Conseils de cybersécurité pour le télétravail

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Mars 2024 | 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. Le travail à distance est pratique et offre de la souplesse. Toutefois, 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.

Dispositifs mobiles

En l'absence d'un poste de travail désigné, vous devrez avoir recours à des appareils mobiles, comme un téléphone intelligent, un portable et une tablette pour travailler à distance. Dans la mesure du possible, utilisez uniquement des dispositifs fournis par votre employeur. Si vous n'avez pas reçu un dispositif de travail, veuillez communiquer avec votre organisation pour obtenir des conseils sur les produits approuvés par l'organisation. Des points terminaux non sécurisés peuvent représenter un risque pour les données et le réseau de votre organisation.

Utilisez l'authentification multifacteur : Vous pouvez ajouter une couche de sécurité sur vos appareils en modifiant vos paramètres de manière à exiger 2 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 les laissez pas sans surveillance lorsque vous travaillez dans un lieu public. Signalez immédiatement le vol ou la perte de votre dispositif à votre bureau des services TI, et ce, qu'il s'agisse d'un dispositif appartenant à l'organisation ou d'un dispositif personnel.

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.

Appliquez les mises à jour et les correctifs sur vos dispositifs : Les mises à jour et les correctifs permettent de corriger les vulnérabilités de sécurité et de protéger vos dispositifs contre les auteures et auteurs de menace.

Activez les pare-feu et les logiciels antivirus : Les pare-feu bloquent le trafic malveillant et les logiciels antivirus balayent les fichiers pour détecter les maliciels.

Pour en apprendre plus sur la façon d'assurer la sécurité de votre dispositif, consultez :

- Application des mises à jour sur les dispositifs (ITSAP.10.096)
- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)
- Messagerie instantanée (ITSAP.00.266)
- Considérations de sécurité liées aux pare-feu (ITSAP.80.039)

Hameçonnage et piratage psychologique

Les escrocs réussissent à voler de l'information sensible 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.

Demeurez vigilante ou 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 l'appel téléphonique ou le message est menaçant ou semble trop beau pour être vrai, c'est probablement le cas.

Pensez-y 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.

Vérifiez les faits : Les escrocs ont aussi recours à la mésinformation pour mieux promouvoir les fraudes par hameçonnage. Les escrocs cherchent à provoquer chez la lectrice ou le lecteur une réaction émotionnelle associée, par exemple, au choc ou à l'indignation, mais cette information peut ne pas être vraie. Avant de cliquer sur des liens ou de répondre aux messages, vérifiez l'information et le nom de domaine.

Pour en apprendre plus sur le piratage psychologique et savoir comment le détecter, consultez :

- Piratage psychologique (ITSAP.00.166).
- Reconnaître les courriels malveillants (ITSAP.00.100)
- Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)
- Qu'est-ce que l'hameçonnage vocal (ITSAP.00.102)
- Repérer les cas de mésinformation, désinformation et malinformation (ITSAP.00.300)

Sécurité du Wi-Fi et réseau privé virtuel

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. Pour en apprendre davantage, reportez-vous à la publication Les réseaux privés virtuels (ITSAP.80.101)

Matériel Wi-Fi

Tenez compte du matériel auquel est connecté votre Wi-Fi, plus particulièrement lorsque vous travaillez à distance.

Il vous appartient d'assurer la sécurité et le maintien des routeurs qui ne sont pas pris en charge par votre organisation, comme ceux que vous avez à la maison. Comme n'importe quel autre matériel, les routeurs vont éventuellement arriver en fin de vie. Les dispositifs qui sont en fin de vie représentent un risque pour la sécurité de votre organisation. La fin de vie signifie que le fournisseur cesse la commercialisation, la vente et le soutien technique ainsi que les mises à jour du dispositif. Lorsque vous utilisez des dispositifs sur lesquels les plus récentes mises à jour de progiciels n'ont pas été appliquées, vous vous exposez à des cyberattaques.

Un progiciel est un logiciel qui a été installé et mis à jour par le fabricant, et qui contient d'importantes mesures de sécurité. Vous pouvez vérifier si votre dispositif est en fin de vie en consultant la liste de produits en fin de vie du fournisseur ou en accédant aux dossiers du routeur dans les journaux du système. S'il n'a pas été mis à jour depuis plusieurs mois, il serait peut-être temps de songer à vous procurer un nouveau routeur. En cas de doute, communiquez avec l'équipe des services informatiques de votre organisation qui saura vous conseiller.

Pour en apprendre davantage, reportez-vous aux publications Pratiques exemplaires en matière de cybersécurité pour les routeurs (ITSAP.80.019) et Produits obsolètes (ITSAP.00.095)

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada