Communication
COVID-19

DESTINATAIRES : Tous les médecins et toutes les personnes œuvrant dans l'établissement

DATE : Le 18 août 2020

OBJET : Cybercriminalité : Soyez vigilants en temps de pandémie

---

Le contexte actuel de pandémie est malheureusement propice à une hausse des tentatives de piratage informatique et autres manœuvres frauduleuses par lesquelles des personnes mal intentionnées tenteront de vous soutirer des informations sensibles ou de l'argent (rançongiciels). Certains types de fraudes reposent aussi sur le chantage et la manipulation psychologique (ingénierie sociale). Nous vous rappelons l'immense importance de déclarer rapidement ce genre d'incident au moyen de l'adresse courriel : incident.informatique.cisssca@ssss.gouv.qc.ca.

Pour éviter la fraude :

- Réduisez au minimum vos accès aux répertoires et systèmes d'information inutiles à votre travail;
- Limitez au maximum l'octroi de comptes à privilèges élevés;
- Portez attention aux pièces jointes des courriels que vous recevez;
- Abstenez-vous de cliquer sur des liens provenant d'expéditeurs inconnus;
- Vérifiez l'adresse du lien avant de cliquer dessus;
- Exigez un numéro de téléphone de rappel si la tentative de fraude est téléphonique;
- En personne ou virtuellement, ne divulguez jamais d'informations à une personne inconnue et avisez votre supérieur.

Si vous croyez avoir été victime de fraude au travail, écrivez à l'adresse incident.informatique.cisssca@ssss.gouv.qc.ca.
Lisez le dépliant en pièce jointe pour savoir comment éviter les pièges des cybercriminels.

Yvan Fournier
Directeur des ressources informationnelles

p. j. Dépliant sur la cybersécurité

Contenu et diffusion approuvés par : Isabelle Barrette

Pour en savoir plus sur les menaces potentielles et comment les éviter

Rendez-vous sur le site de l'ENA au fcp.rtss.qc.ca, connectez-vous avec votre nom d'utilisateur et votre mot de passe de session Windows au bureau, entrez « cybersécurité » dans le moteur de recherche et cliquez sur la formation « Cybersécurité : mission possible ».

Plus d'information sur la cybersécurité :

https://www.pensezcybersecurite.gc.ca/cnt/rsks/cmmn-thrts-fr.aspx#s08

Huit mythes les plus répandus en matière de cybercriminalité :

- Les risques de piratage d'un ordinateur ou d'une tablette sont faibles;
- Les applications sont plus sûres qu'un navigateur;
- Pare-feu + antivirus = protection totale;
- Croire qu'on n'a pas de données sensibles;
- Se dire qu'un MAC est plus sûr;
- Un Wifi ne peut être piraté s'il est caché;
- Les services du Cloud ne sont pas sûrs;
- Les logiciels de protection ralentissent l'ordinateur.

COM 2020-079

Centre intégré de santé et de services sociaux de Chaudière-Appalaches
Québec

www.cisssca.com

Cybersécurité

Soyez vigilants!

Québec

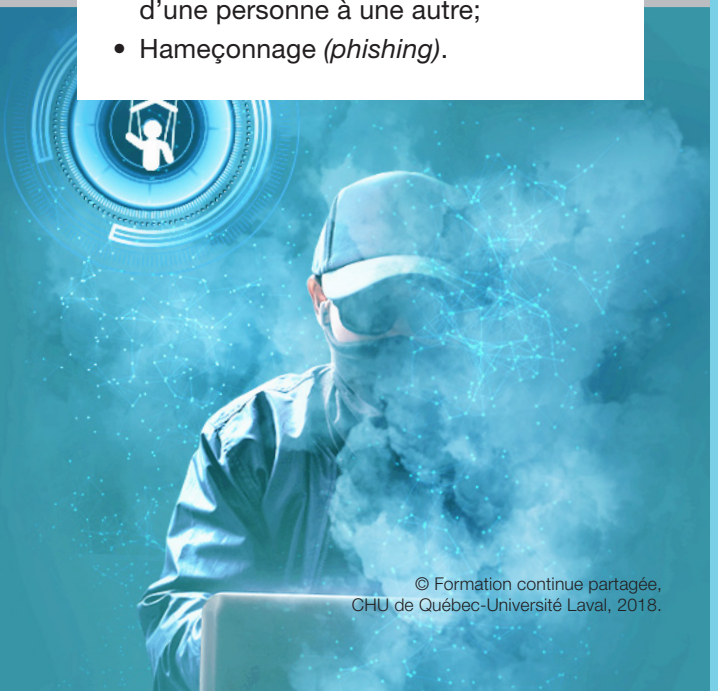
Les vecteurs de propagation d'un virus informatique

La porte d'entrée d'un virus informatique est l'action de l'utilisateur, autrement dit :

Pas d'action (cliquage ou autre), pas de virus. Le maillon faible de la sécurité informatique, **c'est VOUS**.

Portes d'entrée des cybercriminels :

- Courriels frauduleux, souvent au nom d'une compagnie réelle;
- Sites Internet;
- Clé USB et disque dur externe;
- Téléphone et tablette électronique;
- Logiciels et applications «gratuits»;
- Divulgation d'informations confidentielles à un inconnu;
- Divulgation verbale d'information d'une personne à une autre;
- Hameçonnage *(phishing)*.



Les pratiques cybersécuritaires

- Supprimez tous les courriels provenant d'expéditeurs inconnus;
- Videz régulièrement la corbeille;
- Abstenez-vous de cliquer sur une pièce jointe provenant d'expéditeurs inconnus;
- Évitez de donner votre adresse courriel professionnelle si ce n'est pas pour le travail;
- Au bureau, limitez l'utilisation de votre courriel et d'Internet à votre travail;
- Fermez votre session lorsque vous quittez votre poste de travail;
- Supprimez tout courriel inhabituel (s'il a été envoyé par une connaissance, elle vous enverra à nouveau le courriel ou communiquera avec vous autrement);
- Signalez tout courriel ou fichier suspect à la Sécurité de l'information à l'adresse : incident.securiteinformatique.cisssca@ssss.gouv.qc.ca;
- Ne laissez personne introduire une clé USB dans votre ordinateur;
- Informez-vous auprès du Service informatique pour toute installation de logiciels sur votre poste de travail;
- Ne donnez à personne le mot de passe lié à vos accès de connexion pour le branchement au réseau fixe ou au Wifi de l'établissement;
- Ne révélez aucun renseignement à un tiers, surtout par téléphone, et vérifiez l'identité de votre interlocuteur (son nom, son numéro de téléphone, son employeur, etc.).

Cybersécurité : ce qu'il faut savoir

Il existe différents types de logiciels malveillants, soit des programmes informatiques visant à :

- Vous espionner;
- Voler, altérer ou détruire vos données.

Ces programmes peuvent également avoir la capacité de se propager d'un ordinateur à un autre.

Le pourriel

- Utilisé par des personnes malveillantes pour envoyer ou obtenir de l'information;
- Est dérangeant;
- Impose un fardeau aux fournisseurs de services de communication et aux entreprises, qui doivent filtrer les messages électroniques;
- Tente d'obtenir des informations en vous incitant à cliquer sur des liens proposant des offres et des promotions trop belles pour être vraies;
- Permet aux programmes malveillants, aux escroqueries, à la fraude et aux menaces d'atteindre votre ordinateur, créant ainsi un risque d'atteinte à votre vie privée.

Le hameçonnage (phishing)

- Technique malveillante, facile à utiliser et courante;
- Se présente la plupart du temps sous forme de faux courriels, de messages textes et de sites Web imitant les logos et l'apparence associés à des entreprises réelles;
- Les cybercriminels les envoient pour vous voler vos informations personnelles et financières;
- Aussi connu sous le nom de «mystification».