Suivez l’exemple de Herstappe: Empêchez les cybercriminels d’entrer

Qu’est-ce que l’authentification à deux facteurs et pourquoi tout le monde devrait l’utiliser partout ?

CENTRE FOR CYBERSECURITY BELGIUM

febelfin

CYBER SECURITY COALITION

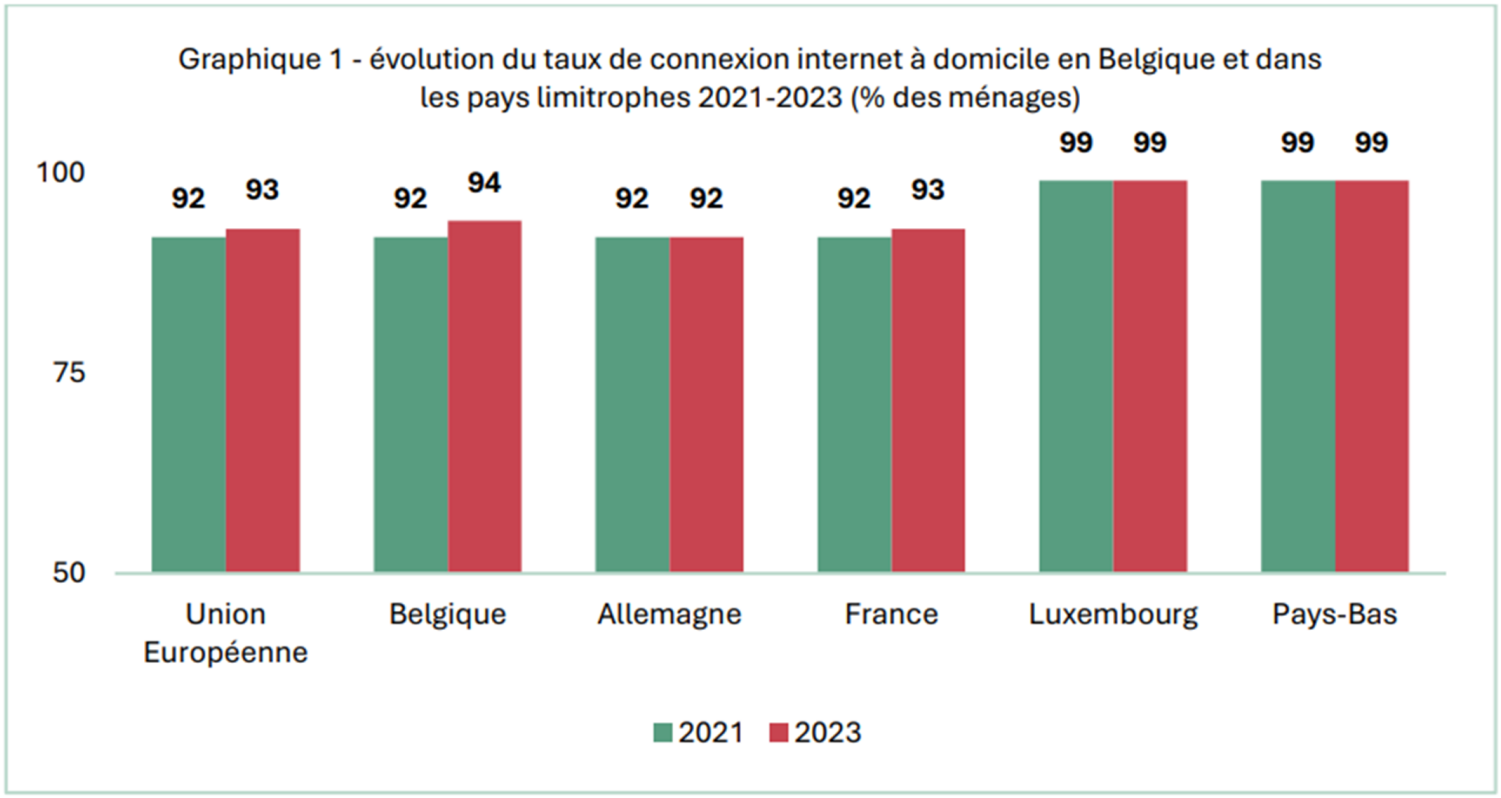
.be

Safeonweb.be

Qui peut encore passer à côté d'Internet ?

- Toutes les informations sont toujours à portée de main :
  - Heures d'ouverture
  - Bulletin météo
  - Itinéraires
- C'est pratique et rapide :
  - Les opérations bancaires peuvent être effectuées par voie numérique
  - Pas de file d'attente au guichet communal
  - Pas d'amende à la bibliothèque
  - Médecin, dentiste, pharmacien en un clin d'œil
- Vous êtes toujours en contact avec tout le monde :
  - La famille et les amis qui habitent loin sont désormais toujours un peu plus proches.
  - RDV rapide pour aller dîner ensemble

Internet est là pour rester



Source : calculs IACCHOS, UCLouvain, d'après les enquêtes Statbel 2021 et 2023.

Les cybercriminels se frayent également un chemin

- **Phishing, smishing**
  - Escroqueries par mails ou SMS suspects : vous donnez vos coordonnées bancaires ou transférez une somme sur le compte d'escrocs.
- **Piratage**
  - Les pirates ont accès à vos comptes (Facebook, mail, etc...), ils envoient des messages en votre nom, font des commandes en votre nom, etc....
- **Escroquerie aux investissements en crypto-monnaie**
  - Les escrocs vous encouragent à investir dans les crypto-monnaies par l'intermédiaire de fausses plateformes de trading.

