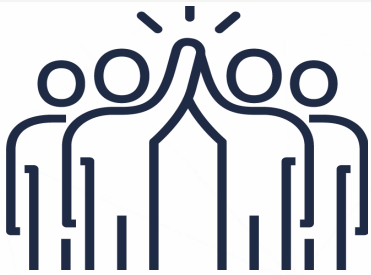
CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Sécurité des TI : enjeux courants chez les employées et employés

Mai 2024

ITSAP.00.005



À titre d'employée ou employé, non seulement vous avez accès à l'information importante et sensible de votre organisation, mais vous avez aussi la responsabilité de la protéger. En ayant des pratiques inadéquates en matière de sécurité, vous rendez vos dispositifs vulnérables aux auteurs de cybermenaces qui pourraient vouloir mettre hors fonction les réseaux de votre organisme et accéder à votre information sensible. Pour éviter ces vulnérabilités, il est indispensable de reconnaître les enjeux courants en matière de cybersécurité et de prendre des mesures pour réduire les risques qui s'y rattachent.

Se laisser piéger par une tentative d'hameçonnage

L'hameçonnage est une forme d'ingénierie sociale et de fraude dans le cadre de laquelle les auteurs de menace tentent de vous amener à ouvrir un courriel malveillant qui contient des pièces jointes ou des liens permettant de télécharger des maliciels sur votre dispositif. Les tentatives d'hameçonnage peuvent avoir pour résultat de compromettre votre organisation et ses informations sensibles. Faites preuve de vigilance et examinez vos courriels avant de les ouvrir.

L'hameçonnage est la façon la plus courante dont les attaquants s'y prennent pour compromettre des systèmes informatiques.

Avoir une sécurité Wi-Fi déficiente

Il existe des points d'accès Wi-Fi pratiquement partout, ce qui est très pratique. Toutefois, utiliser ces réseaux donne aux auteurs de menace des occasions de perpétrer des attaques sur vos dispositifs et d'accéder aux informations qu'ils contiennent. Un point d'accès Wi-Fi qui vous semble inoffensif par analogie avec le lieu d'où vous le consultez, par exemple un café ou un restaurant, pourrait avoir été compromis et servir à des fins malveillantes. Pour réduire ce risque, évitez d'utiliser des points d'accès Wi-Fi inconnus, non protégés ou publics, dans la mesure du possible. Assurez-vous d'avoir mis en place des mesures de sécurité qui vous permettront de protéger vos réseaux, vos systèmes et votre information lorsque vous vous branchez à un point d'accès Wi-Fi public.

Mauvaise gestion de l'information sensible

La perte d'un dispositif, comme une clé USB, un ordinateur portable ou une tablette, pourrait occasionner des problèmes d'ordre financier, juridique ou de relations publiques à votre organisation. Ce genre de problème pourrait aussi entacher votre réputation professionnelle de manière embarrassante. Si vous devez emporter de l'information hors du bureau, adoptez les procédures appropriées. Communiquez avec votre équipe des TI pour vérifier si vos fichiers doivent être chiffrés. Souvenez-vous que le fait de supprimer la mention de sécurité d'un document ne change pas le niveau de sensibilité de l'information que ce document contient.

Utilisation non sécuritaire d'un dispositif mobile

La perte d'un dispositif mobile comme un téléphone, un ordinateur portable ou une tablette, peut permettre un accès non autorisé au réseau de votre organisation. Cela met à risque non seulement votre information, mais aussi celle de votre organisation. Sachez en tout temps où se trouvent vos dispositifs, et demeurez consciente ou conscient de la situation; Si vous constatez qu'un de vos dispositifs manque à l'appel, communiquez immédiatement avec votre service des TI.

Au Canada, on a signalé plus de 150 000 incidents de fraude totalisant des vols évalués à plus de 600 millions de dollars depuis janvier 2021.

Selon un rapport du Centre antifraude du Canada publié en 2023

SÉRIE SENSIBILISATION

Cat. No. D97-1/00-005-2023F-PDF
ISBN 978-0-660-68430-7

Mauvaises pratiques en matière de gestion des mots de passe

Les mots et les phrases de passe constituent des moyens de sécurité simples et votre première ligne de défense. Les mots et les phrases de passe confirment votre identité et mettent vos informations sensibles à l'abri d'un accès non autorisé. Les auteurs de menace peuvent facilement pirater des dispositifs ou des comptes si vous utilisez des mots de passe simples ou si vous utilisez le même mot de passe pour des comptes différents.

Nous vous recommandons d'utiliser des phrases de passe plutôt que des mots de passe dans la mesure du possible. Les phrases de passe sont plus longues et il est plus facile de s'en souvenir, mais pour les auteurs de menace, elles sont plus difficiles à deviner. Vos phrases de passe devraient contenir au moins quatre mots et 15 caractères. Si vous ne pouvez pas utiliser une phrase de passe (certains sites limitent le nombre de caractères qu'il est possible de saisir), adoptez un mot de passe comptant au moins 12 caractères. Assurez-vous d'utiliser à la fois des lettres minuscules et majuscules, de même que des chiffres et des caractères spéciaux.

Voici quelques astuces pour la gestion des mots de passe:

- Choisissez des mots de passe ou des phrases de passe complexes et qui seront difficiles à deviner.
- Utilisez un mot de passe ou une phrase de passe différent pour chaque compte.
- Changez les mots de passe ou les phrases de passe compromis ou qui pourraient avoir été compromis.
- Gardez secrets vos mots de passe ou vos phrases de passe.
- Activez l'authentification multifacteur sur vos comptes.
- Vous pouvez recourir à un gestionnaire de mots de passe pour vous aider à créer, à protéger, à entreposer et à conserver vos justificatifs d'accès.
- Évitez de saisir vos mots de passe sur des ordinateurs publics.
- Gardez votre clavier à l'abri des regards lorsque vous saisissez un mot ou une phrase de passe, ou un NIP.

Téléchargement d'applications non autorisées

Comme il existe une foule d'applications visant à améliorer les flux de travail, vous pourriez avoir la tentation de télécharger sur votre dispositif de travail des applications visant à accroître votre productivité. Toutefois, ceci pourrait mettre votre dispositif et votre réseau à risque en introduisant des vulnérabilités que des auteurs de menace pourraient exploiter.

Assurez-vous de consulter votre service des TI pour savoir si vous avez l'autorisation de télécharger des applications sur votre dispositif, et s'il existe une liste d'applications approuvées. Si vous avez l'autorisation de télécharger des applications, nous vous recommandons d'effectuer une recherche auprès de différents fournisseurs afin de faire un choix éclairé, et de ne télécharger de produits qu'auprès de fournisseurs reconnus, pour réduire les risques au minimum.

Vous devriez aussi tenir vos applications à jour en installant les mises à jour et les correctifs.

Pour en savoir plus

- Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)
- Utiliser le Wi-Fi sans compromettre la sécurité de votre organisation (ITSAP.80.009)
- Protection de l'information de grande valeur : Conseils pour les petites et moyennes organisations (ITSAP.40.001)
- Utiliser son dispositif mobile en toute sécurité (ITSAP.00.001)
- 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)
- Étapes à suivre pour déployer efficacement l'authentification multifacteur (ITSAP.00.105)
- Conseils de sécurité sur les gestionnaires de mots de passe (ITSAP.30.025)
- Application des mises à jour sur les dispositifs (ITSAP.10.096)

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**.