OUCH! | Septembre, 2017

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

OUCH!

Dans ce numéro...

Gestionnaires de mots de passe

Vue d'ensemble

L'une des étapes les plus importantes que vous pouvez prendre en considération pour vous protéger en ligne est d'utiliser un mot de passe unique et solide pour chacun de vos comptes et applications. Malheureusement, il est très probable que vous ne vous souviendrez pas de tous vos différents mots de passe pour tous vos comptes. C'est pourquoi tant de personnes réutilisent le même mot de passe. Malheureusement, la réutilisation du même mot de passe pour différents comptes est dangereuse car, une fois que quelqu'un a compromis votre mot de passe, il peut accéder à tous vos autres comptes requérant le même mot de passe. La solution la plus simple consiste à utiliser un gestionnaire de mots de passe, parfois appelé un coffre-fort de mots de passe. Il s'agit d'un programme qui stocke en toute sécurité tous vos mots de passe, ce qui facilite l'utilisation d'un mot de passe différent pour chacun de vos comptes. Les gestionnaires de mots de passe rendent cela simple car au lieu de devoir se souvenir de tous vos mots de passe, il suffit de vous souvenir uniquement du mot de passe principal de votre gestionnaire de mot de passe.

Editeur invité

Chris Christianson est un consultant en sécurité de l'information basé en Californie. Avec 20 ans d'expérience et en possession de nombreuses certifications techniques, il intervient en qualité de speaker lors d'une variété de conférences et contribue à de nombreux articles. Chris peut être contacté à **@cchristianson** et **https://ismellpackets.com**.

Comment fonctionnent les gestionnaires de mots de passe?

Les gestionnaires de mots de passe stockent vos informations dans une base de données, qui est parfois appelée «coffre-fort». Le gestionnaire de mots de passe chiffre le contenu du coffre-fort et le protège par un mot de passe principal que seul vous connaissez. Lorsque vous devez récupérer vos mots de passe, pour vous connecter à votre banque ou courriel en ligne par exemple, vous devez simplement saisir votre mot de passe principal (ou mot de passe maître) dans votre gestionnaire de mot de passe pour déverrouiller votre coffre-fort. Dans de nombreux cas, le gestionnaire de mots de passe récupère automatiquement votre mot de passe et vous connecte en toute sécurité. Cela facillite le fait d'avoir des centaines de mots de passe uniques et solides, car vous n'avez pas à vous en souvenir.

Certains gestionnaires de mots de passe stockent votre coffre-fort sur votre ordinateur ou sur votre appareil mobile, tandis que d'autres le stockent sur le Cloud. En outre, la plupart des gestionnaires de mots de passe incluent la possibilité de synchroniser automatiquement le contenu de votre coffre-fort avec plusieurs appareils que vous autorisez. De cette façon, lorsque vous mettez à jour un mot de passe sur votre ordinateur portable, ces modifications sont synchronisées avec tous vos autres appareils. Indépendamment du lieu où la base de données est stockée, vous devez installer l'application de

Gestionnaires de mots de passe

gestionnaire de mots de passe sur votre système sur un périphérique que vous utilisez.

Lorsque vous configurez un gestionnaire de mots de passe, vous devez entrer ou importer manuellement vos logins et mots de passe. Par la suite, le gestionnaire de mots de passe peut détecter lorsque vous tentez de vous inscrire à un nouveau compte en ligne ou de mettre à jour le mot de passe d'un compte existant, en mettant automatiquement à jour le coffre-fort en conséquence. Ceci est possible car la plupart des gestionnaires de mot de passe travaillent main dans la main avec votre navigateur Web. Cette intégration permet également de vous connecter automatiquement à des sites Web.

Les gestionnaires de mots de passe sont un moyen simple pour stocker et utiliser tous vos mots de passe différents en toute sécurité.

Il est essentiel que le mot de passe principal que vous utilisez pour protéger le contenu du gestionnaire de mots de passe soit fort et très difficile à deviner pour les autres. En fait, nous vous recommandons de faire de votre mot de passe principal une phrase de passe, l'une des méthodes les plus fiables pour constituer un mots de passe fort. Si votre gestionnaire de mots de passe prend en charge la vérification en deux étapes, utilisez-la pour votre mot de passe principal. Enfin, assurez-vous de vous souvenir de votre mot de passe principal. Si vous l'oubliez, vous ne pourrez accéder à aucun autre mot de passe.

Choix d'un gestionnaire de mot de passe

Il existe de nombreux gestionnaires de mots de passe. Dans la section sources, nous fournissons un lien vers les commentaires des gestionnaires de mots de passe. Pour trouver un gestionnaire de mots de passe qui vous convienne, veuillez bien garder à l'esprit les conseils suivants:

- Votre gestionnaire de mots de passe doit être simple d'utilisation. Si vous trouvez la solution trop complexe à comprendre, trouvez une solution différente qui corresponde mieux à votre style et à votre expertise.
- Assurez-vous que le gestionnaire de mots de passe fonctionne sur tous les systèmes et les appareils mobiles, dont vous pourriez avoir besoin pour accéder à votre coffre-fort. La solution doit aussi permettre de garder facilement le contenu de votre coffre-fort synchronisé sur tous vos appareils.
- Utilisez uniquement des gestionnaires de mots de passe bien connus et fiables. Méfiez-vous des produits qui ne sont pas sur le marché depuis longtemps et qui ont peu ou pas de commentaires. Tout comme les faux logiciels d'anti-virus, les cybercriminels peuvent créer des faux gestionnaires de mots de passe dans le but de voler vos informations. Soyez également très méfiant des fournisseurs qui prétendent développer leurs propres solutions de chiffrement.

Gestionnaires de mots de passe

- Évitez tout gestionnaire de mots de passe prétendant être en mesure de récupérer votre mot de passe principal à votre place. Cela signifie qu'il connait votre mot de passe maître, ce qui vous expose à beaucoup plus de risques.
- Assurez-vous que quelle que soit la solution que vous choisissez, cette dernière continue d'être activement mise à jour et corrigée et assurez-vous également d'utiliser toujours la dernière version.
- Le gestionnaire de mots de passe doit inclure la possibilité de générer automatiquement des mots de passe forts à votre place et de vous démontrer la force des mots de passe que vous avez choisis.
- Le gestionnaire de mots de passe doit vous donner la possibilité de stocker d'autres données sensibles, telles que les réponses à vos questions secrètes de sécurité, vos numéros de cartes de crédit ou encore vos numéros de fidélisation.

Les gestionnaires de mot de passe sont un excellent moyen de stocker de manière sécurisée tous vos mots de passe et autres données sensibles. Cependant, étant donné qu'ils sauvegardent ces informations importantes, assurez-vous d'utiliser un mot de passe principal unique et robuste qui n'est pas seulement difficile à deviner pour un attaquant, mais également facile à retenir pour vous.

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

Le top 2017 des gestionnaires de mots de passe :	https://www.pcmag.com/article2/0,2817,2407168,00.asp
Phrases de passe :	https://securingthehuman.sans.org/ouch/2017#april2017
Vérification en deux étapes :	https://www.securingthehuman.org/ouch/2015#september2015
Vérrouiller votre login :	https://www.lockdownyourlogin.org/
Le conseil de sécurité du jour du SANS :	https://www.sans.org/tip-of-the-day

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