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) à la gestion des risques et sécurité de l'information

Date : Le 21 mars 2022

Objet : Cybersécurité – Hameçonnage usurpant l'image de «Poste Canada»

Bonjour,

Le centre opérationnel de cyberdéfense de la santé (COCD) désire vous informer que depuis plusieurs jours, il y a une augmentation du nombre de campagnes d'hameçonnage qui usurpe l'image de « Poste Canada ». Des acteurs malveillants utilisent une copie de la page web du site de livraison en attente. Ce site est identique à l'officiel de Poste Canada.

Ces courriels d'hameçonnage peuvent être identifiés grâce à :

- Expéditeurs qui changent régulièrement, beaucoup utilisent une adresse telle que :
  - donotreply-nepasrepondre-notifications.canadapost-postes.#####.msn.info@#####.XX

- Sujets divers :
  - You Have Unpaid Package - Canada Post ;
  - Confirmation of Shipment Details for Item / Confirmation des détails de l'envoi de l'article : TRACKING ############## ;
  - Delivery Notification for Item / Avis de livraison pour l'article.

- Certains courriels contiennent une pièce jointe en format PDF, Word, ou Excel ;

- Les liens vers le faux site web sont variés.

Ci-dessous, un exemple de courriel que vous pourriez recevoir :

From: CanadaPost° item:1450420 <donotreply-nepasrepondre-notifications.canadapost-postes.canada.msn.info@j[redacted]n.com>
Sent on: Tuesday, March 15, 2022 11:18:27 AM
To: [redacted]
Subject: Confirmation of Shipment Details for Item / Confirmation des détails de l'envoi de l'article :TRACKING 14504[redacted]4700
Attachments: Confirmation of Shipment Details for Item Confirmation des détails de l'envoi de l'article TRACKING 1450[redacted]4700 (49.28 KB)

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 via courriel ou par un 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 !