CÉGEP de St-Félicien

Guide des bonnes pratiques en cybersécurité

Voici un rappel des bonnes pratiques de cybersécurité

Nous vous référons à la définition du ministère de la Sécurité publique de l'hameçonnage et des rançongiciels :

Hameçonnage : L'hameçonnage (phishing, en anglais) consiste la plupart du temps à envoyer un courriel en demandant des renseignements personnels précis et en prétendant faussement qu'il provient d'une institution réputée et de confiance, telle qu'une institution financière, une entité gouvernementale ou une entreprise commerciale reconnue.

Rançongiciel : Un rançongiciel (de l'anglais ransomware, logiciel rançonneur, logiciel de rançon ou logiciel d'extorsion) est un logiciel malveillant qui prend en otage des données personnelles ou détruit des données.

Comment se présentent les tentatives d'hameçonnage et de rançongiciel ?

Principalement sous la forme de courriels, elles peuvent se présenter comme de fausses factures, de faux avis de paiement, de faux messages vocaux en pièces jointes, de demandes de changement de mot de passe d'une institution financière, de fichiers joints infectés ou de menaces concernant votre intégrité personnelle.

Être vigilant

Votre vigilance est le meilleur outil de sécurité face à ce type d'attaque. **Aucun outil informatique ne permet de s'en prémunir à 100 % et seule l'intervention humaine permet de s'en prémunir.** Cette vigilance est nécessaire autant lors de l'utilisation d'un appareil personnel que d'un appareil appartenant au cégep.

Quelques exemples…

- Un courriel d'hameçonnage typique présente un message à caractère urgent, demandant de cliquer sur un lien menant vers un site Web falsifié et imitant à la perfection celui de l'institution réputée. Une fois sur le faux site, l'internaute est invité à fournir ses renseignements personnels ou télécharger des fichiers infectés.

- Un rançongiciel peut se présenter sous la forme de pièces jointes à un courriel qui peuvent comporter des virus et logiciels malveillants.

Courriel suspect

- S'il est accompagné d'une pièce jointe non attendue;
- Si la pièce jointe a un nom suspect, par exemple : *.exe, *.vbs, *.bin, *.com, *.pif, etc.;
- Si le titre ne vous dit rien;
- S'il vous invite à cliquer sur un autre lien suspect;
- Si l'expéditeur est inconnu.

Quelques conseils

- N'ouvrez jamais une pièce jointe sans raison valable ou par simple curiosité et utilisez un antivirus pour analyser les pièces jointes. Bien qu'il s'agisse d'une méthode courante, l'hameçonnage ne se fait pas uniquement que par courriel. Il peut également se faire par des sites Web falsifiés ou tout autre moyen électronique.

- Vérifiez scrupuleusement l'orthographe de l'adresse Web (celle qui se trouve dans la barre d'adresse du navigateur web) avant de cliquer sur un lien. Certains liens peuvent vous amener vers des sites frauduleux dont l'objectif est de récupérer vos renseignements personnels afin d'usurper votre identité ou de vous installer un logiciel espion ou un virus.

.

Pour plus d'informations sur la cybersécurité, nous vous invitons à consulter différents documents sur **les meilleures pratiques en cybersécurité** sur le site du Gouvernement du Canada.

SÉCURISEZ VOS COMPTES
https://www.pensezcybersecurite.gc.ca/fr/securisez-vos-comptes

SÉCURISEZ VOS APPAREILS
https://www.pensezcybersecurite.gc.ca/fr/securisez-vos-appareils

SÉCURISEZ VOS CONNEXIONS
https://www.pensezcybersecurite.gc.ca/fr/securisez-vos-connexions