

Les règles de cyberhygiène¹ au Cégep Garneau



Depuis quelques années, nous constatons une importante hausse du nombre de cyberattaques. Elles peuvent prendre plusieurs formes qu'il est important de rappeler.

Hameçonnage

Prend habituellement la forme d'un message, souvent un courriel provenant en apparence d'une personne de confiance, qui tente d'obtenir des renseignements confidentiels (mot de passe, renseignements personnels, etc.).

Désinformation et ingénierie sociale

Semblable au hameçonnage. La personne malveillante utilisera les réseaux sociaux ou le téléphone pour obtenir des renseignements ou inciter à une action qui exposera des données confidentielles.

Rançongiciels

Ces logiciels malveillants entrent sur le réseau par un appareil infecté, souvent parce qu'un utilisateur a cliqué sur un lien malicieux. Le logiciel rend alors certaines données inutilisables et exige une rançon pour les récupérer.

Vol de données numériques

Pour avoir accès à des données confidentielles, des personnes peuvent s'introduire sur un réseau ou dans un espace infonuagique (*cloud*) comme ils le font pour un rançongiciel ou encore en utilisant un mot de passe usurpé ou qui n'est pas suffisamment complexe.

Faux ordres de virement

En usurpant l'identité d'une personne de confiance comme un gestionnaire, une demande de virement confidentiel, de paiement de facture ou autre transaction du même genre est demandée à un employé pour se procurer de l'argent.

En adoptant de bonnes habitudes de travail, il est possible de limiter les risques d'être victime d'une cyberattaque. On parle alors des règles de cyberhygiène. Selon le Gouvernement du Québec, la cyberhygiène comprend un ensemble de règles à observer et de bonnes pratiques associées à la sécurité d'un système d'information afin de maintenir une « bonne santé numérique ».



Voici quelques règles importantes à respecter.

1. Si vous utilisez un ordinateur fourni par le Cégep, il doit exclusivement servir à exercer vos activités professionnelles. Si vous devez utiliser un ordinateur personnel, vous assurer que les mises à jour du système d'exploitation et de l'antivirus sont bien appliquées ;
2. Utiliser toujours des mots de passe les plus complexes possible (majuscule, minuscule, chiffre et caractère spécial représentent le quatuor « gagnant ») ;
3. Ne pas installer d'application sur un ordinateur du Cégep sans en avoir l'autorisation de la direction des technologies informatiques (DTI). Au besoin, en faire la demande au soutien informatique au 2626;
4. S'assurer que le réseau sans fil du domicile est sécurisé et que le mot de passe pour y accéder est robuste ;
5. Sauvegarder régulièrement le travail effectué sur le réseau du Cégep. S'assurer que les données ne sont pas sauvegardées uniquement sur l'ordinateur.
6. Se méfier des messages et courriels inusités et qui paraissent inhabituels. En cas de doute, vérifier la légitimité du message en contactant la personne ou l'organisme par un autre moyen, par exemple le téléphone ;
7. Ne jamais partager de documents contenant des renseignements confidentiels sur les réseaux sociaux ;
8. S'assurer de restreindre l'accès à l'appareil utilisé, notamment en verrouillant la session lorsque l'on s'absente ;
9. À l'extérieur du Cégep, se connecter au Cégep uniquement depuis l'accès Internet sécurisé de sa résidence privée. Les accès depuis une connexion Wi-Fi publique ne sont jamais recommandés (ex : dans un restaurant, un centre d'achats ou un hôtel);
10. Toujours s'assurer de déconnecter le VPN lorsque la session de travail à distance est terminée.

Définition :

1. **Cyberhygiène** : (gouvernement du Québec)
Ensemble des règles à observer et des pratiques récurrentes qui sont associées à la sécurité d'un système d'information.

Pour plus d'information, consultez le *Code de conduite des utilisateurs des actifs informationnels du Cégep Garneau* et le document *La nétiquette professionnelle lors d'échanges numériques*

www.cegepgarneau.ca/cegep/documents-institutionnels