CONSEILS DE CYBERSÉCURITÉ POUR LE TÉLÉTRAVAIL

AVRIL 2020

ITSAP.10.116

Au bureau, vous bénéficiez des mesures de sécurité qu'a prises votre organisation pour protéger ses réseaux, ses systèmes, ses dispositifs et son information contre les cybermenaces. Bien que le travail à distance soit pratique et offre de la souplesse aux employés, il peut affaiblir la posture de sécurité de votre organisation et vous exposer à des risques si vous ne prenez pas de précautions. Les conseils que nous présentons ici vous permettront d'adopter de bonnes pratiques de cybersécurité lorsque vous travaillez à la maison, dans un café ou dans tout autre endroit public.

APPAREILS MOBILES

En l'absence d'un poste de travail désigné, vous devrez avoir recours à des appareils mobiles (comme un téléphone intelligent, un portable ou une tablette) pour travailler à distance. Dans la mesure du possible, utilisez uniquement des dispositifs fournis par votre employeur.

- **Utilisez l'authentification multifactorielle.** Vous pouvez ajouter une couche de sécurité sur vos appareils en modifiant vos paramètres de manière à exiger deux facteurs d'authentification différents pour les déverrouiller. Par exemple, vous pouvez utiliser un mot de passe **ET** une caractéristique biométrique, comme une empreinte digitale.
- **Gardez vos dispositifs à la vue en tout temps.** Ne laissez pas vos appareils sans surveillance lorsque vous travaillez dans un lieu public, et signalez immédiatement la perte ou le vol d'un dispositif au centre de soutien technique de votre organisation.
- **Soyez conscient de votre environnement.** Méfiez-vous des personnes qui vous entourent et qui pourraient écouter votre appel téléphonique ou vous épier pendant que vous tapez votre mot de passe.
- **Faites les mises à jour et appliquez les correctifs sur vos appareils**. Les mises à jour et les correctifs permettent de corriger les vulnérabilités de sécurité et de protéger vos appareils contre les auteurs de menace.
- **Activez les pare-feux et les logiciels antivirus**. Les pare-feux bloquent le trafic malveillant et les logiciels antivirus balayent les fichiers pour détecter les maliciels.

RÉSEAU SANS FIL

Lorsque vous travaillez de la maison, vous devriez prendre certaines mesures pour protéger votre réseau sans fil (Wi-Fi). Modifiez le mot de passe par défaut que vous a donné votre fournisseur et choisissez une phrase de passe ou un mot de passe fort qui ne sera pas facile à deviner.

En travaillant à distance, vous avez la possibilité de vous installer n'importe où. Que vous travailliez à la maison, à la bibliothèque ou dans un café, vous devriez toujours utiliser un réseau sans fil sécurisé. Évitez d'envoyer de l'information sensible sur un réseau sans fil public, qu'il s'agisse de renseignements personnels ou d'information liée au travail. Un réseau privé virtuel (RPV) constitue un autre moyen de protéger l'information. Il s'agit d'un tunnel chiffré sécurisé par l'intermédiaire duquel l'information est transmise.

HAMEÇONNAGE ET PIRATAGE PSYCHOLOGIQUE

Les escrocs réussissent à voler des renseignements sensibles en se faisant passer pour quelqu'un d'autre. Ils peuvent même utiliser l'information trouvée dans vos comptes de médias sociaux pour vous faire penser qu'ils vous connaissent — une tactique appelée piratage psychologique.

- **Soyez vigilant**. Méfiez-vous des messages ou des appels d'une personne que vous ne connaissez pas et des demandes reçues de façon imprévue.
- **Faites-vous confiance**. Si un appel téléphonique ou un message semble menaçant ou trop beau pour être vrai, faites confiance à vos instincts et n'y donnez pas suite.
- **Pensez-y à deux fois**. Vérifiez l'URL d'un lien en pointant votre curseur sur le lien, et n'ouvrez pas de pièces jointes que vous ne vous attendiez pas à recevoir.
- **Péchez par excès de prudence.** Évitez d'envoyer de l'information sensible par courriel ou par texto.

POUR EN SAVOIR PLUS

Les conseils présentés ici constituent un bon point de départ, mais vous pouvez en apprendre plus dans les publications ci-dessous :

- *ITSAP.00.100 Reconnaître les courriels malveillants*
- *ITSAP.00.266 Messagerie instantanée*
- *ITSAP.10.096 Application des mises à jour sur les dispositifs*
- *ITSAP.30.032 Pratiques exemplaires de création de phrases de passe et de mots de passe*
- *ITSAP.80.101 Les réseaux privés virtuels*

Toutes ces publications (et d'autres ressources) sont accessibles sur le site Web du Centre canadien pour la cybersécurité à l'adresse **cyber.gc.ca**

SÉRIE SENSIBILISATION