OUCH! | Avril 2015

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

OUCH!

Dans ce numéro...

Les phrases de passe

Contexte

Vous utilisez des mots de passe presque quotidiennement, allant de l'accès à vos mails et vos banques en ligne jusqu'aux achats en ligne ou l'accès à votre smartphone. Toutefois, les mots de passe sont également votre point le plus faible, si quelqu'un connait 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.

Rédacteur Invité

Guy Bruneau est un conseiller sénior en sécurité chez IPSS Inc., un instructeur SANS et un prestataire ISC. Guy mène le GSE SANS et a terminé le programme SANS de cyber gardian. Vous pouvez retrouver Guy sur twitter sous le pseudo **@GuyBruneau** et sur **handlers.sans.org/gbruneau**.

Les phrases de passe

L'enjeu auquel nous sommes tous confrontés est le fait que les cybers criminels 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 est 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 difficiles à pirater. Voici un exemple :

Where is King Julian?

Ce qui rend cette phrase de passe si forte n'est pas simplement dû aux 21 caractères qu'elle comporte, mais surtout au fait qu'elle utilise des lettres et des symboles (souvenez-vous, les espaces et la ponctuation sont 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 zéro. Si un 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.

Utiliser des phrases 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.

Les phrases de passe

L'utilisation de phrases de passe est l'un des moyens les plus efficaces pour protéger votre identité et vos informations.

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 de passe 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. Souvenez-vous, 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 partagiez accidentellement votre phrase de passe avec quelqu'un ou si vous pensez que votre phrase de passe a pu être compromise ou volée, assurez-vous d'en changer immédiatement.

3. Tout comme les mots de passe, évitez les phrases de passe faciles à deviner ou fréquemment utilisées. Par exemple, « les chaussettes de l'archiduchesse » n'est pas une bonne phrase de passe parce qu'elle est très connue.

4. N'utilisez pas les ordinateurs publics, tels que ceux dans les hôtels et bibliothèques, pour vous connecter à votre travail ou à votre banque. Puisque ce sont des ordinateurs publics, n'importe qui peut les utiliser et il se peut qu'ils soient infectés par un programme malveillant qui enregistre toutes vos saisies. Connectez-vous à votre travail ou à votre banque en ligne uniquement sur des ordinateurs ou des appareils mobiles auxquels vous faites confiance.

5. Méfiez-vous des sites qui vous demandent de répondre à des questions personnelles. Ces questions sont utilisées dans le cas où vous oublieriez votre phrase de passe et auriez besoin de la réinitialiser. Le problème c'est que la 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 pour ce faire puisqu'ils vous permettent de stocker ce genre d'information complémentaire.

6. 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

Les phrases de passe

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'identification.

7. 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.

8. Enfin, si vous n'utilisez plus l'un de vos comptes, assurez-vous de le fermer, le supprimer ou le désactiver.

Ressources publiques

N'utilisez jamais les ordinateurs publics, tels que ceux que l'on trouve dans les halls d'hôtels, les librairies ou les cybers cafés. Vous n'avez aucune idée de qui a pu utiliser cet ordinateur avant vous, il se peut que cette personne ait, volontairement ou involontairement, infecté cet ordinateur. Lorsque cela est possible, n'utilisez que des appareils que vous contrôlez et auxquels vous faîtes confiance pour vos activités en ligne. Si vous n'avez d'autre choix que d'utiliser un ordinateur public, n'utilisez aucun service qui vous demande de vous identifier ou d'entrer un mot de passe.

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.answersolutions.ch et http://answersecurity.com/

Sources

Vérification en deux étapes :	http://www.securingthehuman.org/resources/newsletters/ouch/2013#august2013
Gestionnaires de mots de passe :	http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013
Ingénierie sociale :	http://www.securingthehuman.org/resources/newsletters/ouch/2014#november2014
Termes de sécurité communs :	http://www.securingthehuman.org/resources/security-terms

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Traduit par : Marilyn Combet