Les cybercriminels se frayent également un chemin

- **Sextorsion**
  - L'escroc prétend posséder des images sexuellement explicites de vous. Il s'agit d'un bluff. Il menace de partager les images si vous ne payez pas.
- **Escroquerie Microsoft**
  - Vous recevez un appel d'une personne qui prétend être un employé de Microsoft, Apple ou Proximus. La personne prétend qu'il y a un problème avec l'appareil et veut vous aider, si vous payez.
- **Et de nombreuses autres formes de fraude en ligne se développent**

5 conseils pour se protéger en ligne

CENTRE FOR CYBERSECURITY BELGIUM
febelfin
CYBER SECURITY COALITION
.be
Safeonweb.be

5 conseils pour se protéger en ligne

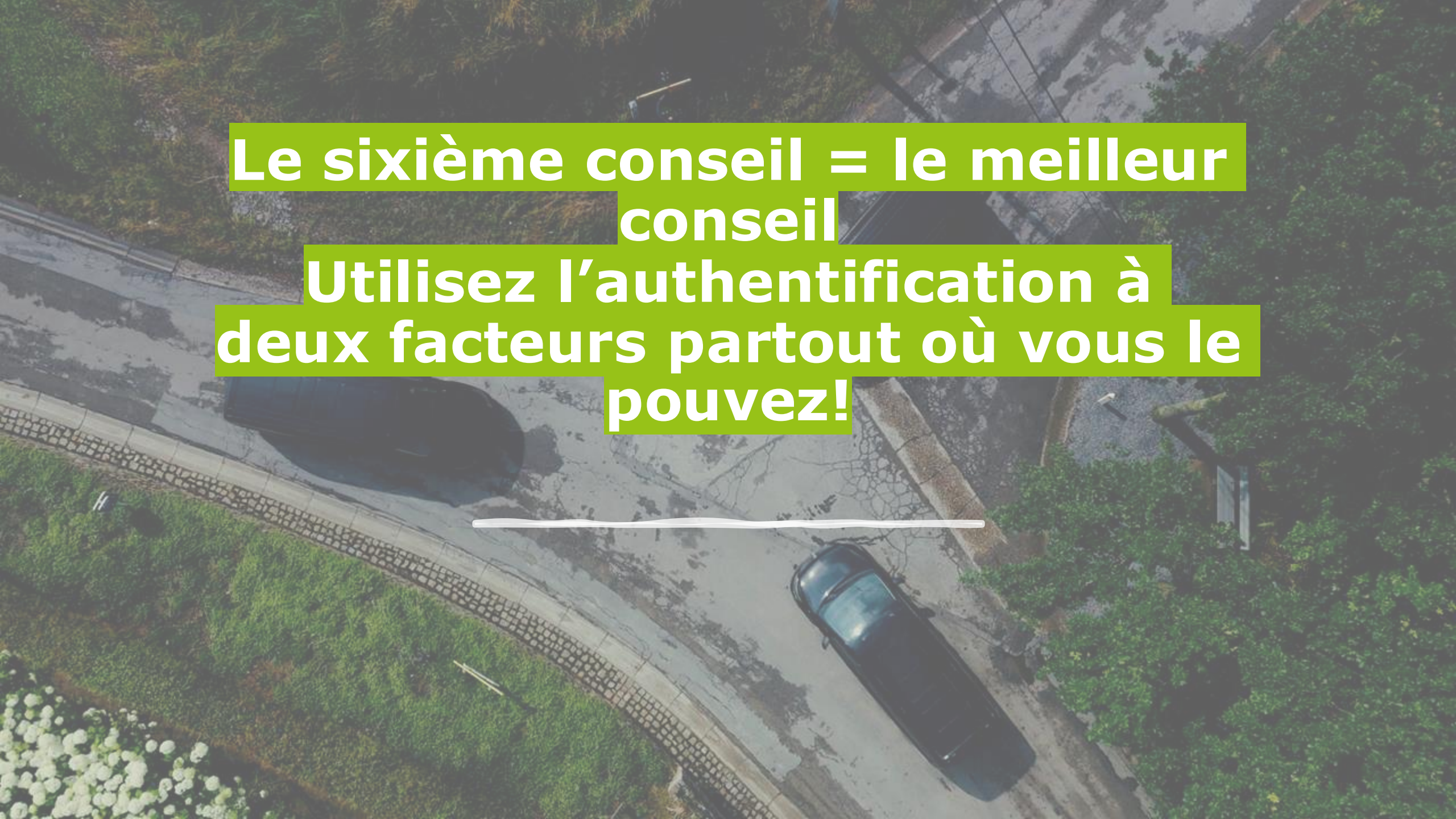
Apprendre à reconnaître le phishing

Télécharger uniquement à partir de stores reconnus

Faire des sauvegardes

Effectuer les mises à jour

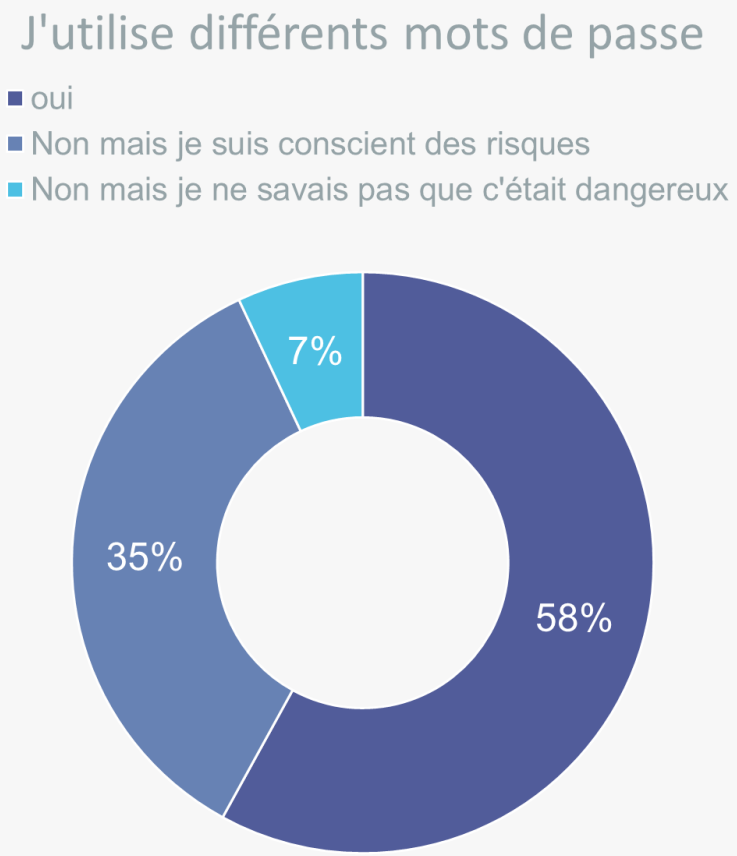
Utiliser un antivirus

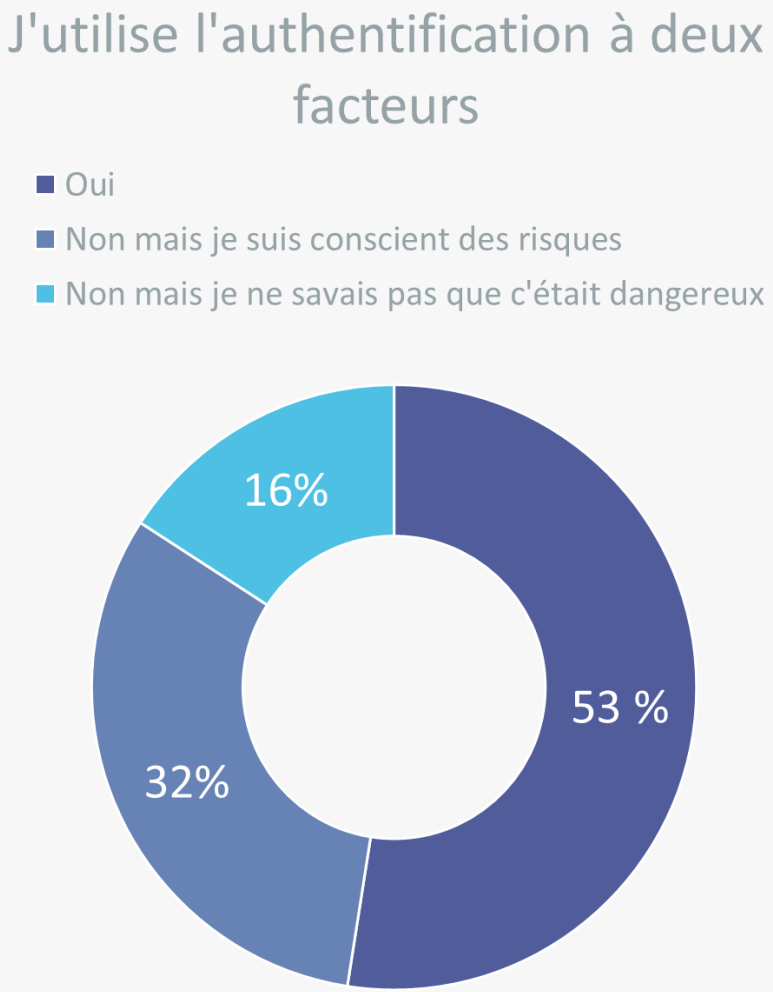

Le sixième conseil = le meilleur conseil
Utilisez l’authentification à deux facteurs partout où vous le pouvez!

https://www.youtube.com/watch?v=FHRBTfkvYnc&list=PLn1l55Gza9pwqGbsJIKy7OKOELUo1Oye0

