PRATIQUES EXEMPLAIRES DE CRÉATION DE PHRASES DE PASSE ET DE MOTS DE PASSE

Vous avez des mots de passe pour tout : vos appareils, vos comptes (services bancaires, médias sociaux, courriels, etc.) et les sites Web que vous visitez. Vous pouvez protéger vos appareils et vos renseignements en utilisant des phrases de passe ou des mots de passe robustes. Lisez les conseils ci-dessous pour apprendre comment créer des phrases de passe, renforcer vos mots de passe et éviter de commettre des erreurs courantes qui pourraient compromettre vos renseignements.

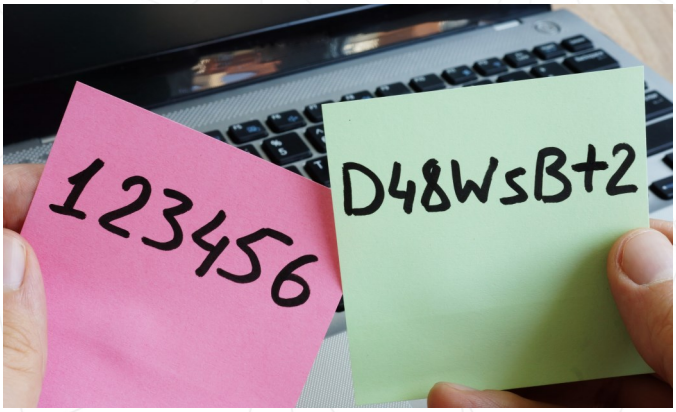
Nous vous recommandons de créer des mots de passe d'au moins 12 caractères. Rappelez-vous que les règles de création de mots de passe ne sont pas les mêmes pour les sites Web et les applications (c.-à-d. que le nombre de lettres, chiffres, signes de ponctuation et caractères spéciaux qu'un mot de passe doit contenir peut varier). Ces règles auront une incidence sur l'application de nos recommandations .

UTILISEZ DES PHRASES DE PASSE

Nous vous recommandons d'utiliser des phrases de passe puisqu'elles sont plus longues, mais plus faciles à retenir qu'un mot de passe composé de divers caractères choisis au hasard. Une phrase de passe est une phrase que vous avez mémorisée et qui se compose d'une suite de mots divers, avec ou sans espaces. Votre phrase de passe devrait compter au moins quatre mots et 15 caractères. Vous pouvez, par exemple, avoir recours à des techniques d'association pour créer votre phrase de passe, notamment en la composant à partir de ce qui se trouve dans une pièce (p. ex. « Armoire lampe Chaise Tapis »).

PROTÉGEZ VOS MOTS DE PASSE ET VOS PHRASES DE PASSE

Les auteurs de menace envoient des courriels **d'hameçonnage** pour vous inciter à dévoiler vos renseignements personnels et, dans certains cas, pour installer un maliciel (comme un enregistreur de frappe). Après avoir installé un **enregistreur de frappe** sur votre appareil, un auteur de menace serait en mesure de saisir les frappes de touche lorsque vous tapez vos mots de passe ou vos phrases de passe. Les attaques par hameçonnage sont courantes, mais vous pouvez vous protéger en suivant les conseils qui figurent dans la publication *ITSAP.00.100, Reconnaître les courriels malveillants,* et en installant des logiciels antimaliciels sur vos appareils.



MOTS DE PASSE COMPLEXES

Si vous ne pouvez pas utiliser une phrase de passe, utilisez un mot de passe aussi complexe que possible (p. ex. lorsqu'un site Web exige que votre mot de passe compte moins de 15 caractères). Un mot de passe composé de majuscules, de minuscules, de chiffres et de caractères spéciaux est bien plus complexe qu'un mot de passe formé uniquement de lettres minuscules.

Vous pouvez aussi utiliser la première lettre de chaque mot d'une phrase complète pour créer un mot de passe complexe plus facile à retenir. Par exemple, la phrase « Le numéro de mon chandail de soccer était le 27! » pourrait donner le mot de passe « L#dmcdsel27! ».

CODES DE VERROUILLAGE OU NIP

Un code de verrouillage ou numéro d'identification personnel (NIP) est une série d'au moins quatre chiffres. Les codes de verrouillage comptent un minimum de quatre chiffres seulement, puisque vos appareils ou vos comptes sont aussi protégés par d'autres mécanismes. Les chiffres de votre NIP doivent toujours être aléatoires. Par exemple, pour accéder à votre compte bancaire, un auteur de menace doit connaître votre NIP ou code de verrouillage et avoir votre carte bancaire en main.

SÉRIE SENSIBILISATION

UTILISEZ L'AUTHENTIFICATION À DEUX FACTEURS

L'authentification à deux (ou à plusieurs) facteurs renforce la sécurité de vos appareils et de vos comptes. Elle offre une meilleure protection puisque l'authentification est effectuée à partir d'au moins deux éléments (un facteur que vous connaissez et un facteur que vous possédez, comme un mot de passe et un jeton, ou un mot de passe et une empreinte digitale) pour ouvrir une session. En ajoutant une couche de protection supplémentaire, l'authentification à deux facteurs vous permet d'utiliser un mot de passe de huit caractères seulement.

