



La lettre d'information mensuelle sur la sensibilisation à la sécurité pour vous

Comment ruiner la journée d'un attaquant ? Avec l'authentification multifactorielle (MFA) !

Si c'est facile pour vous, c'est facile pour un attaquant

James se reposait chez lui lorsqu'il a commencé à recevoir plein de notifications. Le mot de passe de son compte de messagerie personnel avait été changé, mais il ne se souvenait pas avoir fait cette démarche. Peu de temps après, ses comptes de réseaux sociaux ont reçu la même notification, l'alertant que ses mots de passe avaient été changés, puis sa banque l'a prévenu que des achats suspects étaient en cours. En panique, James a essayé de se connecter à ses mails, mais son mot de passe ne fonctionnait plus. Quelqu'un l'avait expulsé de son compte ! Au cours des jours suivants, James a passé des heures entières à essayer de récupérer ses comptes, à contester des prélèvements et à changer ses mots de passe. Ce qu'il ne comprenait pas, c'est qu'il avait tout fait comme il fallait. Il avait utilisé un mot de passe fort qu'il n'avait jamais partagé avec qui que ce soit !

Mais son mot de passe n'était pas le problème : c'était de se fier uniquement à son mot de passe. Ce dont James ne s'est pas rendu compte, c'était que le message urgent qu'il avait reçu la semaine passée ne provenait pas de son fournisseur de messagerie mais d'un cyber-criminel, qui l'avait piégé pour récupérer son mot de passe. Une fois que le cyber-criminel a obtenu le mot de passe personnel du compte mail de James, il avait le contrôle total de son compte. Non seulement il avait accès à tous les mails de James, mais il pouvait également recevoir la confirmation nécessaire pour modifier les mots de passe de ses autres comptes.

La sœur de James, Ariel, a reçu le même message, et comme son frère, elle a été piégée, a cliqué sur le lien malveillant et a entré son mot de passe. Cependant, contrairement à James, Ariel avait mis en place l'authentification multifactorielle (MFA) pour protéger son compte mail. Cela signifiait qu'il manquait le deuxième facteur d'authentification à l'attaquant pour se connecter, en plus du mot de passe, et qu'il avait passé une journée frustrante à essayer de se connecter en vain. Ariel a bloqué l'attaquant, sécurisé son compte mail, et a passé une bien meilleure journée que James. Peu de temps après, elle a aidé son frère à mettre en place la MFA pour qu'il puisse lui aussi ruiner la journée d'un cyber-attaquant.

Qu'est-ce que l'authentification multifactorielle (MFA) ?

L'authentification multifactorielle, ou MFA, est un moyen simple et gratuit d'ajouter un niveau de sécurité supplémentaire à vos comptes. Au lieu de se contenter de votre mot de passe, l'authentification multifactorielle (MFA) ajoute une deuxième étape (ou un deuxième facteur) pour vérifier que c'est bien vous. Avec l'authentification multifactorielle (MFA), la connexion nécessite généralement au moins deux des éléments suivants :

- **Quelque chose que vous connaissez** : votre mot de passe
- **Quelque chose que vous avez** : un code unique envoyé à votre téléphone ou généré par une application
- **Quelque chose que vous êtes** : une empreinte digitale ou une reconnaissance faciale

Même si un cybercriminel parvient à voler votre mot de passe, il ne pourra pas accéder à votre compte sans ce deuxième facteur d'authentification. C'est pour cette raison que l'activation de l'authentification multifactorielle (MFA) est souvent considérée comme **la mesure la plus importante que vous puissiez prendre pour sécuriser vos comptes**.

Comment utiliser la MFA de la bonne manière

La bonne nouvelle, c'est que l'authentification multifactorielle (MFA) est simple à utiliser et largement répandue. La plupart des principaux services (messagerie électronique, services bancaires, réseaux sociaux et sites de vente en ligne) proposent cette fonctionnalité gratuitement. Mieux encore, il suffit souvent de se connecter une seule fois avec l'authentification multifactorielle (MFA) pour chaque site. Par la suite, le site identifie et mémorise votre navigateur, ce qui rend l'authentification non seulement plus sûre, mais aussi plus simple. Voici comment commencer :

1. Activez l'authentification multifactorielle (MFA) pour vos comptes importants : commencez par vos comptes les plus critiques : messagerie électronique, comptes bancaires, placements et tout autre compte important. N'oubliez pas que si quelqu'un parvient à accéder à votre messagerie, il peut souvent réinitialiser les identifiants de vos autres comptes.

2. Utilisez une application d'authentification lorsque cela est possible : l'un des moyens les plus courants d'obtenir votre deuxième facteur d'authentification consiste à recevoir un code unique par SMS sur votre téléphone. Cependant, l'utilisation d'une application d'authentification dédiée constitue une méthode encore plus sûre et plus fiable. Une application d'authentification est une application mobile que vous installez sur votre téléphone et qui génère des codes à usage unique que vous pouvez utiliser, au lieu de les recevoir par SMS.

3. Associez l'authentification multifactorielle (MFA) à des mots de passe forts : la MFA est très efficace, mais elle fonctionne mieux lorsqu'elle est associée à des mots de passe forts et uniques. En plus de l'authentification multifactorielle (MFA), utilisez toujours un mot de passe fort et unique pour chacun de vos comptes. Si certains sites vous demandent si vous souhaitez activer les Passkeys pour votre compte, sachez qu'un Passkey n'est rien d'autre qu'une version très sécurisée de l'authentification multifactorielle (MFA).

4. Protégez vos appareils mobiles : votre appareil mobile est désormais indispensable à la mise en œuvre de l'authentification multifactorielle (MFA) et peut également héberger votre gestionnaire de mots de passe ; à bien des égards, il détient toutes les clés de votre royaume. Assurez la sécurité de votre appareil mobile en activant le verrouillage de l'écran et les mises à jour automatiques.

Prenez le contrôle de votre sécurité

L'activation de l'authentification multifactorielle (MFA) est l'un des moyens les plus efficaces de vous protéger en ligne. N'attendez pas que vos comptes soient piratés, comme ceux de James. Faites comme Ariel, et faites en sorte que ce soit l'agresseur qui passe une mauvaise journée.

Rédacteur invité

Betta Lyon Delsordo, testeuse d'intrusion chez AWS, est spécialisée dans la sécurité des applications, du cloud et de l'IA. Elle est titulaire d'un master en cybersécurité de Georgia Tech et détient la certification GPEN. Betta a notamment pris la parole lors de la DEF CON, à la Banque mondiale, à la WiCyS, ainsi qu'à des conférences organisées aux États-Unis et dans l'Union européenne.



Ressources

Comment les cybercriminels volent vos mots de passe : <https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions>

Le pouvoir des phrases de passe : <https://www.sans.org/newsletters/ouch/power-passphrase-why-longer-beats-smarter>

Le pouvoir des gestionnaires de mot de passe : <https://www.sans.org/newsletters/ouch/stop-password-pain-reliable-password-manager>

Traduit pour la communauté par : Juliette Busson

OUCH ! Publié par SANS Security Awareness et distribué sous [licence Creative Commons BY-NC-ND 4.0](#). Vous êtes libre de partager ou de distribuer cette newsletter à condition de ne pas la vendre ni la modifier. Comité de rédaction : Phil Hoffman, Leslie Ridout, Princess Young.

Vous pouvez trouver plus de contenu OUCH! Sur le lien suivant : <https://www.sans.org/newsletters/ouch>