## Pssst! Quel est le mot de passe?

Les mots de passe font partie intégrante de l'ère numérique. Combien de fois vous êtes-vous connecté à un site Web et avez-vous oublié votre mot de passe? Sans surprise, les mots de passe courants continuent d'être « 1234567 » et, malheureusement, la sécurité cède la place à la commodité. C'est pourquoi il est plus que jamais nécessaire de donner des conseils et d'éduquer les gens sur les mots de passe forts et complexes afin d'assurer notre sécurité!

Les mots de passe sont les clés permettant de déverrouiller nos profils en ligne qui sont hébergés sur divers sites Web. Chacun de nos profils nécessitant un mot de passe distinct, il n'est pas rare que les gens aient besoin de plusieurs mots de passe, mais pour qu'ils soient efficaces, il faut que ce soit un mot ou un mot de passe peu courant.

Pour vous assurer que vos mots de passe protègent efficacement vos renseignements, il est important de vérifier les pratiques exemplaires pour vos mots de passe. Les pratiques exemplaires en matière de mots de passe désignent le degré de sélection et de gestion des mots de passe d'un utilisateur. Il s'agit de veiller à ce que vos mots de passe soient uniques, difficiles à deviner et comportent plusieurs niveaux de protection. Si vous ne vérifiez pas les pratiques exemplaires pour vos mots de passe, vous risquez d'être victime de failles de sécurité, de vol de renseignements et d'usurpation d'identité.

Utilisez notre liste de contrôle de sécurité des mots de passe ci-dessous pour tester vos pratiques exemplaires en matière de mots de passe!

| | | |
|---|---|---|
| Phrases de passe | • Essayez d'utiliser une phrase de passe. Les phrases de passe sont plus longues et plus difficiles à deviner pour quelqu'un. Rendez-vous sur Use a Passphrase (utiliser une phrase de passe) pour plus de renseignements.<br>• Utilisez des lettres majuscules et minuscules, des caractères spéciaux et des chiffres.<br>• Évitez les mots courants ou les termes d'argot. |  |
| Authentification multifactorielle (AMF) | • L'authentification multifactorielle (AMF) exige deux types d'identification ou plus pour se connecter à un compte.<br>• Parmi les exemples d'AMF, |  |

| | | |
|---|---|---|
| | citons un mot de passe ou un code, un jeton ou une application d'authentification, ou encore un balayage des empreintes digitales ou du visage. | |
| Utilisez des mots de passe uniques. | • Utilisez un mot de passe différent pour chaque compte.<br>• Ne réutilisez pas les mots de passe précédents. |  |
| Utilisez un gestionnaire de mots de passe. | • Cela vous aidera à générer des mots de passe forts et à les stocker dans un endroit crypté. |  |

**Cyberdéfenseur, le saviez-vous?** Selon une étude de Microsoft, l'utilisation de l'AMF peut bloquer plus de 99,9 % des attaques visant à compromettre un compte. L'AMF est un élément essentiel de la cybersécurité qui ajoute une couche supplémentaire de protection. Si votre mot de passe est compromis, l'AMF peut empêcher un attaquant d'accéder à votre compte.

Si les mots de passe pratiques et faciles à retenir peuvent être agréables à court terme lors de la connexion à votre compte, ils peuvent entraîner des atteintes à votre sécurité et à celle de votre organisme. N'oubliez jamais que lorsqu'il s'agit de simplicité ou de sécurité, la sécurité est la meilleure solution!