Repensez vos habitudes liées à vos mots de passe de manière à protéger vos comptes des pirates informatiques

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Avril 2024 | ITSAP.30.036

Vous avez des comptes en ligne pour tout, des services gouvernementaux jusqu'au magasinage. Chaque fois que vous créez un nouveau compte, vous devez créer un nom d'utilisateur et un mot de passe. Réutiliser les mêmes justificatifs d'identités dans plusieurs comptes peut être pratique, mais vous rendez ainsi plus facile l'accès à vos comptes et à vos renseignements personnels par les pirates informatiques. Avec un seul mot de passe, ils ont accès à plusieurs comptes.

Réutiliser un mot de passe vous met à risque

Les justificatifs d'identité d'utilisateurs sont de grande valeur pour les pirates informatiques parce qu'ils savent que les gens ont tendance à réutiliser leurs mots de passe plus d'une fois.

Les pirates ciblent les organisations et les personnes, profitent des vulnérabilités des systèmes et des logiciels, envoient des messages d'hameçonnage et en déguisent les logiciels malveillants en fichiers légitimes. Les pirates informatiques utilisent ces techniques pour voler des informations sensibles, comme les justificatifs d'identité des utilisateurs. Une fois qu'ils ont cette information, les pirates informatiques peuvent la vendre ou la publier en ligne, la mettant ainsi à disposition d'autres pirates.

Un mot de passe qui a été volé il y a des années vous met toujours à risque d'être victime de cyberattaques comme le bourrage d'identifiants. Pour vous protéger, évitez de réutiliser un mot de passe, même si vous le jugez complexe et difficile à deviner.

Selon Pensez cybersécurité, 41 % des Canadiennes et Canadiens admettent utiliser le même mot de passe dans plusieurs comptes.

Habitudes à adopter par rapport à vos mots de passe

Le mot de passe est la première ligne de défense de vos comptes. Adopter de bonnes habitudes liées à vos de mots de passe peut vous aider à les sécuriser efficacement.

- Utilisez une phrase de passe ou un mot de passe complexe et unique pour chacun de vos comptes.
- Activez l'authentification multifacteur (AMF) dans vos comptes qui offrent cette option.
  - L'AFM ajoute une couche de protection en demandant de prouver votre identité de plusieurs façons lorsque vous vous connectez à votre compte, en fournissant un code de sécurité ou des identificateurs biométriques.
  - Pour obtenir des instructions sur la configuration de l'AMF dans des services en ligne populaires, consultez les conseils de sécurité en ligne du National Cyber Security Centre du Royaume-Uni dans le document intitulé : Tips for staying secure online: Turn on 2-step verification [en anglais seulement].
- Utilisez un gestionnaire de mots de passe (application autonome ou par navigateur) pour vous aider à vous rappeler vos mots de passe complexes ou phrases de passe uniques. Assurez-vous d'utiliser un mot de passe principal qui est robuste et d'activer l'AFM de votre gestionnaire de mots de passe.
- Ne révélez pas vos mots de passe et phrases de passe à qui que ce soit. Évitez de conserver une copie de vos mots de passe dans un lieu public, par exemple scotché sur le côté de votre ordinateur ou sous votre clavier.
- N'utilisez pas les options « Se souvenir de moi » ou « Enregistrer le mot de passe » lorsque vous utilisez un ordinateur public ou partagé et déconnectez-vous toujours de vos comptes lorsque vous avez terminé vos activité

Bourrage d'identifiants (Credential Stuffing)

Dans le cas d'une attaque par bourrage d'identifiants, les pirates informatiques utilisent des justificatifs d'identité précédemment volés d'un site Web en particulier et « bourrent » les pages de connexion d'autres sites Web ou systèmes jusqu'à ce qu'ils trouvent des correspondances. Les pirates informatiques utilisent des outils comme des réseaux de zombies, un ensemble de robots Internet ou de dispositifs connectés à Internet, et des applications pour tenter d'établir des correspondances entre des justificatifs d'identité et des comptes afin d'automatiser les attaques afin de tester les justificatifs sur plusieurs sites Web.

Lorsqu'un pirate informatique a accès à un compte, il peut :

- modifier votre mot de passe
- voler des informations sur votre carte de crédit
- effectuer des transactions non autorisées
- mener d'autres activités frauduleuses

Des sites Web comme monitor.mozilla.org peuvent vous dire si votre adresse courriel ou votre mot de passe apparaît sur une liste de justificatifs d'identité volés.

Étapes à suivre si un de vos comptes est compromis

1. Changez immédiatement votre phrase ou mot de passe.
2. Si vous avez réutilisé ce mot de passe pour d'autres comptes, assurez-vous de modifier les mots de passe de ces comptes et de ne plus jamais utiliser le mot de passe ou la phrase de passe qui ont été piratés.
3. Vérifiez attentivement les informations de votre compte pour vous assurer qu'il n'y a pas de modifications ou de transactions non autorisées. Le cas échéant, modifiez vos questions et réponses de sécurité.
4. Vérifiez qu'aucune activité suspecte n'ait été menée avec votre carte de crédit ou dans vos comptes bancaires. Si votre carte de crédit est liée à un compte compromis, communiquez avec votre banque.
5. Communiquez avec le Centre antifraude du Canada et avec la police locale si vous suspectez des activités frauduleuses et si vous vous inquiétez d'un vol d'identité. Vous devriez peut-être également communiquer avec un bureau de crédit.
6. Informez vos contacts de la violation de sécurité, car votre compte pourrait être utilisé pour envoyer des messages d'hameçonnage qui semblent provenir de vous.

Pour en savoir plus

Consultez les documents suivants pour en savoir plus sur les points importants que nous avons abordés :

- Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)
- Protéger votre organisation contre les maliciels (ITSAP.00.057)
- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)
- Conseils de sécurité sur les gestionnaires de mots de passe (ITSAP.30.025)

Centre de la sécurité des télécommunications Canada | Communications Security Establishment Canada

Canada

No de cat. D97-1/30-036-2024F-PDF ISBN 978-0-660-71284-0