MESSAGE AUX EMPLOYÉS

Appel à la vigilance
Tentatives d'hameçonnage et cybersécurité

Soyons prêts à faire face à une recrudescence des campagnes d'hameçonnage

En temps de pandémie, comme nous le vivons actuellement, les cyberpirates tentent de tirer parti de l'attention accordée au virus et de la peur qu'il crée pour mener des campagnes d'hameçonnage se présentant comme des alertes relatives à la COVID-19.

Ces courriels contiennent généralement des pièces jointes qui prétendent offrir des informations sur l'épidémie, des mises à jour sur la façon dont vous pouvez rester en sécurité, ou encore des offres alléchantes sur des produits très recherchés (comme des masques ou du désinfectant). Dans un environnement où les gens ont peur et recherchent toujours plus d'informations, les risques de se faire prendre par ce genre de courriel et de laisser de côté les meilleures pratiques de sécurité sont plus élevés.

C’est pourquoi nous tenons à vous rappeler les règles de base en matière de cybersécurité et de protection contre les risques d’hameçonnage.

- Restez vigilant et ne vous fiez pas au nom de l'expéditeur (portez une attention particulière aux fautes d’orthographe et à la signature du courriel).
- Regardez, mais ne cliquez sur rien.
- N’ouvrez aucune pièce jointe ou aucun lien dont vous ne connaissez pas l’origine.
- Méfiez-vous si une offre est trop belle pour être vraie ou si on vous demande des informations personnelles.
- Portez une attention à l'urgence.
- Ne croyez pas tout ce que vous voyez.

Plus particulièrement, suspectez les courriels dans lesquels, par exemple :

- notre DG ou un membre de l'équipe de direction vous demande un virement bancaire, et ce peu importe le montant;
- un membre de votre famille vous indique qu’il est en difficulté et qu’il a besoin d’argent;
- on vous offre des équipements de protection comme des gants, des masques et du désinfectant à coûts avantageux;
- on vous invite à cliquer pour obtenir une information inédite concernant la pandémie.

Pour de plus amples informations à ce sujet, consultez notre texte de blogue. Soyons proactifs pour le maintien de la cybersécurité! En cas de doute, communiquez avec notre service des technologies.