Safeonweb.be

Quelques chiffres





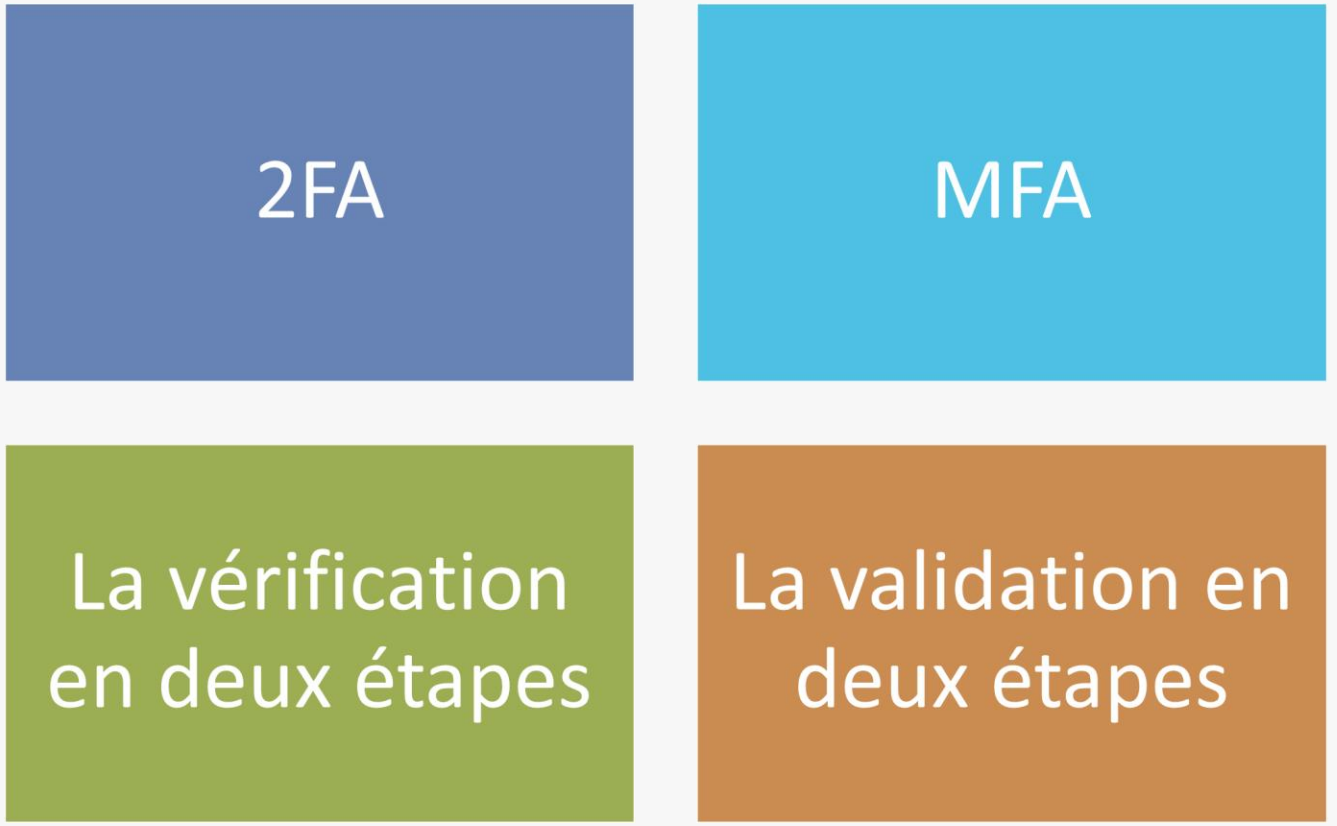
Quelques chiffres

- La 2FA permet de réduire de 99 % le piratage de comptes :
  - Les mots de passe volés par piratage sont inutiles avec l'utilisation de la 2FA.
  - Les logiciels malveillants et les virus ne peuvent plus avoir d'impact sur la sécurité des comptes utilisant la 2FA.
  - Les comptes paramétrés avec la 2FA ont un risque de piratage considérablement réduit.

- Two-Factor Authentication Statistics By Users, Industry, Adoption Rate and Benefits; 12/2023; https://www.enterpriseappstoday.com/stats/two-factor-authentication-statistics.html#:~:text=According%20to%20TechCrunch%2C%20Facebook%202FA,more%20than%201.5%20million%20accounts.&text=95%25%20of%20companies%20that%20used,benefits%20of%20software%2Dbased%20authentication

Safeonweb.be

L’authentification à deux facteurs ou …



Authentification quoi ? Qu’est-ce que la 2FA ?

Il s’agit d’une mesure de sécurité visant à empêcher les pirates ou les escrocs d’accéder à vos comptes en utilisant deux formes d’authentification différentes :

- Quelque chose que vous connaissez : mot de passe
- Ce que vous avez : smartphone
  - Code reçu par SMS,
  - Application (Itsme, Authenticator App, etc.),
- Ce que vous êtes : empreinte digitale, reconnaissance faciale, ...

Image : Kaspersky

Et la MFA alors?

Lorsqu’on utilise plus que 2 facteurs de protection on parle de Multi Factor Authentication ou MFA

Si seulement ils avaient utilisé l'authentification à 2 facteurs

MERCREDI 26 JUIN 2024 SUDINFO 7

FLOREFFE

LES PAGES DU « BAROMÈTRE » HACKÉES : LE PIRATE DEMANDE 250€ POUR LES RÉSERVATIONS

Le restaurant « Le Baromètre » à Floreffe a rouvert il y a quelques semaines après une courte pause. Mais le patron a des soucis avec les réservations. Il demande aux clients de lui sonner directement pour réserver afin d'éviter les arnaques en ligne.

Les lieux existent depuis sept ans. © F.B.

SHANTI DUPARQUE

La brasserie « Le Baromètre », situé rue Camille Giroul à Floreffe, a rouvert après une interruption hivernale.

Le chef, Christophe Delahaye, propose à nouveau ses plats préparés minute dans sa cuisine ouverte. Mais depuis deux mois, il galère un peu pour ses réservations. Pourtant, les clients sont toujours nombreux à vouloir venir chez lui.

Le souci se pose ailleurs : « Depuis presque deux mois, mon compte Facebook a été hacké par une personne malintentionnée qui répond à ma place aux demandes de réservation », commence le chef.

BESOIN D'UN PRO

« Au début, ce hacker demandait même aux clients de verser un acompte de 250 euros pour confirmer leur réservation. Heureusement, il n'avait pas laissé de numéro de compte donc personne ne s'est fait avoir »

Le chef tente de joindre quelqu'un chez Facebook pour régler le souci. « En fait, mon compte privé a été piraté et donc mes cinq pages commerces liés à celui-ci, comme celle du restaurant et de la chambre d'hôtes, sont aussi inaccessibles ».

Il précise à ses clients que pour réserver, la seule possibilité est de téléphoner au 081 45 16 91. « Et évidemment aucun acompte ne vous sera demandé ».

Le chef, un peu désemparé, en profite pour lancer un appel : « Si vous avez des solutions ou l'expérience pour récupérer un compte piraté, vous pouvez me contacter sur la ligne fixe, bien évidemment », précise le restaurateur. ■

Piratage chez Ticketmaster : attention si vous avez utilisé cette plateforme, voici les mesures à prendre contre le vol de votre argent

100 millions de mots de passe volés et publiés en ligne. Voici comment vérifier si les vôtres en font partie

6 LA MEUSE MERCREDI 21 FÉVRIER 2024

LIÈGE

La messagerie de Willy Demeyer piratée

On a beau être bourgmestre d'une des plus grandes villes du pays, on n'est pas à l'abri d'une usurpation d'identité. Willy Demeyer, le bourgmestre de Liège, vient d'en faire les frais.


