01 oct 2020 -11:00

Les mots de passe, c’est dépassé. Passez à l’authentification à deux facteurs(2FA)

Les mots de passe nous rendent □□□□! Imaginer, retenir et utiliser des mots de passe, c’est ennuyeux, frustrant, chronophage et en plus pas sécurisé à 100% puisque même le mot de passe le plus sûr peut être dérobé et utilisé à mauvais escient. Autant de raisons pour le Centre pour la Cybersécurité Belgique (CCB) de mener une campagne pour promouvoir une meilleure sécurisation des comptes !

Dans le cadre du *European Cyber Security Month*, le Centre pour la Cybersécurité Belgique (CCB) et la Cyber Security Coalition lancent pour la sixième fois une campagne de sensibilisation sur la cybersécurité. Cette année, ces deux organisations souhaitent encourager les internautes à sécuriser leurs comptes à l’aide de l’authentification à deux facteurs.

Les comptes en ligne (par exemple : e-mail, réseaux sociaux, internet banking et magasins en ligne) sont généralement sécurisés à l’aide d’un nom d’utilisateur et d’un mot de passe. Hélas, les internautes choisissent souvent des mots de passe faciles à retenir sans compter qu’ils utilisent régulièrement le même mot de passe pour plusieurs comptes. Si une personne extérieure accède à l’un de ces comptes, elle peut se faire passer pour le propriétaire et utiliser ce compte à mauvais escient.

> "Nous conseillons donc à tous les utilisateurs d’activer autant que possible l’authentification à deux facteurs, d’utiliser différents mots de passe et de les gérer via un gestionnaire de mots de passe en ligne. En ce qui me concerne, je ne connais qu’un seul mot de passe : celui de mon gestionnaire de mots de passe ! Ce gestionnaire conserve tous mes mots de passe. Il a généré en outre des mots de passe sûrs de plus de 20 signes pour tous mes comptes, que je n’ai jamais à connaître et encore moins à retenir."
>
> Miguel De Bruycker
> Directeur du CCB

> "Dans un contexte professionnel, nous conseillons également d'imposer l'authentification à deux facteurs à tous les collaborateurs, afin d'éviter que les cybercriminels puissent s'introduire dans les réseaux internes par une simple attaque de phishing"

Jan Deblauwe
Président de la Cyber Security Coalition Belgium

En chiffress

- En 2019, des mots de passe faibles ont été à l'origine d'environ 30 % de toutes les infections causées par un ransomware. (https://www.precisesecurity.com/articles/weak-passwords-caused-30-of-ransomware-infections-in-2019/)
- 1 seconde : le temps nécessaire pour pirater un mot de passe de 4 signes
- 1 semaine : le temps nécessaire pour pirater un mot de passe fort de 10 signes.
- Dans l'état actuel des technologies, un pirate informatique prendra des siècles pour pirater un mot de passe de 13 signes. C'est pour cette raison que les pirates essaient plutôt de dérober les mots de passe… ou de les découvrir en faisant usage de la ruse (phishing, smishing, scam…) (https://www.grc.com/haystack.htm)
- 15 % des internautes utilisent le même mot de passe pour tous leurs comptes et 53 % quelques mots de passe. Seuls 32 % d'entre eux utilisent de nombreux mots de passe différents (Indice de santé digitale, nov. 2019)

Résultats de notre enquête sur l'utilisation de l'authentification à deux facteurs, août 2020

- 30 % des internautes utilisent un gestionnaire de mots de passe et 40 % utilisent l'authentification à deux facteurs lorsque c'est possible.
- 33 % d'entre eux n'ont jamais entendu parler de l'authentification à deux facteurs ou 2FA

- Ceux qui connaissent bel et bien l'authentification à deux facteurs ne l'utilisent souvent pas parce qu'ils ne savent pas que la fonctionnalité existe. Par exemple, 57 % des utilisateurs de Facebook ne savent pas qu'il peuvent avoir recours à l'authentification à deux facteurs ou comment activer cette fonctionnalité. Le même constat vaut pour Twitter et Instagram.
- La méthode de l'authentification à deux facteurs la plus utilisée est l'envoi d'un sms avec un code (89 %), suivi par une application d'authentification comme Itsme ou Google Authenticator (80 %) et un token (70 %), puis la méthode biométrique (empreinte digitale ou reconnaissance faciale) (56 %).

Oubliez ce mot de passe !

Utiliser des mots de passe, c'est frustrant. Il faut constamment trouver de nouveaux mots de passe qui doivent contenir tout un arsenal de signes différents (signes spéciaux, majuscules, minuscules, chiffres) et être suffisamment longs. Tellement longs qu'il faut souvent s'y prendre plusieurs fois avant d'encoder le mot de passe sans faute de frappe. Et ainsi de suite. La galère.

