Vous n'utilisez pas de gestionnaire de mots de passe? Voici pourquoi vous devriez en utiliser un !

Article paru dans The Guardian, langue : anglais
Autrice : Kate O'Flaherty,
Samedi 19 Mars 2022 17.00 GM
Traduction :Google Translate et le rédacteur.

Les experts recommandent d'utiliser es gestionnaires de mots de passe pour plus de commodité et une sécurité en ligne améliorée, mais peu d'entre nous les utilisent.

Dans le domaine ouvert d'internet, les mots de passe sont l'un des plus grands risques.

Les mots de passe longs et complexes sont les plus sûrs mais sont difficiles à retenir, ce qui oblige de nombreuses personnes à utiliser des informations d'identification faibles et faciles à deviner. Une étude du National Cyber Security Center (NCSC) du Royaume-Uni a révélé comment des millions de personnes utilisent le nom de leur animal, les noms des équipes de football, le « mot de passe » et « 123456 » pour accéder aux services en ligne

Mais cela vous laisse à la merci des attaques : les cybercriminels peuvent déchiffrer des mots de passe faibles en quelques secondes à l'aide d'outils automatisés. "Un pirate informatique a besoin d'environ deux secondes pour déchiffrer un mot de passe à 11 caractères composé de chiffres", explique Alex Balan, directeur de la recherche sur la sécurité chez Bitdefender. Si le mot de passe est plus complexe, contenant des chiffres, des symboles et des lettres majuscules et minuscules, le temps nécessaire pour le casser passe à 400 ans.

Cela peut sembler complexe au début, mais un gestionnaire de mots de passe vous facilitera la vie.

Les experts disent qu'un bon mot de passe doit être unique et contenir une combinaison de lettres, de chiffres et de caractères spéciaux.

La clé d'un solide est la longueur, déclare le chercheur indépendant en sécurité Sean Wright. "Bien que la complexité du mot de passe aide, la longueur compte beaucoup plus."

Les experts recommandent un minimum de 11 caractères, plus si possible.

L'internaute type dispose d'environ 100 ensembles d'informations de connexion . La mémorisation de ce nombre de mots de passe complexes dépasse largement les capacités de rappel de la plupart des gens.

Les applications de gestion de mots de passe peuvent résoudre ce problème en créant pour vous des informations d'identification longues et complexes et en les mémorisant pour la prochaine fois que vous vous connecterez. Pourtant, seule une personne sur cinq au Royaume-Uni en utilise une, selon des estimations récentes.

Beaucoup de gens sont rebutés par les tracas, tandis que d'autres hésitent à autoriser une entreprise à stocker tous leurs mots de passe. Comment savoir quel entreprise est digne de confiance et que se passe-t-il si celle-ci est piratée?

Cela peut sembler intimidant au début, mais un gestionnaire de mots de passe vous facilitera grandement la vie. Voici tout ce que vous devez savoir.

Pourquoi devriez-vous rejoindre les 20% de personnes qui en utilisent un?

Une fois que vous avez téléchargé un gestionnaire de mots de passe, tel que 1Password, LastPass, Bitwarden ou Dashlane[1], vous pouvez suivre les instructions pour importer vos identifiants depuis un autre emplacement, tel que votre navigateur. Vous pouvez également recommencer à zéro si vous le souhaitez et supprimer les comptes dont vous n'avez plus besoin au fur et à mesure.

Après l'avoir configurée, l'application peut générer pour vous des mots de passe forts pour tous les nouveaux sites que vous utilisez, et ceux-ci seront documentés automatiquement au fur et à mesure que vous naviguez. Cela résout l'un des aspects les plus difficiles de la sécurité des mots de passe: mémoriser de nombreuses informations d'identification complexes.

"Étant donné que les gestionnaires de mots de passe s'occupent de la partie mémorisation, chaque mot de passe peut être une sélection longue et totalement aléatoire de caractères", explique Jake Moore, conseiller mondial en cybersécurité chez la société de sécurité ESET.

Les gestionnaires de mots de passe garantissent également que vous utilisez un identifiant unique pour chaque compte, plutôt que de répéter les mêmes identifiants en se connectant aux différents services. Ceci est crucial pour empêcher le "credential stuffing" (voir chapitre sur ce sujet dans ce document) attaques, qui se produisent lorsqu'un pirate utilise votre mot de passe compromis, par exemple de Facebook, pour essayer d'accéder à d'autres services bien connus que vous pourriez utiliser, tels que Netflix ou Spotify.