Willy Demeyer est victime d'une usurpation d'identité. © MT

Des mails d'amis « coincés à l'étranger », privés de tous leurs papiers d'identité et de leurs cartes bancaires, ou de services, publics ou privés, qui réclament le montant d'une facture impayée, tout le monde en a déjà reçu. Et chacun sait donc que verser de l'argent pour les aider à se tirer d'affaires est tout sauf une bonne idée. Mais quand ce mail émane du bourgmestre de Liège et arrive sur la messagerie d'un Liégeois, ça pourrait prêter à confusion. Sauf que ce n'est évidemment jamais le bourgmestre qui se charge des rappels des paiements…

C'est pourtant ce qui risque d'arriver dans les prochains jours. Mais sur le sujet, M. Demeyer est clair : « Si on vous demande de l'argent à mon nom, merci de ne rien me verser. Mon compte a été piraté. »

Selon les premiers éléments, il semblerait qu'un escroc ait créé une adresse mail au nom du bourgmestre. Et s'en serve donc maintenant pour réclamer des versements. Une usurpation d'identité donc, conte laquelle le bourgmestre lui-même a voulu mettre en garde. ■

G.W.

Safeonweb.be

Pourquoi protéger vos comptes en ligne?

Les cybercriminels qui ont accès à vos comptes :

- Peuvent vous faire vivre un **cauchemar financier**
  - accès à vos comptes de paiement en ligne
  - achats en votre nom
  - fraude en votre nom
- Peuvent prendre le contrôle de votre **identité en ligne**
  - Atteinte à la réputation
  - Escroquerie de vos amis et de votre famille en votre nom
  - Accès aux informations personnelles

Comment savoir si mon compte a été piraté ?

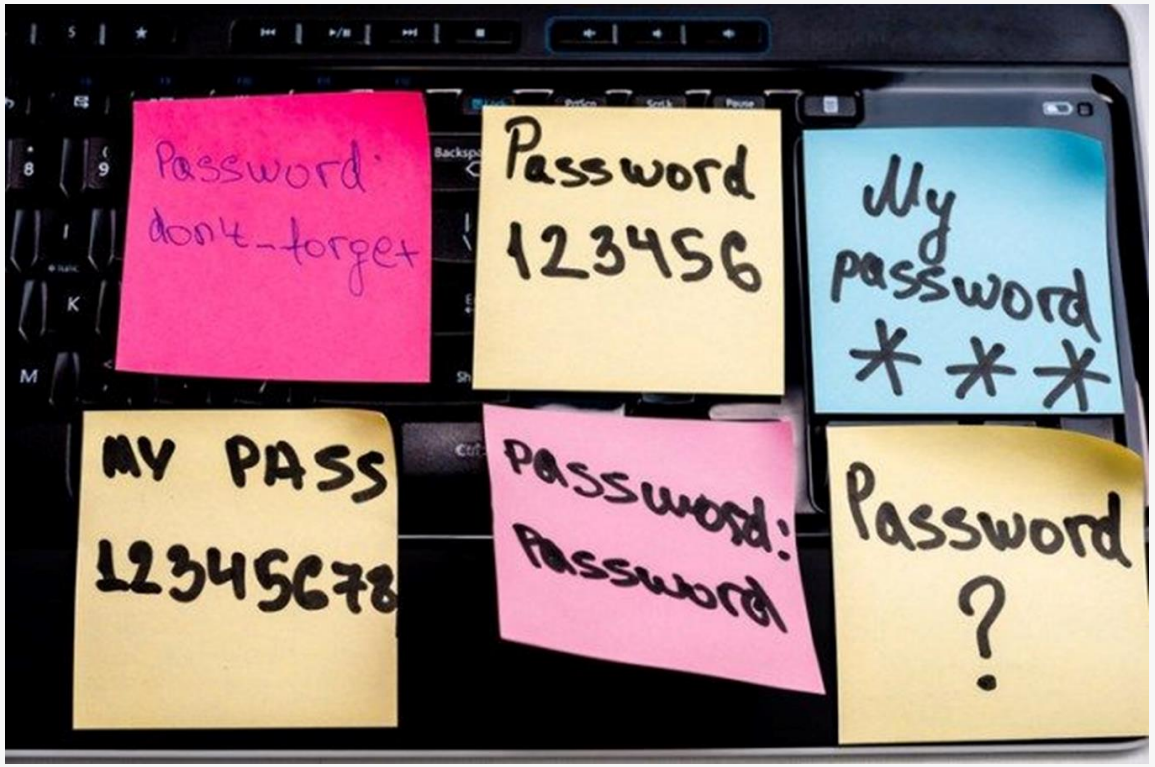
- Vous recevez un mail qui indique une connexion avec un nouvel appareil
- Vous constatez des activités suspectes: ex: derniers films vus sur Netflix
- Vos amis vous disent avoir reçu un mail étrange de votre part
- Vous constatez un paiement frauduleux sur votre compte
- Des publications étranges apparaissent sur vos réseaux sociaux

Mon compte est piraté, que faire ?

- Comment retrouver le contrôle de votre compte ?
  - Vous avez encore accès à votre compte ? Modifiez alors immédiatement le mot de passe de ce compte et de tous vos autres comptes.
  - Vous n'avez plus accès à votre compte ? Utilisez les options de restauration pour retrouver l'accès et modifiez ensuite tous vos mots de passe.
- Que faire de plus ?
  - Scannez votre ordinateur à la recherche de virus.
  - Si vos données bancaires ont été volées, avertissez votre banque et contactez Card Stop au 078 170 170 si vous constatez des transactions suspectes.
- Si des données professionnelles ont été volées, avertissez au plus vite votre employeur.
- Activez la 2FA

Les mots de passe sont dépassés

- Les mots de passe sont frustrants
- Nous continuons à utiliser des mots de passe faibles
- Mais même les mots de passe forts ne sont pas sûrs...