Les solutions à deux facteurs ne s'équivalent pas toutes, mais elle permettent d'améliorer globalement la posture de cybersécurité de l'organisation. Les organisations devraient avoir des politiques d'authentification des utilisateurs qui répondent aux besoins, tant sur le plan de la convivialité que celui de la sécurité.

PROTÉGEZ VOS MOTS DE PASSE, VOS PHRASES DE PASSE ET VOS NIP

Les phrases de passe, les mots de passe complexes, les codes de verrouillage et les NIP doivent être traités et conservés avec soin pour empêcher qu'ils ne soient compromis. Tenez compte des conseils suivants :

- Soyez conscient de votre environnement lorsque vous entrez un mot de passe, une phrase de passe, un code de verrouillage ou un NIP en public.
- Utilisez un mot de passe, une phrase de passe ou un NIP différent pour chaque appareil et chaque compte, surtout les comptes qui renferment des renseignements sensibles.
- Ne divulguez jamais vos mots de passe, phrases de passe, codes de verrouillage ou NIP en ligne ou au téléphone.
- Ne dites jamais vos mots de passe, phrases de passe, codes de verrouillage ou NIP à qui que ce soit, même à un membre de la famille.
- Fermez les sessions et faites une déconnexion dans vos comptes ou dans les sites Web lorsque vous avez fini de les consulter.
- Utilisez les phrases de passe et les mots de passe les plus robustes possible pour protéger vos comptes sensibles (p. ex. comptes bancaires, comptes de l'ARC).

ÉVITEZ LES ERREURS COURANTES

S'ils sont créés et protégés adéquatement, les mots de passe, les phrases de passe et les NIP sont des moyens efficaces de protéger vos appareils, vos comptes et vos renseignements. Voici quelques exemples d'erreurs courantes à éviter :

- N'utilisez pas de mots de passe, de phrases de passe ou de NIP faciles à deviner (comme « mot de passe », « laisse-moi entrer » ou « 1234 »), même s'ils comprennent des caractères de remplacement (comme « mot de p@sse »).
- N'utilisez pas d'expressions courantes, de titres ou paroles de chanson, de titres de film ou de citations.
- N'utilisez pas d'information personnelle (comme votre date de naissance, votre ville natale ou le nom de votre animal).

CONNAISSEZ LE FONDEMENT DES RÈGLES

Les règles de création de phrases de passe et de mots de passe ont leur raison d'être. Si vous ne prenez pas de précautions pour protéger vos mots de passe ou vos phrases de passe, les auteurs de menace pourraient facilement s'infiltrer dans vos appareils et vos comptes pour avoir accès à vos renseignements. Les méthodes qu'ils utilisent sont de plus en plus nombreuses et ont souvent recours au hachage de mot de passe, soit une version chiffrée de votre mot de passe en clair. Le code de hachage sert souvent à vérifier vos mots de passe dans les applications ou les sites Web.

Les auteurs de menace ont parfois recours aux méthodes suivantes :

- La **force brute** est une méthode qui consiste à faire des essais successifs en entrant tous les mots de passe courants pour trouver le bon. Cette méthode a habituellement recours à des tables de dictionnaire de mots de passe.
- Les **tables arc-en-ciel** sont des listes de combinaisons de mots de passe précompilées et des codes de hachage correspondants. Elles servent à associer un code de hachage connu à un mot de passe qui permet d'accéder à un compte.

Les mots de passe plus courts sont plus faciles à percer. Vous pouvez toutefois compliquer la tâche aux auteurs de menace qui tentent de pirater vos appareils et vos comptes en utilisant de longues phrases de passe ou des mots de passe plus complexes.

GESTIONNAIRE DE MOTS DE PASSE

Si vous êtes dépassé par le nombre de mots de passe que vous devez retenir, vous pouvez utiliser un gestionnaire de mots de passe pour les générer et les conserver. Les mesures suivantes peuvent vous aider à protéger les mots de passe stockés dans un gestionnaire de mots de passe :

- Stockez uniquement les mots de passe associés à vos comptes peu sensibles, et non à vos comptes sensibles, comme ceux qui nécessitent des privilèges administratifs ou des justificatifs d'identité liés à des comptes bancaires.
- Utilisez un mot de passe robuste et une authentification à deux facteurs pour sécuriser le gestionnaire de mots de passe.
- Vérifiez que le gestionnaire de mots de passe provient d'un site Web sécurisé et qu'il est mis à jour régulièrement.

Avant d'utiliser un gestionnaire de mots de passe, consultez le document *ITSAP.30.025, Conseils de sécurité sur les gestionnaires de mots de passe*.

Vous avez des questions ou besoin d'assistance? Vous voulez en savoir plus sur les questions de cybersécurité? Visitez le site Web du Centre canadien pour la cybersécurité (CCCS) au **cyber.gc.ca.**