SÉCURITÉ DES TI : DIFFICULTÉS OBSERVÉES CHEZ LES EMPLOYÉS

OCTOBRE 2020

ITSAP.00.005

LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION EST L'AFFAIRE DE TOUS

À titre d'employé, non seulement vous avez accès à l'information importante et sensible de votre organisme, mais vous avez la responsabilité de la protéger. En vous livrant à des pratiques inadéquates en matière de sécurité, vous créez, pour les auteurs de cybermenaces, des occasions de mettre hors fonction les réseaux de l'organisme et d'accéder à l'information sensible. Pour empêcher des cyberattaques, il vous suffit d'éviter certains pièges connus en matière de sécurité.

VICTIME DE TENTATIVE D'HAMEÇONNAGE

Les auteurs de cybermenaces tentent de tromper les employés et de les inciter à ouvrir des courriels, puis à cliquer sur des liens menant à des sites malveillants ou à ouvrir des fichiers joints malveillants. De telles tentatives d'hameçonnage peuvent mener à la compromission de l'information et des systèmes informatiques de votre organisme. Demeurez vigilant et examinez vos courriels avant de les ouvrir.

Pour en apprendre davantage sur le sujet, consultez *Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage*.

L'HAMEÇONNAGE EST ENCORE LA TECHNIQUE LA PLUS SOUVENT EMPLOYÉE DANS LES TENTATIVES DE COMPROMISSION DES SYSTÈMES INFORMATIQUES

SÉCURITÉ WI-FI DÉFICIENTE

La quasi-omniprésence des points d'accès Wi-Fi donne aux auteurs de menaces l'occasion d'accéder aux dispositifs et à l'information d'autrui. Ces points d'accès (p. ex. dans un café ou un restaurant) sont considérés comme inoffensifs, mais pourraient très bien avoir été compromis ou avoir été conçus à des fins malveillantes.

Pour atténuer les risques de compromission, évitez d'utiliser les points d'accès Wi-Fi publics, dont la source est inconnue ou qui ne sont pas protégés. Pour en apprendre davantage sur le sujet, rendez-vous sur le site Web du Centre canadien pour la cybersécurité et consultez l'application interactive *La cybersécurité et les technologies sans fil*.

GESTION LACUNAIRE DE L'INFORMATION SENSIBLE

La perte d'une clé USB, d'un ordinateur portable ou d'une tablette peut engendrer des problèmes financiers ou juridiques pour votre organisme ou encore lui causer des difficultés sur le plan des relations publiques en plus d'entacher votre réputation professionnelle. Lorsque vous devez apporter de l'information en dehors du contexte sécurisé du milieu de travail, suivez les procédures prescrites et prenez contact avec le groupe des TI pour voir si les fichiers à transporter doivent être chiffrés. 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.

ABC DE LA SÉCURITÉ DES DISPOSITIFS MOBILES

La perte, le vol ou la compromission d'un dispositif mobile (p. ex. un téléphone, un ordinateur portable ou une tablette) peut donner lieu à un accès non autorisé au réseau de votre organisme, ce qui menace à la fois la sécurité de votre information et de celle de votre organisme. Pour atténuer ce risque, suivez les conseils prodigués dans le document *ITSAP.00.001 Utiliser son dispositif mobile en toute sécurité.*

> « […] le nombre de Canadiens touchés par une atteinte à la protection des données dépasse largement **28 millions.** »
>
> Selon un rapport sur les déclarations obligatoires des atteintes à la protection des données publié par le Commissariat à la protection de la vie privée du Canada – octobre 2019.

SÉRIE SENSIBILISATION

© Gouvernement du Canada
Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production, reproduction ou publication, en tout ou en partie, est strictement interdite sans l'autorisation expresse du CST.