50 Most Commons Passwords 2024

Safeonweb.be

Même un mot de passe fort n’est pas sûr

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Comment les pirates informatiques volent-ils votre mot de passe ?

- Ils volent votre mot de passe par le biais du **phishing** ou de faux messages.
- Une **fuite de données** dans un service en ligne d'une entreprise pourrait laisser votre mot de passe à la portée de tous sur internet.
- Avec les **virus** qui volent les mots de passe

Nous facilitons la tâche des pirates informatiques !

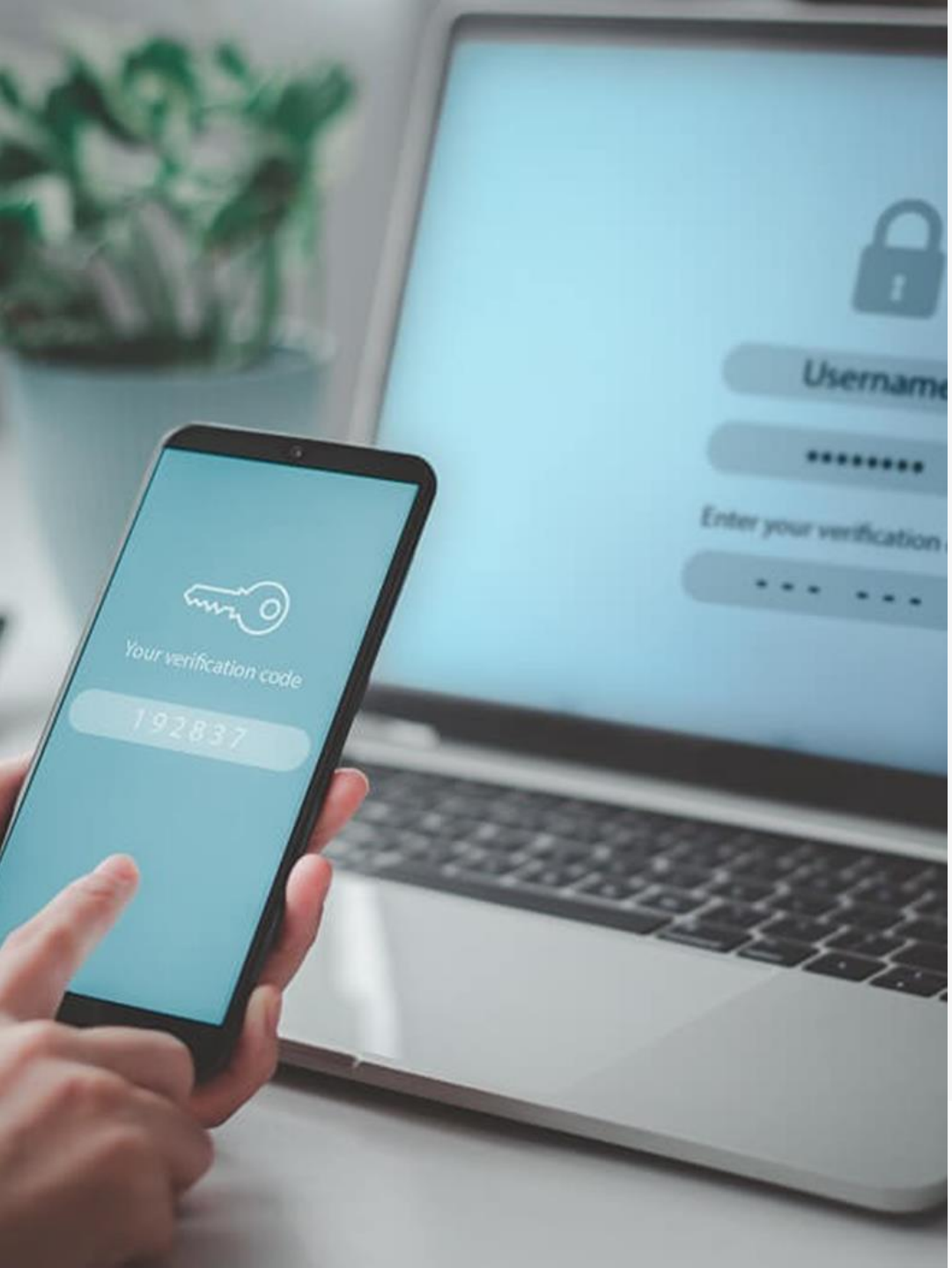
- Nous écrivons les mots de passe sur des post-it
- Nous révélons les mots de passe au téléphone
- Nous donnons un mot de passe lors d'un faux concours en ligne

Comment éviter cela ?

Utiliser l’authentification à deux facteurs lorsque c’est possible

- Commencez par votre compte mail
- Activez-la sur les sites web où vous laissez vos coordonnées bancaires : sites d’achats en ligne, site de réservation de location de vacances, site de réservation de tickets, site de revente, …
- Protégez vos médias sociaux avec la 2FA

Bref, prenez l’habitude de l’utiliser partout où elle est disponible



Comment activer la 2FA ?

L'activation de la 2FA varie d'une plateforme à l'autre, mais les étapes sont généralement assez similaires :

- Accédez aux paramètres de sécurité du compte que vous souhaitez sécuriser.
- Recherchez l'option permettant d'activer la 2FA et sélectionnez-la.
- Choisissez le deuxième facteur que vous souhaitez utiliser (par exemple, SMS, application d'authentification, etc.).
- Suivez les instructions à l'écran pour configurer le deuxième facteur.
- Testez si tout est configuré correctement en vous déconnectant et en vous connectant à nouveau avec le deuxième facteur.

Quel est le meilleur deuxième facteur?

