SÉCURITÉ DES TI : DIFFICULTÉS OBSERVÉES CHEZ LES EMPLOYÉS

OCTOBRE 2018 ITSAP.00.005

La sécurité des technologies de l'information est l'affaire de chacun

Certes, les employés ont accès à de l'information importante et sensible, mais ils sont également responsables de la protection de cette information. Dès lors qu'ils se livrent à des pratiques inadéquates en matière de sécurité des technologies de l'information (STI), les employés créent, pour les auteurs de cybermenaces, des occasions de mettre hors fonction les réseaux de leur organisme et d'accéder à des informations sensibles. Pour empêcher les auteurs de cybermenaces de causer des dommages, il faut éviter les pièges qui pourraient amener les utilisateurs à involontairement compromettre la sécurité des TI.

Se laisser tromper par une tentative d'hameçonnage ou de harponnage

Les auteurs de cybermenace ont recours à toutes sortes de ruses pour tromper les utilisateurs et les inciter à ouvrir des courriels, puis à cliquer sur des liens menant à des sites malveillants ou à ouvrir des fichiers joints qui contiennent du code malveillant. Ces tentatives d'hameçonnage peuvent mener à la compromission des systèmes informatiques de votre organisation. Demeurez vigilant et examinez vos courriels avant de les ouvrir. Pour de plus amples renseignements, veuillez lire le document intitulé Reconnaître les courriels malveillants.

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

Pourquoi opter pour une sécurité Wi-Fi déficiente?

La quasi-omniprésence des points d'accès Wi-Fi facilite la tâche des auteurs de menace qui tentent d'accéder aux données confidentielles d'autres utilisateurs. Généralement considérés comme étant pratiques (p. ex. dans un café ou au restaurant), les points d'accès Wi-Fi pourraient très bien avoir été compromis ou avoir été conçus à des fins malveillantes.

Pour atténuer les risques de compromission, il serait préférable que vous limitiez votre utilisation des points d'accès Wi-Fi dont la source est inconnue. Pour de plus amples informations, visionnez la vidéo du CST *La cybersécurité et les technologies sans fil*.

25%

des atteintes à la protection des données résultent d'erreurs commises par les employés.

Étude de la Ponemon Institute intitulée Cost of Data Breach (2016)

Gestion lacunaire de l'information sensible

La perte d'une seule clé USB, d'un seul ordinateur portable ou d'une seule tablette peut engendrer des problèmes financiers ou juridiques ou encore des difficultés sur le plan des relations publiques pour votre organisme et entacher votre réputation professionnelle. Lorsqu'il est nécessaire d'apporter de l'information en dehors du contexte sécurisé du milieu de travail, il est important de suivre les procédures prescrites et de prendre 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. Il conviendra donc de consulter le document Utiliser son dispositif mobile en toute sécurité, dont les conseils vous indiqueront comment vous pourrez grandement atténuer ce risque.