TÉLÉCHARGEMENT D'APPLICATIONS NON AUTORISÉES

Comme il existe une foule d'applications visant à améliorer les flux de travail, il pourrait être tentant de télécharger des applications non approuvées sur le dispositif fourni par son employeur. Or, comment peut-on savoir ce que l'application produit exactement ou à quelles données cette application aura accès une fois téléchargée? Si vous avez l'autorisation de télécharger des applications, n'acceptez que celles qui proviennent de fournisseurs réputés pour atténuer les risques.

Vous devriez aussi garder vos applications à jour en installant les mises à jour et les correctifs. Pour obtenir de plus amples informations, consultez le document ITSAP.10.096 *Application des mises à jour sur les dispositifs*.

PRATIQUES LACUNAIRES EN MATIÈRE DE GESTION DE MOTS DE PASSE

Mesure de sécurité simple et premier mécanisme de défense, les mots de passe et les phrases de passe permettent de vérifier votre identité et de protéger l'information sensible contre tout accès non autorisé. Les auteurs de menaces peuvent facilement pénétrer un dispositif ou un compte si vos mots de passe sont faciles à deviner ou sont utilisés pour plusieurs comptes. Lorsque vous le pouvez, optez pour des phrases de passe, car elles sont plus longues et plus faciles à mémoriser que les mots de passe, mais plus difficiles à deviner pour les auteurs de menaces.

Votre phrase de passe devrait contenir **au moins quatre mots et 15 caractères**. Par exemple, vous pouvez créer une phrase de passe en balayant une salle du regard et en choisissant des objets que vous voyez(p. ex. « PlacardLampeToiletteTasse »).

- Choisissez des mots de passe ou des phrases de passe complexes qui ne sont pas facilement devinables.
- 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 vos mots de passe ou vos phrases de passe secrets.

Pour obtenir plus de détails sur le sujet, consultez le document ITSAP.30.032 *Pratiques exemplaires de création de phrases de passe et de mots de passe*.

MOTS DE PASSE ET PHRASES DE PASSE ROBUSTES

MISER SUR LA COMPLEXITÉ

Si vous ne pouvez pas utiliser une phrase de passe (p. ex. sur un site Web qui n'autorise pas les mots de passe de plus de 15 caractères), optez pour un mot de passe le plus complexe possible, préférablement d'au moins 12 caractères. Les mots de passe composés de lettres majuscules et minuscules, de chiffres et de caractères spéciaux sont plus complexes que ceux qui contiennent uniquement des lettres minuscules. Il vous faudra aussi respecter les règles de création de mots de passe qui diffèrent selon les sites Web et les applications (p. ex. les lettres, les chiffres, les marques de ponctuation et les caractères spéciaux qui sont obligatoires ou interdits).

Il est aussi recommandé d'opter pour l'authentification à deux facteurs (mot de passe **et** donnée biométrique) lorsque cela est possible. L'authentification à deux facteurs est plus sécuritaire.

ÊTRE VIGILANT

Le piquage de mots de passe peut survenir partout, particulièrement dans les endroits publics. Soyez prudent, observez votre environnement, évitez d'utiliser les ordinateurs publics et gardez toujours votre clavier à l'abri des regards indiscrets lorsque vous entrez un mot de passe, une phrase de passe ou un NIP.

OPTER POUR LA DIVERSITÉ

Rappelez-vous que l'utilisation du même mot de passe ou de la même phrase de passe pour plusieurs comptes accroît les risques de sécurité advenant la découverte de ce mot de passe. Utilisez un mot de passe ou une phrase de passe différent pour chaque compte.

PROTÉGER LES MOTS DE PASSE OU LES PHRASES DE PASSE

Évitez d'inscrire vos mots de passe, vos phrases de passe et vos NIP sur un bout de papier caché sous votre clavier, sur une note autocollante à côté de votre ordinateur ou dans un fichier enregistré dans votre dispositif électronique. 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.

AGIR SANS TARDER

Si vous soupçonnez qu'un mot de passe, une phrase de passe ou un NIP a été compromis, n'attendez pas : changez-le immédiatement et communiquez avec le groupe des TI pour obtenir de plus amples conseils.

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 au **cyber.gc.ca.**