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) – Direction de la qualité, évaluation, performance et éthique

Date : Le 2 décembre 2021

Objet : Cybersécurité - Hameçonnage et temps des fêtes

Bonjour,

La période du temps des fêtes, étant à nos portes, est une occasion parfaite pour les fraudeurs de s'emparer des données personnelles ainsi qu'aux personnes mal intentionnées de commettre des méfaits. La façon la plus simple étant de piéger un grand nombre de personnes en envoyant un courriel électronique frauduleux via des campagnes d'hameçonnage ou « phishing ».

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

- **Suivi d'un colis**
  La victime reçoit un faux courriel d'une entreprise (Ex. : Amazon, UPS, Purolator), l'invitant à cliquer sur un lien afin d'effectuer le suivi de son colis.

- **Refus d'une transaction**
  La victime reçoit un faux courriel l'avisant qu'une transaction a été refusée et l'invite à cliquer sur un lien pour autoriser la transaction.

- **Faux solde**
  La victime reçoit un faux courriel lui offrant un solde ou une carte cadeau pour des achats en ligne. Pour obtenir le solde ou la carte, elle doit cliquer sur un lien qui semble légitime, mais qui est en fait frauduleux.

- **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 afin de confirmer que les informations sont véridiques.

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 ;
- **Le plus important est se poser les questions suivantes:**
    - **Suis-je client de cette banque?**
    - **Ai-je commandé du matériel dans ce magasin ou sur ce site web ?**

Par ailleurs, 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 !

Nous en profitons également pour vous souhaiter un beau temps des fêtes.