Un autre avantage souvent négligé est que la plupart des gestionnaires de mots de passe aident à prévenir les attaques de phishing, où les escrocs vous encourageront à cliquer sur un lien afin qu'ils puissent voler vos informations d'identification. « Comme ils lient les informations d'identification à une adresse Web spécifique, la saisie semi-automatique ne fonctionnera pas sur les sites de phishing », explique Wright.

Dans certains cas, vous pouvez même utiliser des gestionnaires de mots de passe pour partager en toute sécurité une connexion avec d'autres personnes de confiance, telles que des membres de la famille. Ils vous permettent également de stocker en toute sécurité des codes PIN, des détails de carte de crédit et des identifiants bancaires en ligne.

Pourquoi ils sont dignes de confiance et pas aussi compliqués que vous le pensez Une idée fausse et majeure à propos des gestionnaires de mots de passe est que le fait de stocker vos informations d'identification au même endroit est un risque. "On me demande souvent: « Et si quelqu'un peut accéder à mon gestionnaire de mots de passe? », mais en utiliser un est bien

[1] Le Club Informatique L@ssourie recommande KEEPASSXC , une gestionnaire de mots de passe open source , multi-plateformes et gratuit.

mieux que de réutiliser les mêmes informations d'identification pour tous les comptes", déclare Moore.

Bien qu'il y ait un petit risque à placer toutes vos identifiants au même endroit, la probabilité que le gestionnaire de mots de passe soit violé est extrêmement faible.

Vos identifiants et informations confidentielles sont cryptées.

Les gestionnaires de mots de passe sécurisent vos informations en cryptant vos identifiants afin qu'ils ne soient accessibles que lorsque vous saisissez le mot de passe principal. « Vos mots de passe en clair ne sont jamais stockés sur votre appareil ou sur les serveurs du gestionnaire de mots de passe », déclare Paul Bischoff, défenseur de la confidentialité chez Comparitech.

La configuration d'un gestionnaire de mots de passe est probablement le plus grand obstacle pour ceux qui commencent leur utilisation mais vous pouvez le faire progressivement, en changeant les mots de passe au fur et à mesure. Une fois que vous avez configuré votre application, cela vous fera gagner du temps que vous avez passez à réinitialiser les connexions que vous avez oubliées.

Certains voient le coût comme un problème, mais les gestionnaires de mots de passe sont souvent gratuits ou disponibles pour quelques euros par mois. Si vous décidez de payer, l'abonnement en vaudra la peine si vous considérez les coûts du piratage et lla protection dont vous bénéficiez par exemple pour les comptes bancaires auxquels vous accédez.

Que pensez des gestionnaires de mots de passe offerts par les GAFA ?

Apple Keychain et Google Password Manager sont-ils équivalents aux applications gestionnaires de mots de passe ?

Apple Keychain et Google Chrome Password Manager sont des gestionnaires de mots de passe, mais ils n'ont pas toutes les fonctionnalités des applications gestionnaires de mots de passe. Rester avec Apple ou Google signifie que vous ne pourrez pas utiliser facilement votre gestionnaire de mots de passe avec d'autres appareils ou navigateurs.

Apple Keychain et Google Chrome aident à renforcer la protection, mais vous aurez du mal à passer facilement d'un appareil à l'autre sans gestionnaire de mots de passe indépendant, explique Moore. "Bien que ce soit mieux que de réutiliser des mots de passe, un gestionnaire de mots de passe tiers offre généralement plus de fonctionnalités et est facilement accessible sur tous les appareils."

Étapes pour améliorer votre sécurité

Gardez à l'esprit que le gestionnaire de mots de passe aura besoin d'un mot de passe principal, dont vous devrez être capable de vous souvenir. Celui-ci doit être aussi long et complexe que possible, par exemple une phrase ou un ensemble de mots mémorisables comprenant certains caractères et nombres aléatoires.

Certaines applications de mot de passe vous permettent de savoir quand l'un de vos comptes a été compromis. Le site « HaveIBeenPwned » est une autre méthode fiable pour vérifier si vos mots de passe sont apparus dans une violation connue.

Apple propose également une fonction pour détecter les mots de passe piratés, sous Paramètres > Mots de passe > Recommandations de sécurité. Si l'un de vos mots de passe a été compromis, c'est une bonne idée de le changer, pour le site piraté ainsi que sur tout autre site Web où vous utilisez les mêmes informations d'identification.

Le nettoyage de printemps numérique: comment trier vos mots de passe, votre vie privée et votre dossier photo volumineux.

De tous vos mots de passe, celui se rapportant à votre email est le plus important. Si un criminel est en mesure d'accéder à votre courrier électronique, il pourrait voler des informations, y compris des coordonnées bancaires, ou envoyer des messages se faisant passer pour vous pour voler les gens. Pire encore, ils pourraient utiliser votre e-mail pour réinitialiser tous vos autres mots de passe, prenant ainsi le contrôle de vos comptes. Pour cette raison, le NCSC[2] recommande de créer un mot de passe extra-fort pour ce compte, en utilisant un gestionnaire de mots de passe si possible.

Les experts recommandent que les mots de passe - et les gestionnaires de mots de passe - soient associés à une authentification à deux facteurs, dans laquelle on vous demande quelque chose comme un code à usage unique en plus d'un mot de passe lorsque vous vous connectez à l'aide d'un nouvel appareil.

Pour les plus aventureux d'entre vous, il est possible d'utiliser une clé de sécurité telle qu'une YubiKey – un jeton que vous pouvez insérer dans votre appareil pour doubler les comptes à haut risque tels que les e-mails. Une applications d'authentification telles que Authy est une autre option.

Ceux-ci génèrent un code unique que vous pouvez entrer sur le site et sont très simples à utiliser.

La moins mauvaise alternative…

Si tout cela semble trop technique, ou si vous gérez les mots de passe d'un parent ou d'un grand-parent âgé, il existe une autre option. Bien qu'ils soient parfois moqués, les carnets de mots de passe physiques ne sont pas une mauvaise idée, tant que vous suivez les directives pour créer des connexions solides et uniques, et que le carnet est conservé dans un endroit sécurisé et ne quitte jamais le domicile de la personne . Et il va sans dire que vous ne devez jamais créer un carnet ou un document "virtuel" (sous un tableur par exemple sur votre ordinateur, qui pourrait être visible si votre appareil est piraté ou volé .

[2] NCSC : National_Computer_Security_Center, département de la NSA, NSA organisation des États-Unis qui coordonne et dirige des activités hautement spécialisées pour protéger les systèmes d'information des États-Unis et produire des informations de renseignement étrangères

Annexes.

Ces paragraphes ont été ajoutés dans ce document pour une meilleur compréhension , ils ne font pas partie de l'article d'origine.

« Credential Stuffing »

Le « credential stuffing » est un type de cyberattaque où des informations de comptes volées consistant généralement en des listes d'identifiants et de mots de passe associés (souvent obtenus de manière frauduleuse) sont utilisés pour obtenir un accès non autorisé à des comptes utilisateurs par le biais de demandes de connexion automatisée à grande échelle adressées à des applications Web.

Contrairement au cassage de mots de passe, une attaque de « credential stuffing » ne tente pas de trouver un mot de passe par une attaque par force brute. L'attaquant automatise plutôt des tentatives de connexions en utilisant des milliers ou même des millions de paires d'identifiants / mots de passe précédemment découverts. Pour ce faire, il utilise des outils d'automatisation Web standards comme Selenium, cURL, PhantomJS ou des outils conçus spécifiquement pour ces types d'attaques comme Sentry MBA2,3.

Site « Have I Been Pwned »

Site ai-je été piraté ?

Ce site ou vous préciser votre adresse mail , a deux objectifs principaux : premièrement, il fournit évidemment un service public, en indiquant si vitre mail a été trouvé dans les données volées de sites piratés et en indiquant quels sites sont concernés pour vous permettre changer immédiatement les mots de passes correspondants. Ce site est mis à jour quotidiennement.

https://haveibeenpwned.com/

KeepassXC

Le Club Informatique L@ssurie vous recommande le gestionnaire de mots de passes KeepassXC , Open Source et gratuit qui possède un base de données entièrement cryptée pour génerer, conserver et restituer vos mots de passe,. KeepassXC fs'installe et fonctionne sur les environnements Windows, Linux et Mac. Il est compatible avec les principaux navigateurs WEB.

https://keepassxc.org/