Communication
COVID-19

DESTINATAIRES : Tous les employés du CISSS de Chaudière-Appalaches

DATE : Le 9 avril 2020

OBJET : Vigilance à l'égard de la sécurité informatique

Les cybercriminels profitent de la COVID-19 en ciblant les hôpitaux afin de crypter leurs données pour en tirer profit. Un type précis de rançongiciel (fraude par laquelle de l'argent est exigé) semble se propager par courriel ces derniers temps. L'émetteur du courriel se fait passer pour un employé d'une agence gouvernementale et prétend offrir des informations ou des conseils sur le coronavirus. Il encourage le destinataire à cliquer sur un lien ou une pièce jointe qui sont en réalité des virus informatiques.

Ensemble, protégeons les données du CISSS de Chaudière-Appalaches

Quelques conseils à appliquer :

- Ouvrez uniquement des courriels provenant de sources fiables;
- Ne cliquez jamais sur les liens ou les pièces jointes de courriels dont vous n'attendiez pas la réception, et n'ouvrez aucun message provenant d'un expéditeur inconnu;
- Utilisez des systèmes de messagerie sécurisés pour vous protéger des pourriels qui pourraient être infectés;
- Sauvegardez fréquemment tous vos fichiers importants, et stockez-les dans le réseau de l'établissement;
- Utilisez des mots de passe robustes (difficiles à deviner) et uniques pour tous les systèmes, et faites-en la mise à jour régulièrement.

Fraude : en ligne ou par téléphone
Gardez à l'esprit que la fraude téléphonique et l'hameçonnage augmentent, car les cybercriminels adaptent leurs techniques à la situation actuelle. Les escroqueries liées à la COVID-19 comprennent :

- La fraude téléphonique – les criminels appellent des gens en se faisant passer pour des responsables de cliniques ou d'hôpitaux, et affirment qu'un parent de la personne appelée est atteint du virus. Ils demandent des paiements pour des soins médicaux;
- Le hameçonnage : de faux courriels prétendant provenir d'autorités sanitaires nationales ou mondiales incitent les individus à fournir des informations personnelles ou des détails de paiements, ou encore à ouvrir une pièce jointe contenant des logiciels malveillants.

…2

Les cybercriminels ciblent les établissements de santé critiques avec un rançongiciel
Les hôpitaux et autres institutions de première ligne dans la lutte au coronavirus sont confrontés à des dangers concrets, mais aussi à des menaces de cybercriminels. Interpol a lancé un avertissement aux organisations de première ligne dans la lutte mondiale à la pandémie, car elles sont devenues les cibles de rançongiciels, qui verrouillent leurs systèmes d'informations critiques dans le but de leur extorquer des paiements.

Fournitures médicales et médicaments contrefaits
Les criminels profitent de la pandémie pour gagner de l'argent. Nous constatons une augmentation des articles médicaux contrefaits disponibles en ligne, y compris les masques chirurgicaux jetables, les désinfectants pour les mains, les médicaments antiviraux et antipaludiques, les vaccins et les ensembles de tests de dépistage de la COVID-19.

Redoublez de vigilance dans l'achat de produits, particulièrement en ligne.

Pour en savoir davantage : https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-rançongiciel

L'équipe de sécurité de l'information du CISSS de Chaudière-Appalaches