SÉRIE SENSIBILISATION

TÉLÉCHARGEMENT D'APPLICATIONS NON AUTORISÉES

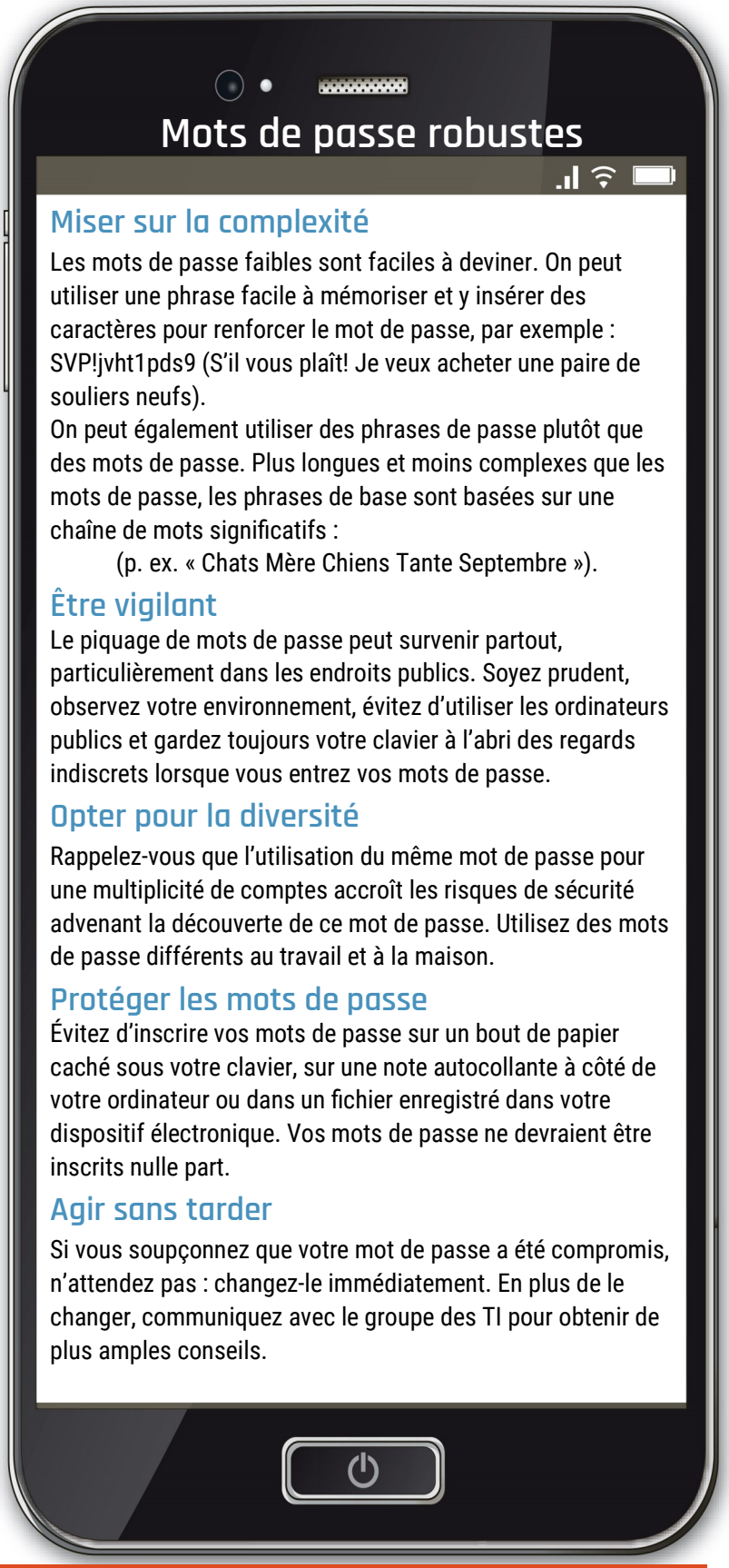
Compte tenu de la multiplicité des applications visant à améliorer les flux de travail, il pourrait être tentant de télécharger des applications non approuvées sur le dispositif fourni par son employeur. Or, comment peut-on savoir ce que l'application produit exactement ou à quelles données cette application aura accès une fois téléchargée? Si vous avez l'autorisation de télécharger des applications, n'acceptez que celles qui proviennent de fournisseurs réputés (p. ex. iTunes, Google Play ou Microsoft).

PRATIQUES LACUNAIRES EN MATIÈRE DE GESTION DES MOTS DE PASSE

Les mots de passe représentent la première ligne de défense et constituent la plus simple des mesures de sécurité. Ils permettent de vérifier l'identité et de contrôler les accès aux informations sensibles, qu'il s'agisse des bases de données de l'employeur ou des données bancaires auxquelles on accède en ligne depuis le domicile.

- Il conviendra d'utiliser des mots de passe complexes qui ne sont pas facilement devinables.
- Il importe d'utiliser des mots de passe différents pour chaque compte et de les modifier régulièrement.
- Il faut changer les mots de passe qui ont été compromis ou pourraient avoir été compromis.
- Il est primordial de garder les mots de passe secrets.

Comprendre la sécurité des TI n'est pas si difficile, et c'est particulièrement important dans le contexte technologique actuel. En évitant les pièges tendus, vous contribuerez au renforcement de la posture de sécurité de votre organisme et décourager les auteurs de menace.



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 (CCC) au **cyber.gc.ca.**