Centre intégré universitaire de santé et de services sociaux de l'Est-de-l'Île-de-Montréal
Québec

Note de service

Destinataire : Tout le personnel du CIUSSS de l'Est-de-l'Île-de-Montréal

Expéditeur : Stéphane Gagnon, conseiller cadre – responsable de la sécurité de l'information (RSI)

Date : Le 25 février 2022

Objet : Cybersécurité – Situation politique en Ukraine

Bonjour,

Le Centre canadien pour la cybersécurité désire rappeler à la population que la situation politique actuelle en Ukraine, est propice pour les pirates informatiques désirant lancer des attaques contre les entreprises et organisations incluant celles faisant partie du réseau de la santé et des services sociaux québécois. Le courriel frauduleux via des campagnes d'hameçonnage ou « phishing » demeure la meilleure tactique pour eux.

Les types de courriels les plus fréquemment utilisés par les pirates informatiques sont les suivants :

- **Informations (vidéo, fausse nouvelle)**
  La victime reçoit un faux courriel prétendant contenir des séquences vidéo exclusives de l'Ukraine ou des liens vers des sites Internet frauduleux.

- **Demande d'aide**
  La victime reçoit un faux courriel d'une personne lui demandant de l'aide pour quitter le pays en lui envoyant de l'argent.

- **Alerte bancaire**
  La victime reçoit un courriel d'une institution bancaire ou d'une carte de crédit lui indiquant qu'une fraude a été suspectée. Afin que le compte ne soit pas bloqué, elle est invitée à cliquer sur le lien et se connecter pour confirmer que les informations sont véridiques.

- **Désactivation des accès à un site Internet**
  La victime reçoit un faux courriel lui mentionnant que ses accès informatiques sont désactivés et qu'elle doit se connecter sur le site Internet pour les valider. Il y a un lien Internet dans le courriel qui amène la personne à se connecter sur un faux site et celle-ci inscrit son code d'utilisateur et son mot de passe qui est alors intercepté par le pirate informatique.

Voici quelques bonnes habitudes à adopter :

- Ne jamais utiliser le courriel du CIUSSS-EMTL pour effectuer des achats en ligne ;
- Porter attention à l'adresse du destinataire ;
- Porter attention à l'adresse du site web (du lien) ;
- Ne jamais cliquer sur un lien douteux ou sur une pièce jointe dont vous ne connaissez pas la provenance ;
- Ne pas faire suivre ou répondre à un courriel douteux ;
- Ne pas oublier que les institutions bancaires ou de crédit ne vous demanderont jamais votre NIP ou vos informations personnelles dans un courriel ou par un site web.

Nous vous demandons de contacter rapidement le service des ressources informationnelles au poste 5656 si vous constatez :

- Des messages intempestifs ;
- Un comportement anormal de votre poste de travail ;
- Des caractères étranges apparaissant à l'écran ;
- Des fichiers renommés automatiquement.

Aidez-nous à poser les bons gestes collectivement pour protéger ces données sensibles et confidentielles !