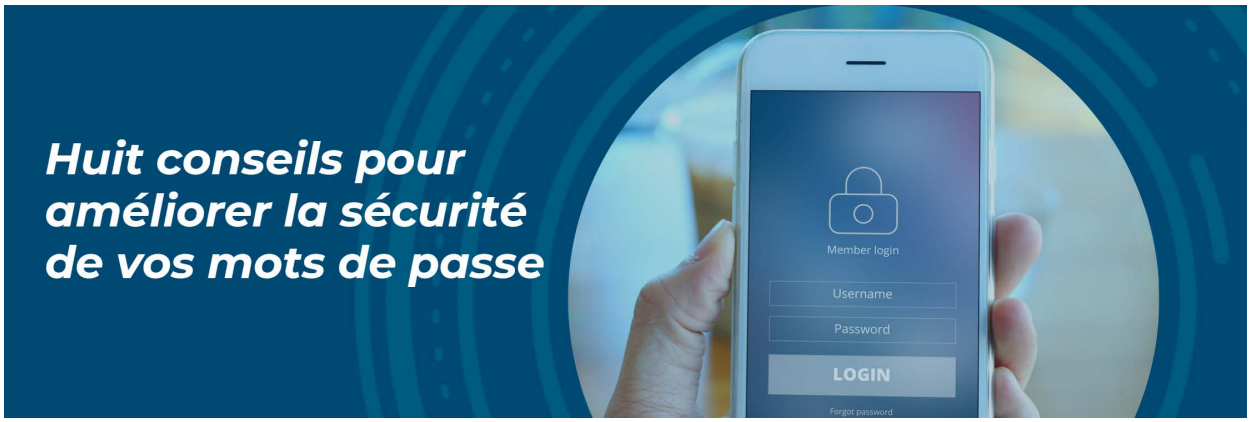
NPC



Les cybercriminels sont toujours à la recherche du point d'entrée le moins sécurisé pour accéder à vos comptes. Lorsque vos comptes contiennent des données commerciales, y compris des renseignements personnels identifiables (PII) de clients, il est d'autant plus important que vos mots de passe ne constituent pas le maillon faible de votre chaîne de sécurité.

Vous trouverez ci-dessous huit conseils où nous vous expliquons en quoi la création et la gestion de mots de passe les plus forts possible vous aideront à mieux sécuriser vos comptes et comment l'ajout d'un deuxième niveau de sécurité empêchera qu'on y accède par la simple utilisation de votre mot de passe.

1 Privilégiez la longueur plutôt que la complexité

Les mots de passe complexes sont moins sécurisés que vous ne le pensez parce que les cybercriminels utilisent des processus de décryptage automatisés. Les *attaques par force brute* consistent à trouver le bon mot de passe en testant chaque combinaison de caractères possible. Les *attaques par dictionnaire* consistent à comparer les mots de passe aux mots courants pour obtenir rapidement une correspondance.

Même si remplacer des lettres par des symboles rend le mot de passe plus difficile à deviner par un humain, cette technique ne ralentit pas un ordinateur qui tente de le pirater. En ajoutant des caractères à votre mot de passe, vous augmentez de façon exponentielle le temps nécessaire à un ordinateur pour le pirater, c'est pourquoi les mots de passe plus longs sont beaucoup plus sécurisés.

Dans la mesure du possible, choisissez un mot de passe contenant au moins 14 caractères.

2 Optez pour des phrases passe pour plus de commodité

Il est plus pratique et plus facile de retenir un long mot de passe qu'un mot de passe complexe. On vous propose donc de transformer votre long mot de passe en une phrase pour qu'il soit plus facile à saisir et à retenir.

MOT DE PASSE COMPLEXE **Melis3a!**	PHRASE PASSE LONGUE **s@lto avant de melissa**
8 caractères	22 caractères
Peut être piraté en : **59,36 secondes**	Peut être piraté en : **72 mille ans**

3 Utilisez un gestionnaire de mots de passe sécurisé

Si vous avez un long mot de passe pour chacun de vos comptes, vous feriez mieux d'utiliser un gestionnaire de mots de passe. Trouvez-en un qui est sécurisé et digne de confiance avant d'y enregistrer tous vos identifiants et authentifiants de connexion.

Nous vous recommandons d'en utiliser un qui stocke les mots de passe localement (plutôt que dans le nuage) et qui se déverrouille à l'aide d'un lecteur d'empreintes digitales. Vous bénéficierez ainsi d'une sécurité accrue et d'un accès plus facile.

