Conseils de sécurité sur les gestionnaires de mots de passe

Février 2024

ITSAP.30.025

Il peut être difficile d'utiliser des mots de passe complexes et différents pour chaque site Web, compte et application. La surabondance de mots de passe pourrait vous pousser à faire preuve d'imprudence. Peut-être consignez-vous tous vos mots de passe par écrit ou utilisez-vous toujours un même mot de passe facile à retenir? Adopter de telles habitudes vous met à risque, vous et vos comptes. Pour de plus amples renseignements sur les pratiques exemplaires en matière de mots de passe, consultez l'ITSAP.30.036, *Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques* et l'ITSAP.30.032, *Pratiques exemplaires de création de phrases de passe et de mots de passe*.

Vous pouvez avoir recours à un gestionnaire de mots de passe pour vous aider à créer, à stocker et à retenir vos mots de passe. Ainsi, vous n'aurez pas à retenir des dizaines de mots de passe. Les gestionnaires de mots de passe favorisent l'utilisation de mots de passe complexes et dissuadent les utilisatrices et utilisateurs de recycler les mêmes mots de passe. Quoiqu'ils offrent de nombreux avantages, ces outils exposent néanmoins les renseignements des utilisatrices et utilisateurs à certains risques que nous expliquerons dans le présent document.

Un gestionnaire de mots de passe sert de coffre-fort dans lequel sont stockés les noms d'utilisateur et les mots de passe associés à divers sites Web, applications et services. Leur conception, leurs caractéristiques et leurs vulnérabilités sont uniques. Si vous décidez d'utiliser une gestionnaire de mots de passe, renseignez-vous au sujet des différents fournisseurs afin de prendre une décision éclairée quant à ce qui vous convient le mieux.

Types de gestionnaires de mots de passe

Il existe deux types de gestionnaires de mots de passe : les gestionnaires en ligne et les gestionnaires autonomes.

Gestionnaires de mots de passe en ligne

Les gestionnaires de mots de passe en ligne sont commodes, puisqu'ils sont intégrés à votre navigateur Web et ne vous obligent pas à vous souvenir d'un long mot de passe principal. Ils font appel à la fonction « Se souvenir de moi » au moment où vous vous connectez à un site Web. Cette fonction constitue cependant une vulnérabilité lorsqu'une autre personne a accès à ce même appareil. De plus, comme les gestionnaires de mots de passe en ligne ne synchronisent pas toujours les données d'un appareil à l'autre, vous devez vous souvenir de vos mots de passe lorsque vous ouvrez une session à partir d'un autre appareil. De plus, vous devez garder votre navigateur à jour pour assurer une sécurité optimale.

Gestionnaires de mots de passe autonomes

Pour utiliser un gestionnaire de mots de passe autonome, il faut d'abord installer un logiciel localement ou dans le nuage, puis créer un compte pour accéder au service. En général, ces outils sont plus sécurisés que leurs équivalents en ligne puisqu'ils permettent d'utiliser un mot de passe principal complexe et, habituellement, d'avoir recours à l'authentification à deux facteurs. Ils sont également dotés de fonctions avancées, comme des alertes qui signalent la compromission d'un site Web ou relèvent les mots de passe faibles. Ils vous permettent aussi de synchroniser les mots de passe entre vos appareils.
Peu importe le type de gestionnaire de mots de passe que vous choisissez, nous vous recommandons, dans la mesure du possible, d'activer l'authentification multifacteur (AMF). Pour de plus amples renseignements sur l'authentification multifacteur, consultez l'ITSAP.30.030, *Sécurisez vos comptes et vos appareils avec une authentification multifacteur*.

