Le pouvoir de la phrase de passe : pourquoi plus long est mieux que plus intelligent

Un mot de passe simple, un gros problème

Daniel s'était toujours considéré comme "à l'aise avec les ordinateurs". Il faisait ses achats en ligne, gérait ses finances sur l'ordinateur, et communiquait avec ses amis via les réseaux sociaux. Comme beaucoup de gens, il a protégé son compte e-mail personnel avec un mot de passe qu'il utilisait depuis des années. C'était un mot de passe court, simple à retenir, et qui comportait son équipe de sport favorite avec un caractère spécial et un chiffre. Il s'était dit que c'était suffisant.

Un matin, Daniel s'est réveillé avec une dizaine de notifications. Des e-mails de réintialisation de mot de passe, d'échec de connexion, et de messages d'amis lui demandant pourquoi il envoyait des liens étranges. Son compte de messagerie avait été piraté pendant la nuit. Une fois connecté, le pirate a réinitialisé les mots de passe de ses comptes de réseaux sociaux, de sites marchands et de stockage en ligne. En l'espace de quelques heures, de faux messages ont été envoyés à ses contacts, des achats ont été effectués en son nom et des photos privées ont été téléchargées.

La cause profonde n'était pas un piratage sophistiqué ni un logiciel malveillant de pointe. La raison la plus probable était un mot de passe faible et réutilisé, qui avait soit été divulgué lors d'une fuite de données sur un autre site web, soit simplement deviné par les outils automatisés du pirate. Un seul mot de passe faible a permis à un cybercriminel d'accéder à toute la vie numérique de Daniel.

Pourquoi les mots de passe nous font-ils défaut ?

Les mots de passe restent le moyen le plus courant de protéger nos comptes en ligne, mais ils constituent également l'un des maillons faibles de notre sécurité. En général, les cybercriminels ne devinent pas les mots de passe en essayant une combinaison après l'autre, comme on le voit dans les films. Au lieu de cela, ils utilisent des outils automatisés. Ces outils peuvent tester très rapidement des millions, voire des milliards, de combinaisons de mots de passe. Ils s'appuient également largement sur des listes de mots de passe volés lors de failles de sécurité antérieures. Si vous réutilisez vos mots de passe ou si vous en choisissez des courts et faciles à deviner, les pirates ont déjà une longueur d'avance sur vous.

L'utilisation de mots de passe forts est l'un des moyens les plus efficaces de protéger vos comptes et votre vie numérique en ligne. Le problème avec les mots de passe complexes, c'est qu'ils sont difficiles à retenir et à saisir. Une méthode encore plus efficace pour créer un mot de passe solide et sécurisé consiste à utiliser ce qu'on appelle une « phrase de passe ». Une phrase de passe est simplement un mot de passe composé de plusieurs mots, parfois regroupés en une courte phrase. Ce n'est pas seulement leur complexité qui les rend difficiles, mais aussi leur longueur. Par exemple :

C'est l'heure d'un café fort !
perdu-escargot-ramper-plage

Les mots de passe plus longs sont nettement plus difficiles à pirater pour les outils automatisés, tout en restant faciles à mémoriser et à saisir. Dans certains cas, il peut vous être demandé de renforcer la sécurité de votre mot de passe, par exemple en y ajoutant des caractères spéciaux, des lettres majuscules ou des chiffres.

Gardez vos phrases de passe uniques

La longueur ne suffit pas. Votre phrase de passe doit également être unique pour chaque compte. Si vous utilisez le même mot de passe ou la même phrase secrète sur plusieurs sites, une violation de sécurité sur un seul compte peut compromettre tous vos autres comptes. Les pirates testent régulièrement les identifiants volés sur les plateformes de messagerie électronique, bancaires et de réseaux sociaux, dans le cadre d'un processus appelé « credential stuffing ».

Conservez en toute sécurité toutes ces phrases de passe

Vous n'arrivez pas à vous souvenir de toutes ces longues phrases de passe uniques pour chacun de vos comptes ? Nous avons une autre solution à vous proposer : les gestionnaires de mots de passe. Il s'agit de logiciels 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 au coffre-fort, il vous suffit de vous souvenir du mot de passe principal. Le gestionnaire de mots de passe peut récupérer automatiquement vos mots de passe dès que vous en avez besoin et vous connecter automatiquement aux sites web à votre place. Les gestionnaires de mots de passe ont évolué et proposent désormais d'autres fonctionnalités, comme le stockage des réponses aux questions de sécurité, l'alerte en cas de réutilisation d'un mot de passe ou de connexion à un site web frauduleux, ou encore la création de mots de passe robustes grâce à des générateurs. La plupart des gestionnaires de mots de passe se synchronisent également en toute sécurité sur presque tous les ordinateurs ou appareils ; ainsi, quel que soit le système que vous utilisez, vous bénéficiez d'un accès simple et sécurisé à tous vos mots de passe.

Allez encore plus loin

Même la phrase de passe la plus sûre n'est pas infaillible. C'est pourquoi vous devriez activer l'authentification multifactorielle (MFA) dès que possible. L'authentification multifactorielle (MFA) offre une protection supplémentaire en exigeant soit quelque chose que vous possédez, comme un code à usage unique envoyé sur un autre appareil, soit quelque chose qui vous est propre, comme une vérification biométrique. Cela signifie que même si votre phrase de passe est volée, les pirates sont toujours bloqués.

Des habitudes simples, une protection efficace

L'histoire de Daniel aurait pu se terminer tout autrement s'il avait utilisé une phrase de passe longue et unique, voire activé l'authentification multifactorielle. Les mots de passe faibles ou réutilisés sont encore très courants et permettent aux cybercriminels de vous prendre pour cible, même si vous êtes par ailleurs prudent ou expérimenté.

Rédacteur invité

Tarun Preetham Bulla est un formateur et un professionnel de la cybersécurité qui possède une expérience professionnelle dans les domaines de la gestion des incidents, de l'analyse post-incident et de la détection des menaces. Tarun dispense des cours de cybersécurité aux étudiants de premier cycle, gère des laboratoires de cybersécurité, encadre des projets de fin d'études et s'attache à préparer les étudiants au monde du travail en intégrant dans son enseignement une expertise pratique issue du secteur.

Ressources

Le pouvoir des gestionnaires de mots de passe : https://www.sans.org/newsletters/ouch/stop-password-pain-reliable-password-manager
Comment les cybercriminels volent vos mots de passe : https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/
Aller plus loin que les phrases de passe : https://www.sans.org/newsletters/ouch/passkeys-simpler-safer-way-sign-in

Traduit pour la communauté par : Juliette Busson

Vous pouvez trouver plus de contenu OUCH! Sur le lien suivant : https://www.sans.org/newsletters/ouch