4 Changez votre mot de passe régulièrement (tous les 90 à 120 jours)

Si un cybercriminel obtient votre mot de passe, il pourrait avoir accès à votre compte un certain temps sans que vous vous en rendiez compte. En changeant votre mot de passe régulièrement, vous pouvez empêcher toute personne ayant eu accès à votre compte à votre insu de s'y connecter à nouveau.

5 N'envoyez jamais votre nom d'utilisateur et votre mot de passe ensemble

Si vous devez communiquer vos identifiants de connexion ou le mot de passe d'un fichier chiffré, transmettez les deux éléments (nom d'utilisateur/mot de passe ou fichier/mot de passe) séparément, en passant préférablement par différents moyens de communication. Par exemple, donnez-en un par courriel et l'autre par téléphone.

Vous ne devez jamais communiquer ou confirmer un mot de passe sur un site Web inconnu ou via un courriel, un message texte ou un appel téléphonique dont vous ne connaissez pas la source.

6 N’utilisez jamais le même mot de passe deux fois ou dans plus d’un endroit

Lorsqu’un cybercriminel obtient un nom d’utilisateur et un mot de passe, il essaie de se connecter à d’autres sites Web importants à l’aide de ces identifiants. On vous suggère donc de créer un mot de passe différent pour chacun de vos comptes, même pour ceux qui vous semblent moins importants (p. ex., médias sociaux et services de diffusion en continu).

Au moins 91 % des gens connaissent les risques liés au fait d’utiliser un même mot de passe pour plusieurs comptes en ligne. Et pourtant, 66 % des gens le font quand même[1].

7 Faites attention aux renseignements que vous communiquez en ligne

Les cybercriminels utilisent les médias sociaux et les sites Web personnels pour pirater les mots de passe plus rapidement en les parcourant à la recherche de renseignements personnels qui pourraient être utilisés dans un mot de passe (comme votre date de naissance ou votre équipe de sport préférée), ou pour contourner les questions de sécurité (comme le nom de votre animal de compagnie quand vous étiez enfant ou le modèle de votre première voiture).

8 Activez l’authentification multifacteur

Les piratages de comptes se produisent souvent en raison de mots de passe faibles faciles à pirater ou de mots de passe qui ont été exposés lors d’une cyberattaque. L’activation d’un deuxième niveau de sécurité peut empêcher qu’on accède à votre compte, peu importe la façon dont on obtient votre mot de passe.

L’authentification multifacteur (AMF) exige l’utilisation de deux ou plusieurs méthodes d’identification pour vérifier votre identité. Ces « facteurs » comprennent quelque chose que vous seul *connaissez*, comme un mot de passe ou un NIP, quelque chose que vous seul *possédez*, comme votre téléphone ou votre clé de sécurité USB, et quelque chose qui vous *distingue* des autres, comme votre voix ou votre empreinte digitale.

L’AMF peut bloquer plus de 99,9 % des attaques par compromission de comptes en ligne[2].

Visionnez notre webinaire sur les pratiques informatiques sécuritaires intitulé Enhancing Password Security and the Power of Multi-Factor Authentication [en anglais seulement], pour obtenir plus d’information et d’autres conseils pour améliorer la sécurité de votre mot de passe.

Programme sur les pratiques informatiques sécuritaires de NPC

Le réseau d'assurance IDC Worldsource a choisi de s'associer à NPC pour vous offrir un programme sur les pratiques informatiques sécuritaires visant à aider les conseillers à protéger leurs activités et les renseignements sensibles qu'ils gèrent. NPC se spécialise dans les solutions informatiques gérées et sécurisées pour aider les professionnels à garder une longueur d'avance sur les cybermenaces émergentes.

Laissez NPC vous aider à protéger les données de vos clients afin que vous puissiez vous concentrer sur le développement de votre entreprise. Le programme sur les pratiques informatiques sécuritaires comprend une offre spéciale qui contribue à améliorer la posture de cybersécurité.

Sources [en anglais seulement]:
1) « Psychology of Passwords: The Online Behavior That's Putting You at Risk », Rapport de LogMeIn inc., 13 mars 2020.
2) Melanie Maynes. « One simple action you can take to prevent 99.9 percent of attacks on your accounts », Microsoft Security, 20 août 2019.

NPC DataGuard, une division de Compugen inc.
www.npcdataguard.com

Pour plus d'informations, veuillez contacter:
Denis Goulet
Email: dgoulet@npcdataguard.com
Phone: 905-305-6543