OUCH!

SANS SECURITY AWARENESS

Le bulletin mensuel de sensibilisation à la sécurité pour vous

Simplifier les mots de passe

Aperçu

On vous dit souvent que vos mots de passe sont la clé pour protéger vos comptes (à juste titre !), mais il est rare qu'on vous explique comment créer et gérer vos mots de passe de manière sécurisée. Ci-dessous, nous couvrons trois étapes pour simplifier vos mots de passe, fermer vos comptes et protéger votre futur.

Phrases de passe

L'ère des mots de passe dingues et compliqués est révolue. Ces mots de passe sont difficiles à mémoriser et à taper. Avec les ordinateurs ultra rapides de nos jours, ils sont faciles à craquer pour un cyber attaquant. La clé est de créer des mots de passe longs. Le plus de caractères il y aura, le mieux ce sera. C'est ce qu'on appelle des phrases de passe, un type de mot de passe long qui utilise des phrases courtes ou des mots au hasard. Voici deux exemples

C'est l'heure du café !

perdu-escargot-rampe-plage

Ces deux exemples sont forts, avec plus de vingt caractères, faciles à mémoriser et à taper, mais difficiles à craquer. Vous allez bien entendu rencontrer des sites ou des situations où vous devrez ajouter des symboles, des chiffres ou des majuscules. Souvenez-vous juste que c'est la longueur qui compte.

Gestionnaire de mots de passe

Vous devez avoir un mot de passe unique pour chacun de vos comptes. Si vous réutilisez le même mot de passe pour différents comptes, vous vous mettez en danger. Tout ce qu'un cyber attaquant a à faire est de pirater un site web que vous utilisez, voler tous les mots de passe (le vôtre inclus), puis utiliser votre mot de passe pour se connecter à vos autres comptes. Cela arrive plus régulièrement que l'on croit. Vous n'y croyez pas ? Vérifier sur ce site www.haveibeenpwned.com pour voir quels sites vous utilisez ont été piratés et donc vos mots de passe potentiellement compromis. Alors, que pouvez-vous faire ? Utilisez un gestionnaire de mots de passe.

Ce sont des programmes spéciaux qui stockent tous vos mots de passe de manière sécurisée dans un coffre chiffré. Vous n'avez à vous rappeler que d'un mot de passe, celui du gestionnaire. Le gestionnaire de mots de passe récupère vos mots de passe automatiquement quand vous en avez besoin et vous identifie sur les sites à votre place. Ils ont aussi d'autres utilités, comme stocker les réponses aux questions secrètes, vous prévenir quand vous réutilisez un mot de passe, générer des mots de passe pour vous assurer que vous en utilisiez des forts, et pleins d'autres fonctions. La plupart des gestionnaires de mots de passe se synchronisent avec presque tout ordinateur ou appareil, donc qu'importe le système utilisé, vous avez un accès simple et sécurisé à tous vos mots de passe.

Finalement, prenez soin d'écrire le mot de passe de votre gestionnaire et rangez-le dans un lieu secret à la maison. Certains gestionnaires de mot de passe vous laissent imprimer un kit de récupération du gestionnaire. Donc, si vous oubliez le mot de passe de votre gestionnaire, vous avez une solution alternative. Ou encore, si vous êtes malade ou dans une urgence, votre concubin(e) ou un membre de votre famille pourra récupérer l'information à votre place.

La vérification à deux étapes

La vérification à deux étapes (aussi appelée identification à deux facteurs ou à multiples facteurs) ajoute une couche de sécurité supplémentaire. Cela requiert deux choses pour vous connecter à vos comptes : votre mot de passe et un code numérique généré par votre appareil mobile ou envoyé sur votre téléphone. Cette procédure vous assure que même si un cyber attaquant vole votre mot de passe, il ne pourra pas accéder à vos comptes. La vérification à deux étapes est facile à mettre en place et vous n'avez généralement qu'à l'utiliser une fois lors de la première connection depuis un nouvel appareil. Mettez-la en place dès que possible, surtout pour vos comptes importants comme votre banque, caisse de retraite ou l'accès à votre messagerie. Si vous utilisez un gestionnaire de mots de passe, nous recommandons de le protéger avec une phrase de passe ET une vérification à deux étapes.

Cela peut paraître superflu, mais ces trois étapes simples peuvent vous aider à conserver votre emploi, réputation et futur financier.

Rédacteur Invité

Justin Henderson *(@SecurityMapper) est co-fondateur de H & A Security Solutions, instructeur certifié de SANS Institute et auteur pour les formations SANS Cyber Defense et SIEM. Il aime tout ce qui touche à la cyber défense et est consultant depuis quinze ans.*

Ressources

Have I Been Pwned:	https://haveibeenpwned.com/
Two-factor Authentication Site:	https://twofactorauth.org/
NIST SP800-63B Digital Identity Guidelines:	https://pages.nist.gov/800-63-3/sp800-63b.html
Poster: You Are a Target:	https://www.sans.org/u/OGi

Comité de rédaction : Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley