou créé à l'aide d'une app installée sur son smartphone, ou procéder à la confirmation de sa demande d'identification via une app liée au service. C'est un exemple typique d'authentification à deux facteurs (2FA).

À quoi sert l'authentification multifacteur ?

tivirus, pare-feux et autres mesures de sécurité en place ne vous seront d'aucun secours si un cybercriminel se fait passer pour un utilisateur légitime. Si un cybercriminel se connecte avec vos identifiants, le système pensera que c'est vous et lui accordera donc toutes les autorisations et tous les pouvoirs dont vous disposez.

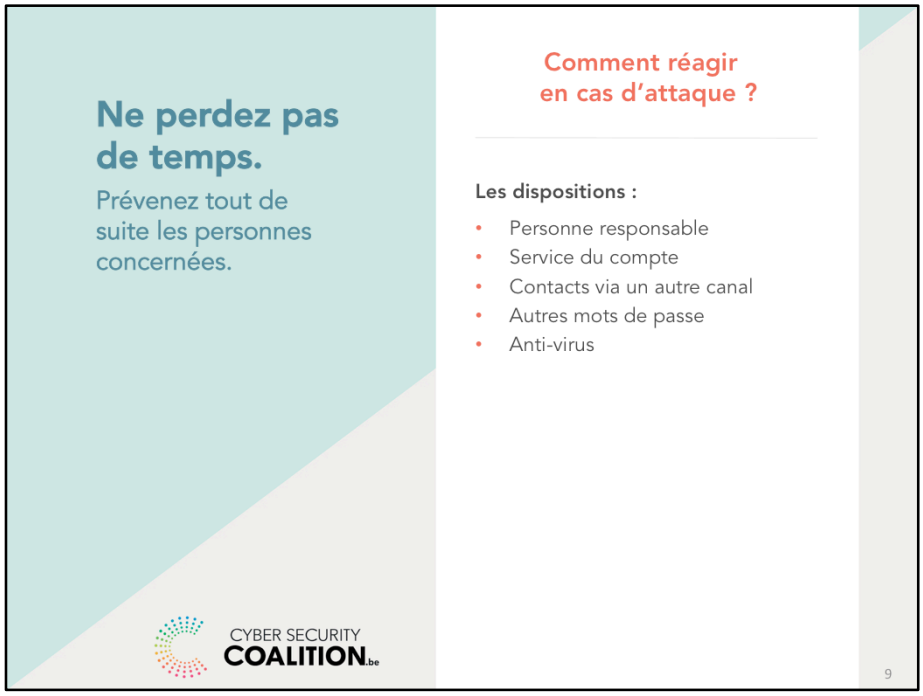
La MFA améliore la sécurité de vos identifiants et est devenue un élément très important de la sécurisation des informations. Si votre mot de passe est compromis, le cybercriminel ne pourra pas directement s'en servir, car il lui manquera encore le deuxième facteur pour pouvoir s'authentifier.

La MFA améliore aussi la conformité juridique. Le Règlement général sur la protection des données (RGPD) impose notamment d'optimiser la protection des données sensibles liées à la personne. La MFA est une étape importante en ce sens.

Limitations de l'authentification multifacteur

La MFA n'est pas 100 % à l'épreuve de la cybercriminalité. Par exemple, les utilisateurs peuvent toujours tomber dans le piège d'attaques de phishing qui les réorienteront vers un site Internet frauduleux qui leur demandera leurs données MFA. Le cybercriminel obtient ainsi les deux facteurs et pourra s'en servir pour s'authentifier une fois. En outre, si le deuxième facteur vous est envoyé par SMS, ces SMS peuvent être interceptés par le biais d'un clonage de carte SIM (les criminels font une copie de votre téléphone et reçoivent alors des copies de tous les SMS que vous recevez).

Malgré ces limitations, la MFA reste la méthode de sécurisation la plus simple et un système très efficace pour lutter contre l'exploitation de mots de passe compromis. De plus en plus, la MFA est donc considérée comme une norme de sécurisation minimale.



Réagissez en cas d'attaque par piratage de mot de passe

- Prévenez la **personne responsable** au sein de votre entreprise.
- Contactez le **service** auquel appartient votre compte.
- Prévenez vos **contacts** via un autre canal.
- Changez et renforcez vos **mots de passe**, partout ailleurs.

Modifiez et renforcez (= rallongez) les **mots de passe** de tous vos comptes ; faites-le notamment si quelqu'un a eu ou a pu avoir accès à votre compte, par exemple si vos contacts disent avoir reçu des messages étranges de votre part. Modifiez aussi votre mot de passe si le service lié à votre compte a été confronté à une fuite de données. Vous éviterez ainsi que la personne qui a eu accès aux données puisse également usurper vos identifiants de compte. Le site www.haveibeenpwned.com vous permet de vérifier si votre adresse e-mail figure dans une base de données compromise.

- 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 !