Centre intégré universitaire de santé et de services sociaux du Saguenay–Lac-Saint-Jean
Québec

AIDE-MÉMOIRE
Comportements informatiques sécuritaires

1. Soyez extrêmement vigilants sur les messages de type hameçonnage (phishing) – Courriel et SMS

Les cybercriminels aiment les périodes de crise. Les dernières semaines ont entraîné une augmentation considérable des escroqueries en lien avec des courriels professionnels. Celles-ci ont entraîné le piratage de comptes Office365, de messagerie Outlook ou de comptes Google par exemple. Les tentatives d'hameçonnage peuvent également survenir par le biais de la messagerie texte (SMS/Textos) ou d'appels téléphoniques.

Soyez à l'affût des courriels et messages textes d'hameçonnage conçus pour vous inciter à cliquer sur la dernière nouvelle ou le dernier outil lié aux protections contre le Coronavirus (COVID-19).

Évitez de visiter des sites Web méconnus comportant des cartes du monde démontrant la progression du virus. Dans un même ordre d'idées, évitez les applications mobiles de suivis de la progression du virus.

Ne téléchargez aucun logiciel depuis Internet.

Si une situation vous paraît le moindrement suspicieuse ou si vous avez le moindre besoin d'informations en lien avec la sécurité informatique, n'hésitez pas et contactez immédiatement le service informatique du CIUSSS au reg02.dri.support@ssss.gouv.qc.ca ou au poste téléphonique 2646.

Cette vigilance doit être accrue autant dans l'utilisation d'Internet que dans l'usage des stations de travail ou des appareils mobiles.

2. Bureau de la maison

Afin de préserver la confidentialité de l'information que vous traitez, il est recommandé d'installer votre espace de travail dans un endroit isolé et à l'abri des regards. Lorsque vous quittez votre station de travail temporairement, prenez soin de verrouiller votre session de travail. À la fin de la journée, prenez le temps de fermer vos logiciels, vos sessions en ligne et votre accès distant (votre jeton).

3. Pratiquer une bonne cyberhygiène

Dans un ordre plus général, il est important de garder une bonne « hygiène numérique » :

- Assurez-vous que tous vos comptes numériques (ex. courriel, réseaux sociaux, banques, etc.) aient un mot de passe robuste.
- Évitez les mots de passe comme soleil123, 123456789, password, dieu, amour, etc.

- Évitez d'utiliser le WiFi dans un lieu public ou de vous connecter à un réseau sans-fil inconnu ou un réseau sans-fil sans mot de passe.
- Si disponible, favoriser l'utilisation de l'authentification multifacteurs sur tous les comptes numériques pour lesquels elle est disponible.
- Ne laissez pas vos enfants ou d'autres personnes utiliser votre station de travail ou votre appareil mobile. Surtout lorsqu'il s'agit d'appareils que vous utilisez pour votre travail.
- Faites attention aux informations que vous publiez sur les réseaux sociaux (informations personnelles, numéro de téléphone, message, numéro d'employé, etc).
- Faites attention aux sites web que vous consultez.
- Favorisez les sites web de « streaming » légitimes (ex. Netflix, Disney+, Tou.TV).
- Évitez les sites de Torrents ou de « streaming » illégaux.

4. Utilisez uniquement le WiFi sécurisé

N'utilisez qu'un accès WiFi protégé par mot de passe ROBUSTE

N'utilisez pas un accès WiFi public (restaurants, hôtels, autres). Si vous devez utiliser le WiFi public, assurez-vous de vérifier auprès du propriétaire que le réseau auquel vous vous connectez est son réseau légitime et est sécurisé par un mot de passe (ex. l'accès WiFi du CIUSSS).

Évitez d'accéder à des informations confidentielles ou sensibles à partir d'un réseau WiFi public (ex. compte bancaire). Les pirates essaieront de vous tromper en imitant le nom d'un réseau sécurisé.

5. Signaler immédiatement les appareils perdus ou volés

Le travail à distance augmente le risque de perte ou de vol de vos appareils. Assurez-vous de signaler *immédiatement tout* appareil perdu ou volé au service informatique du CIUSSS afin de minimiser le risque de compromission et de fraude.

6. Signaler immédiatement les événements suspicieux

Le contexte de la crise actuelle favorise les cyberattaques. Si vous avez un doute sur un message, un appel téléphonique ou tout autre événement suspicieux, signalez-le immédiatement au service informatique du CIUSSS, au reg02.dri.support@ssss.gouv.qc.ca ou au 2646, afin de minimiser les risques de compromissions et de fraudes.

7. Réception des appels de soutien technique

IMPORTANT : Vous ne recevrez aucun appel de la part de Microsoft ou autre organisation que le CIUSSS du Saguenay–Lac-Saint-Jean pour vous soutenir au niveau informatique. Si vous recevez un appel de la sorte, vous devez impérativement le signaler au service informatique du CIUSSS.