OUCH! Décembre 2023

Votre bulletin mensuel sur la sensibilisation à la sécurité

Le pouvoir de la phrase de passe

Vous en avez assez de créer constamment des mots de passe complexes ? Frustré de devoir se souvenir et taper tous ces caractères, symboles et chiffres ? Nous avons une solution pour vous : la phrase d'authentification, toujours aussi puissante !

Phrases de passe

Vous ne vous en rendez peut-être pas compte, mais les mots de passe sont l'un des principaux vecteurs d'attaque des cyberattaquants. Des acteurs malveillants ciblent vos mots de passe et, s'ils parviennent à deviner correctement ou à pirater le bon, ils peuvent facilement accéder à votre courrier électronique, à vos comptes bancaires, voire voler toute votre identité. Plus vos mots de passe sont faibles, plus il leur est facile d'entrer. C'est pourquoi des mots de passe forts constituent l'un des moyens les plus efficaces de protéger vos comptes et votre vie numérique en ligne. Traditionnellement, vous êtes habitués à utiliser des mots de passe très complexes. L'idée est que plus la complexité est grande, plus il est difficile pour les cyber-attaquants et leurs programmes automatisés de deviner le mot de passe. Mais le problème est que les mots de passe complexes sont également difficiles à retenir et à taper avec précision. Une meilleure façon de créer un mot de passe fort et sûr est d'utiliser ce que l'on appelle une phrase de passe. Au lieu d'être complexes, ils sont forts en raison de leur longueur. Voici quelques exemples :

C'est l'heure du café !
perdu-escargot-rampe-plage

Les phrases de passe ne sont rien d'autre qu'une série de mots et peuvent contenir plus de vingt caractères si le site le permet. Cela peut sembler beaucoup, mais les deux exemples ci-dessus contiennent plus de vingt caractères et, contrairement aux mots de passe, les phrases de passe sont beaucoup plus faciles à retenir et à taper. Plus la phrase de passe est longue, plus elle est sûre. Dans certaines situations, il peut vous être demandé de complexifier votre phrase de passe, c'est-à-dire d'ajouter des symboles, des lettres majuscules ou des chiffres. Le moyen le plus simple d'y parvenir est de modifier certaines lettres de votre phrase de passe par des symboles ou des chiffres. Par exemple, en remplaçant la lettre « e » par le chiffre 3, les exemples ci-dessus deviennent plus complexes, tout en restant suffisamment faciles à mémoriser et à taper :

C'3st l'h3ur3 du caf3 !
p3rdu-3scargot-ramp3-plag3

Une phrase de passe unique

Pour que la phrase de passe soit vraiment sûre, elle doit également être unique pour chaque compte. Si vous utilisez la même phrase de passe, ou une phrase contenant un motif facilement identifiable, pour plusieurs comptes, vous vous mettez en danger.

© SANS Institute 2023

Il suffit à un cyber-attaquant de pirater un site web que vous utilisez fréquemment, de voler la phrase de passe que vous utilisez pour ce site particulier et, si tous vos mots de passe/phrases de passe sont les mêmes, il aura alors accès à tous vos autres comptes. Vous ne vous souvenez plus des phrases de passe longues et uniques pour chacun de vos comptes ? Nous avons une solution pour vous : les gestionnaires de mots de passe.

Les gestionnaires de mots de passe sont des programmes informatiques spéciaux qui stockent en toute sécurité tous vos mots de passe dans un coffre-fort crypté protégé par un mot de passe principal. Pour accéder à la chambre forte, il suffit de se souvenir du mot de passe principal. Le gestionnaire de mots de passe peut récupérer automatiquement vos mots de passe chaque fois que vous en avez besoin et se connecter automatiquement aux sites web pour vous. Les gestionnaires de mots de passe ont évolué pour inclure d'autres fonctionnalités, notamment le stockage des réponses aux questions secrètes, l'avertissement lorsque vous réutilisez des mots de passe ou que vous vous retrouvez sur un site web piraté, l'utilisation de générateurs qui créeront des mots de passe ou des phrases de passe forts pour vous, et bien d'autres choses encore. La plupart des gestionnaires de mots de passe se synchronisent en toute sécurité sur presque tous les ordinateurs ou appareils, de sorte que, quel que soit le système que vous utilisez, vous pouvez accéder facilement et en toute sécurité à tous vos mots de passe.

L'étape finale : l'authentification multifactorielle

La dernière étape pour rendre vos phrases de passe vraiment infaillibles consiste à leur ajouter une deuxième couche de protection, appelée authentification multifactorielle (AMF). L'AMF exige que vous ayez deux moyens d'authentification lorsque vous vous connectez à vos comptes. Il peut s'agir de votre mot de passe et d'un élément biométrique tel qu'une empreinte digitale, ou de votre mot de passe et d'un code numérique généré automatiquement et envoyé à un autre appareil ou à un autre compte de messagerie. Le code est unique à chaque fois et peut être généré à partir d'un téléphone portable ou d'un autre appareil de confiance. Ce processus garantit que même si un cyber-attaquant obtient votre phrase de passe, il ne peut pas accéder à vos comptes, car il ne dispose pas du deuxième facteur. L'AMF doit être activée autant que possible, en particulier pour vos comptes les plus importants, tels que vos comptes bancaires, de retraite ou de messagerie électronique personnelle. Si vous utilisez un gestionnaire de mots de passe, il est fortement recommandé de le protéger par une phrase de passe forte ET une authentification multifactorielle.

Les phrases de passe sont un excellent moyen de simplifier la sécurité et de sécuriser vos comptes. Pour rendre votre vie numérique en ligne encore plus simple et plus sûre, nous vous suggérons de combiner la puissance des gestionnaires de mots de passe et de l'AFM pour vos phrases de passe.

Rédacteur Invité

Quintana Patterson est responsable de l'informatique clinique et de la conformité à l'université du Colorado Anschutz Medical Campus et présidente du comité de défense de l'équité de WiCyS (Women in CyberSecurity). Elle s'est engagée à faire en sorte que les femmes de ce secteur se sentent accueillies, soutenues et valorisées.

Ressources

Gestionnaires de mots de passe : https://www.sans.org/newsletters/ouch/power-password-managers/
Biométrie : https://www.sans.org/newsletters/ouch/biometrics-making-security-simple/
Authentification multifactorielle : https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/

Traduit pour la communauté par : Juliette Busson

OUCH! Est publié par SANS Security Awareness et est distribué sous la licence Creative Commons BY-NC-ND 4.0. Vous êtes libre de partager ou de distribuer ce bulletin d'information, à condition de ne pas le vendre ou le modifier. Comité de rédaction : Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.