- Le deuxième facteur que vous utilisez n'a pas d'importance*. Deux facteurs de sécurité valent toujours mieux qu'un seul.
- Utilisez deux types de facteurs différents, et non pas, par exemple, deux fois quelque chose que vous connaissez.

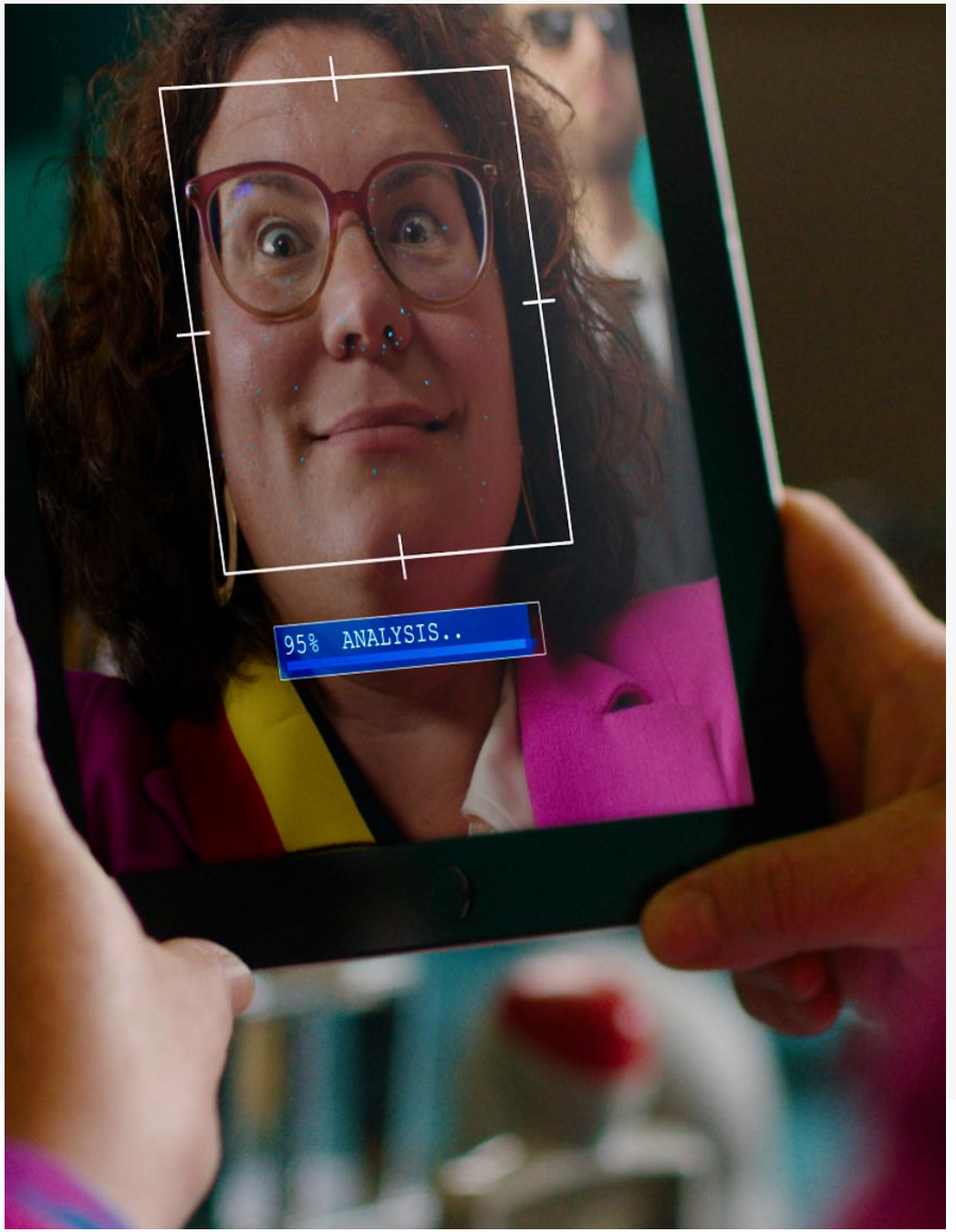
- ** Un code envoyé par SMS est facile à obtenir et ce système est généralement bien connu. C'est peut-être la solution la plus accessible, mais... les escrocs essaient de l'obtenir en échangeant la carte SIM. Si l'escroc parvient à s'emparer de votre téléphone et qu'il n'est pas verrouillé ou qu'il affiche les messages même lorsqu'il est verrouillé, il peut alors utiliser le code...*

SMS ou application d’autentification?

- Application Authenticator : vous téléchargez une application via App Store ou Google Play (par exemple Google Authenticator ou Microsoft Authenticator). Via un code QR, vous ajoutez le compte à votre application. Chaque fois que vous vous connectez, l’application génère un code à usage unique que vous insérez à l’endroit indiqué.
- SMS : vous entrez votre numéro de téléphone et vous recevez un SMS contenant un code que vous devez saisir à l’endroit indiqué.
- C’est un choix libre (en fonction de la maturité du public cible)
- Important: ne jamais partager les codes!!!

Vous avez des doutes ?

- Voir comment utiliser la 2FA sur les comptes les plus couramment utilisés sur Safeonweb
- https://safeonweb.be/fr/2FA
- Demandez de l'aide à quelqu'un à qui vous faites confiance: un membre de la famille, des amis ou les Espaces Publics Numériques (EPN)



Safeonweb.be

Excuses stupides pour ne pas utiliser la 2FA

- Je perds trop de temps avec ça !
  - Quelques secondes seulement. Négligeable par rapport au temps que l'on perd en cas de piratage.
- Et si je perds mon téléphone ?
  - Vous pouvez toujours saisir une adresse électronique de récupération, ou récupérer et enregistrer des codes.

