info Prévention Sensibilisation
Communiqué aux familles, visiteurs, résidents, bénévoles et employés évoluant dans les installations du GROUPE SANTÉ ARBEC

**Suite de l'article sur la Sensibilisation aux courriels d'hameçonnage**

# Cinq conseils à avoir toujours en tête

1. Ne cliquez **jamais** sur des liens ni sur des fichiers joints contenus dans un courriel suspect.
2. Avant de cliquer sur un lien, assurez-vous qu'il pointe vers une URL légitime en passant votre souris sur le lien.
3. Ne fournissez **jamais** d'informations personnelles en réponse à un message non sollicité.
4. Lorsque vous recevez un courriel suspect, **supprimez-le immédiatement.** Si jamais il s'agissait d'un courriel légitime, l'expéditeur pourra toujours vous le retourner à nouveau !
5. Ne **jamais** fournir de renseignements personnels dans un formulaire dont l'accès vous est fourni par un hyperlien contenu dans un courriel ou un message texte.

**Donner votre code d'utilisateur et votre mot de passe à une personne malveillante peut avoir des conséquences graves sur la sécurité de vos données personnelles et celles de l'organisation.**

Voici quelques indices permettant de reconnaître une tentative d'hameçonnage par courriel :

- Le courriel provient d'un expéditeur inconnu.
- Bien que l'expéditeur vous soit connu, la signature de l'expéditeur présente des irrégularités (téléphone, adresse, etc.).
- Le courriel est écrit dans une autre langue que celle habituellement utilisée par l'organisation ou il reste quelques traces d'une langue étrangère à travers le message.
- Le courriel est écrit dans des termes vagues et généraux qui peuvent s'appliquer à toutes les organisations du même genre.
- Le courriel donne un sentiment d'urgence ou fait croire qu'il y a un problème à régler.
- Le courriel est court et ne donne pas de détails spécifiques.

## VOUS PENSEZ ÊTRE VICTIME D'UNE TENTATIVE D'HAMEÇONNAGE?

Si vous avez fourni vos renseignements personnels après avoir cliqué sur un lien contenu dans un courriel ou un site Web suspect, ou encore si des courriels frauduleux portent votre adresse comme expéditeur du courriel, veuillez dans les plus brefs délais :

- Modifier votre mot de passe ainsi que les questions secrètes de sécurité qui sont utilisés pour votre boîte de courriel,
- Prévenir vos contacts que des courriels frauduleux contenant votre adresse pourraient leur être envoyés, et
- Si vous avez des questions ou que le phénomène prend trop d'ampleur, veuillez informer l'équipe d'assistance technique de XTI Conseils sans tarder.

**support@xticonseils.com** 514-360-1751 #201

***La vigilance et le bon jugement demeurent vos meilleures défenses contre l'hameçonnage.***

Merci de votre habituelle collaboration.