La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

OUCH!

Dans ce numéro...

Phrases de passe

Contexte

Vous utilisez des mots de passe presque quotidiennement, allant de l'accès à vos mails et votre banque en ligne jusqu'aux achats en ligne ou encore l'accès à votre smartphone. Toutefois, les mots de passe sont également votre point le plus faible. En effet, si quelqu'un connaît votre mot de passe, il peut voler votre identité, transférer de l'argent ou avoir accès à vos informations personnelles. Il est essentiel pour votre sécurité que vos mots de passe soient forts. Dans ce numéro, vous allez apprendre à créer des mots de passe forts, faciles à retenir, en utilisant un type différent de mot de passe appelé les phrases de passe.

Editeur invité

My-Ngoc Nguyen (prononcé Me-Nop Wynn) est une instructrice certifiée SANS et CIO/Consultante principale dédiée aux solutions de sécurité IT. Avec ses certifications et ses 14 années en développement, elle apporte son expertise en gestion de programmes de cybersécurité pour des industries et secteurs variés. Twitter: **@MenopN** LinkedIn: My-Ngoc "Menop" Nguyen.

Phrases de passe

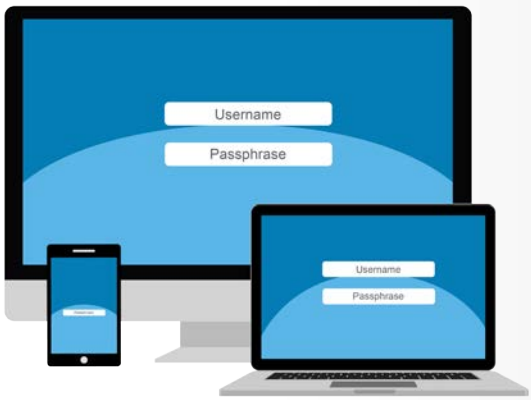
L'enjeu auquel nous sommes tous confrontés est le fait que les cybercriminels ont développé des méthodes sophistiquées pour deviner ou « forcer » les mots de passe et ils s'améliorent de jour en jour. Cela signifie qu'ils sont en mesure de compromettre vos mots de passe si ceux-ci sont faibles ou faciles à deviner. Utiliser des mots de passe forts est une étape importante pour vous protéger. Plus le mot de passe comporte de caractères, plus il est fort et plus il sera difficile pour les malfaiteurs de le deviner. Toutefois, un mot de passe long et complexe peut être difficile à retenir. A la place, nous vous recommandons d'utiliser des phrases de passe qui sont des phrases simples et faciles à retenir mais difficile à pirater.

Voici deux exemples différents :
Faire-Agir-Vérifier
L'Heure du thé est à 1:23

Ce qui rend cette phrase de passe si forte n'est pas seulement dû aux nombreux caractères qu'elle comporte, mais surtout au fait qu'elle utilise des lettres et des symboles (souvenez-vous que les espaces et la ponctuation sont considérés comme des symboles). Vous pouvez renforcer encore plus votre phrase de passe si vous remplacez les lettres par des chiffres ou des symboles, par exemple remplacez la lettre « a » par le symbole « @ » ou la lettre « o » par le chiffre « 0 ». Si un

Phrases de passe

site limite le nombre de caractères que vous pouvez utiliser pour votre mot de passe, utilisez le nombre maximum de caractères auxquels vous avez droit.



Les phrases de passe sont la manière la plus simple de créer et de se souvenir de mots de passe forts.

Utiliser une phrase de passe en toute sécurité

Vous devez également faire attention à la manière dont vous utilisez vos phrases de passe. Utiliser une phrase de passe ne vous aidera pas plus si les malfaiteurs peuvent facilement la voler ou la copier.