Une mauvaise idée

- Si j'utilise un deuxième facteur, puis-je choisir un mot de passe faible ?
  - Ce n'est pas une bonne idée. L'idée est de choisir deux méthodes sûres. Un mot de passe faible n'est jamais une bonne idée.

Si l’authentification à deux facteurs (2FA) n’est pas disponible pour un service particulier

- Assurez-vous que votre mot de passe est complexe et différent des mots de passe utilisés pour d’autres comptes.
- Vérifiez régulièrement votre compte pour détecter toute activité inhabituelle ou tout accès non autorisé.
- Mettez en place des notifications pour les activités du compte, telles que les connexions ou les modifications de paramètres.
- Utilisez les autres fonctions de sécurité fournies par le service, telles que les questions de sécurité ou les options de récupération de compte.
- Envisagez de passer à un fournisseur de services qui offre des fonctions de sécurité robustes, y compris la 2FA.
- Contactez le fournisseur de services actuel pour lui faire part de votre intérêt pour la 2FA ou pour vous renseigner sur les autres options de sécurité qu’il propose.

Est-il impossible de hacker la 2FA?

- Les escrocs peuvent également essayer d'obtenir votre deuxième facteur de protection :
  - en vous appelant et en utilisant une excuse pour vous convaincre de partager votre code ou d'utiliser Itsme (pour une authentification que l'escroc a lui-même demandée !)
  - En vous envoyant un message de phishing
  - En volant votre téléphone et en vous demandant les codes qui s'y trouvent

- Ne partagez donc jamais vos codes avec quelqu'un qui vous les demande !

En savoir plus sur la 2FA ?

https://safeonweb.be/fr

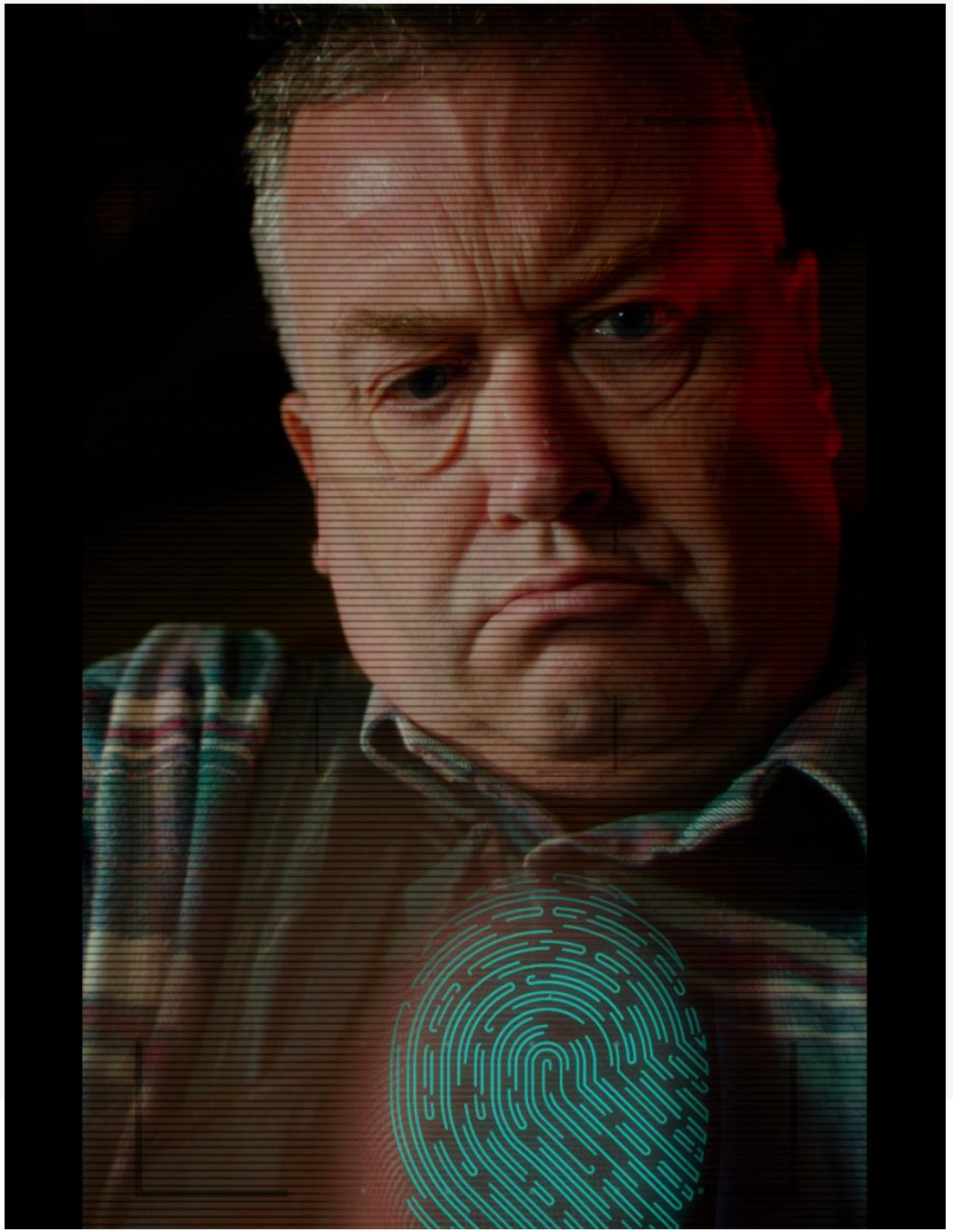
Suivez-nous !

Facebook - Safeonweb.be

Instagram - Safeonweb.be

X – Safeonweb

YouTube - @safeonwebbe



Safeonweb.be

Cette présentation vous est offerte par Safeonweb dans le cadre de la campagne 2024

CENTRE FOR CYBERSECURITY BELGIUM

febelfin

CYBER SECURITY COALITION

.be

Safeonweb.be