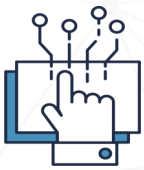
SÉRIE SENSIBILISATION

No de cat. D97-1/30-025-2023F-PDF
ISBN 978-0-660-68383-6

Considérations liées à la sécurité

Les gestionnaires de mots de passe sont des cibles de choix puisqu'ils représentent, en somme, un guichet unique. Quoiqu'ils offrent de nombreux avantages, notamment en vous aidant à gérer une surabondance de mots de passe, ils comportent certains risques; le plus important étant la compromission simultanée de tous vos comptes. Advenant la compromission de votre gestionnaire de mots de passe, que ce soit par l'intermédiaire de votre compte ou suivant la compromission d'un fournisseur, tous les mots de passe associés à vos comptes qui y sont stockés seraient exposés. Si vous choisissez d'enregistrer les mots de passe de vos comptes sensibles (comme votre compte bancaire en ligne), le niveau de risque auquel vous vous exposez s'élèvera en conséquence. Nous vous recommandons d'évaluer l'importance des comptes pour lesquels vous envisagez d'utiliser un gestionnaire de mots de passe et de prendre toutes les précautions possibles si vous décidez de vous en servir.

Il faut prendre en compte de nombreuses considérations liées à la sécurité avant d'utiliser un gestionnaire de mots de passe. Des auteures et auteurs de menace peuvent s'attaquer à votre gestionnaire de mots de passe de plusieurs façons. Ils peuvent, entre autres, tenter d'obtenir votre mot de passe principal en menant une attaque par force brute. Si vous devez écrire votre mot de passe principal sur papier, assurez-vous de l'entreposer convenablement (comme dans un coffre verrouillé) et de restreindre le nombre de personnes qui y ont accès.



Authentification multifacteur

Pour ajouter une couche de sécurité supplémentaire, nous vous recommandons d'utiliser un gestionnaire de mots de passe qui fait appel à l'authentification multifacteur.

Comme les menaces sont de plus en plus sophistiquées (pensons aux attaques par hameçonnage ou à l'enregistrement de la frappe), votre mot de passe principal peut facilement être piraté. C'est pourquoi il est préférable d'avoir recours à l'authentification multifacteur plutôt qu'un mot de passe, puisqu'elle combine plusieurs facteurs, comme quelque chose que vous connaissez, quelque chose qui vous caractérise et quelque chose que vous avez. Par exemple, vous pouvez combiner un mot de passe avec un jeton, une empreinte digitale ou un code additionnel pour accéder à votre gestionnaire de mots de passe.

Conseils sur l'utilisation d'un gestionnaire de mots de passe

- **Utilisez un gestionnaire de mots de passe qui :**
  - prend en charge l'authentification multifacteur;
  - chiffre les mots de passe de manière à n'être visibles que par vous et à être illisibles par le fournisseur (selon une architecture à divulgation nulle de connaissance);
  - vous invite à changer vos vieux mots de passe;
  - signale les mots de passe faibles ou recyclés;
  - révèle la façon dont il protège vos mots de passe;
  - stocke des liens Web légitimes et vous avise des sites Web compromis;
  - vous avise si votre mot de passe semble avoir fait l'objet d'une violation de données connue;
  - s'intègre à votre téléphone, à votre ordinateur, à votre tablette et à vos autres appareils.
- **Utilisez une phrase de passe ou un mot de passe principal robuste**
  - Les phrases de passe sont des phrases mémorisées qui comptent au moins quatre mots (avec ou sans espaces) et un minimum de quinze caractères
  - Les mots de passe comptent au moins douze caractères, dont des lettres majuscules et minuscules, des chiffres et des caractères spéciaux
- **Installez régulièrement les mises à jour du gestionnaire des mots de passe**
- **Utilisez un gestionnaire de mots de passe uniquement pour générer vos propres mots de passe**
- **Évitez d'utiliser le même mot de passe pour différents sites Web**
- **N'enregistrez pas les mots de passe de vos comptes sensibles (comme votre compte bancaire ou votre compte courriel)**
- **Ne divulguez pas votre mot de passe principal**
- **Établissez un plan pour récupérer vos mots de passe si jamais vous perdiez accès au gestionnaire de mots de passe à la suite d'une panne d'ordinateur.**

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