1. Assurez-vous d'utiliser une phrase de passe différente pour chacun de vos comptes ou appareils. Par exemple, n'utilisez jamais la même phrase de passe pour votre travail ou pour votre banque en ligne que pour vos comptes personnels, tels que Facebook, YouTube ou Twitter. De cette manière, si l'un de vos comptes est piraté, les autres demeurent sécurisés. Si vous avez trop de phrases à retenir (ce qui n'est pas rare), pensez à utiliser un gestionnaire de mots de passe. Ceci est un programme spécial qui stocke toutes vos phrases de passe de manière sécurisée. Ainsi, les seules phrases de passe que vous aurez à retenir seront celles de votre ordinateur et celles du gestionnaire de mots de passe.
2. Ne partagez jamais une phrase de passe ni la manière dont vous vous y prenez pour en créer une avec quiconque, y compris vos collègues et votre superviseur. Souvenez-vous qu'une phrase de passe doit rester secrète ; si quelqu'un d'autre connait votre phrase de passe, celle-ci n'est plus sécurisée. Si vous partagez accidentellement votre phrase de passe avec quelqu'un ou si vous pensez que votre phrase de de passe a pu être compromise ou volée, assurez-vous de la changer immédiatement. La seule exception est de partager vos phrases-clés personnelles avec un membre de la famille fiable en cas d'urgence. Vous pouvez dans ce cas écrire vos phrases de passe personnelles (assurez-vous qu'elles ne sont pas liées au travail), les stocker dans un endroit sécurisé, et partager cet endroit avec un membre de votre famille fiable. De cette façon, si quelque chose vous arrive et que vous avez besoin d'aide, vos proches peuvent accéder à vos comptes critiques.
3. N'utilisez pas les ordinateurs publics, tels que ceux mis à disposition dans les hôtels ou les cybercafés. N'importe qui peut les utiliser et de ce fait, ils peuvent être infectés par un programme malveillant qui enregistre toutes vos saisies. Connectez-vous à vos comptes uniquement à partir d'ordinateurs ou d'appareils mobiles auxquels vous faites confiance.
4. Méfiez-vous des sites qui vous demandent de répondre à des questions personnelles. Ces questions sont utilisées dans le cas où vous oublierez votre phrase de passe et auriez besoin de le réinitialiser. Le problème c'est que la

Phrases de passe

réponse à ces questions peut souvent être trouvée sur internet ou même sur votre page Facebook. Assurez-vous que si vous répondez à ces questions personnelles, vous utilisez uniquement des informations qui ne sont pas publiques ou que vous inventez. Les gestionnaires de mots de passe peuvent vous aider puisqu'ils permettent de stocker ce genre d'information complémentaire.

5. Beaucoup de comptes en ligne proposent l'identification en deux temps, autrement appelée la vérification en deux étapes. Cela signifie que vous ne pouvez pas vous connecter avec votre simple phrase de passe, vous aurez besoin par exemple d'un code de passe supplémentaire qui sera envoyé sur votre smartphone. Cette option est beaucoup plus sûre qu'une phrase de passe seule. Dès que cela s'avère possible, utilisez toujours ces méthodes d'authentification.
6. Les appareils mobiles demandent souvent un code PIN pour en protéger l'accès. Souvenez-vous qu'un code PIN n'est rien d'autre qu'un nouveau mot de passe. Plus le code PIN sera long, plus il sera sécurisé. Beaucoup d'appareils mobiles vous permettent de changer votre code PIN en vraie phrase de passe. De nombreux appareils mobiles vous permettent de modifier votre numéro PIN à une phrase de passe réelle ou d'utiliser une biométrie comme votre empreinte digitale.
7. Enfin, si vous n'utilisez plus l'un de vos comptes, assurez-vous de le fermer, le supprimer ou le désactiver.

Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients. Pour en savoir plus, veuillez vous référer aux liens suivants : http://www.answer.ch et http://answersecurity.com/

Sources

Gestionnaire de mots de passe : https://securingthehuman.sans.org/ouch/2015#october2015

Vérification à deux étapes : https://securingthehuman.sans.org/ouch/2015#september2015

Verrouillez votre login : https://lockdownyourlogin.com

SANS SEC301 – Cours de cinq jours sur les bases de la cybersécurité : https://sans.org/sec301

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traduit par : Marilyn Combet