Si la plupart des internautes se rendent bien compte qu'un mot de passe court et simple n'a rien de sûr, nous remarquons pourtant que les mots de passe faibles restent une réalité. 123456, azerty, motdepasse, un prénom, une équipe préférée, « loulou » ou « pokemon » : voici quelques mots de passe tirés du top 30 des mots de passe les plus utilisés en Belgique. Plus un mot de passe est court et simple, plus un pirate informatique le découvrira rapidement.

Top 30 des mots de passe les plus utilisés en Belgique (2015-2020)

123456	computer
azerty	thomas
123456789	mercedes
12345	charlotte
azertyuiop	standard
wachtwoord	vergeten
abc123	unknown
pokemon	nicolas
azerty123	lol123
password	nathalie

voetbal	snoopy
12345678	motdepasse
anderlecht	bolleke
sloeber	1234567890
loulou	isabelle

SOURCE: Scattered Secrets

> "Les mots de passe sont les clés de votre logement virtuel. Elles peuvent donc même permettre d'accéder au coffre-fort. Conservez-les donc précieusement."
>
> Olivier Bogaert
> Federal Computer Crime Unit

Frustrant, et pourtant même pas sûr à 100 %

Utiliser des mots de passe sûrs est un must absolu... mais ils ne vous permettent pas pour autant de dormir sur vos deux oreilles. Même les mots de passe sûrs peuvent être dérobés.

- Les criminels essaient de vous mener en bateau pour dérober votre mot de passe à l'aide d'un mail de phishing. Ils essaient ainsi par exemple de vous convaincre d'encoder votre mot de passe sur un faux site Internet qui leur permettra de tout simplement lire votre mot de passe.
- Nous ne sommes pas non plus à l'abri des fuites de données. Une plateforme que vous utilisez, comme LinkedIn ou Facebook, peut se faire pirater et toutes les données des utilisateurs être dérobées, dont les mots de passe.

Parfois, nous facilitons la tâche des pirates informatiques :

- en laissant des mots de passe sur un Post-it accroché à l'écran ;

- en dévoilant des mots de passe au téléphone à une personne qui se fait passer pour un collaborateur de Microsoft ;
- en encodant des données pour participer à l'un ou l'autre questionnaire ou concours ;
- en conservant les mots de passe sur notre ordinateur, dans un document intitulé « mots de passe » ;
- etc.

Il est absolument essentiel d'utiliser des mots de passe sûrs, mais nous recommandons aussi d'ajouter une couche de sécurité supplémentaire : l'authentification à deux facteurs (2FA).

La solution ? L'authentification à deux facteurs (2FA) !

La solution ? L'authentification à deux facteurs (2FA) !

L'authentification à deux facteurs, la vérification en deux étapes ou, tout simplement, la 2FA est une solution simple pour mieux protéger vos données. Pour accéder à votre compte, vous devez prouver que vous êtes bien la personne que vous prétendez être. Cela peut se faire de 3 manières ou à l'aide de 3 facteurs :

- avec un élément que vous seul connaissez (votre mot de passe ou votre code PIN),
- avec un élément que vous seul détenez (votre téléphone ou votre token),
- avec un élément qui fait partie de vous (votre empreinte digitale, votre visage, votre iris...).

Généralement, vous utilisez l'un de ces facteurs pour prouver qui vous êtes, mais il est préférable d'utiliser 2 facteurs ou plus : on parle alors d'authentification à deux facteurs ou d'authentification multifactorielle (2FA ou MFA). Vous pouvez par exemple utiliser un mot de passe et faire envoyer un code à votre téléphone portable, ou utiliser votre empreinte digitale et un code pour accéder à votre compte.

> "Pour un hacker, il n'y a rien de plus frustrant que de constater, après l'euphorie du piratage d'un mot de passe, que la cible a activé la 2FA"
>
> Inti De Ceukelaire
> Ethical Hacker

Faisons campagne ensemble !

Faisons campagne ensemble !

Tout au long de la campagne d'octobre, nous souhaitons attirer l'attention du public sur le thème à l'aide de spots radio, de vidéos sur les médias sociaux, de bannières et autres matériels de campagne. Le site Internet de la campagne https://campagne.safeonweb.be/fr regorge de conseils et informations utiles. L'Indice de sante digitale y est également disponible, pour tester ses connaissances en cybersécurité. Tout le matériel de campagne est téléchargeable sur le site https://safeonweb.be/fr/materiel-de-campagne.

> "Nous sommes très reconnaissants envers tous nos partenaires qui ont contribué au message de la campagne. La campagne bénéficie du soutien de services publics fédéraux, d'institutions académiques, de petites et grandes entreprises, mais aussi d'ASBL et autres organisations. Cette année encore, plus de 500 partenaires nous aideront à diffuser le matériel de campagne"
>
> Phédra Clouner
> Directrice Adjointe du CCB

Centre pour la Cybersécurité Belgique
Rue de la Loi 16
1000 Bruxelles
Belgique
http://www.ccb.belgium.be

Andries Bomans
Responsable communication
+32 471 66 00 06
andries.bomans@ccb.belgium.be

Katrien - Eggers
Responsable communication
+32 485 76 53 36
katrien.eggers@cert.be