## Parlons prévention

Des conseils pour vous et votre entreprise

# Vous faites du télétravail? Voici cinq conseils pour éviter d'être victime d'hameçonnage

Comme le nombre d'employés travaillant à domicile est en hausse en raison de la pandémie de COVID-19, les entreprises sont de plus en plus visées par des campagnes d'hameçonnage.

Suivez les cinq conseils ci-dessous pour protéger vos adresses courriel et votre entreprise des cybermenaces :

- **N'envoyez pas de renseignements confidentiels par courriel**
  Les courriels sont pratiques et universels, mais ils ne sont pas un moyen particulièrement sûr de transmettre de l'information. Évitez d'envoyer des renseignements confidentiels, comme des formulaires fiscaux, des numéros de carte de crédit, des renseignements bancaires ou des mots de passe par courriel.

- **Appelez pour confirmer les demandes**
  Si vous recevez un courriel d'un collègue ou de votre employeur vous demandant de lui envoyer de l'argent ou des renseignements, prenez le temps d'appeler cette personne pour vérifier la légitimité de la demande. Il pourrait s'agir d'une escroquerie au faux ordre de virement, un type de fraude qui a coûté plus de 5 milliards de dollars aux entreprises à l'échelle mondiale.*

- **Prenez votre temps**
  Les courriels frauduleux qui ciblent les entreprises contiennent souvent une demande d'action urgente ou immédiate. Les fraudeurs comptent sur le fait que leurs cibles répondront trop vite à ces courriels pour remarquer quoi que ce soit. Prenez donc le temps de relire deux ou trois fois un courriel qui vous presse de cliquer sur un lien ou une pièce jointe.

- **Activez l'authentification à deux facteurs**
  Avec l'authentification à deux facteurs, l'utilisateur doit confirmer son identité au moyen d'un code reçu par message texte ou courriel. Cela ajoute un degré de sécurité supplémentaire pour protéger vos courriels et autres comptes contenant des renseignements confidentiels. Elle n'est pas sans faille, mais elle peut prévenir le piratage de comptes, surtout si l'utilisateur a un mot de passe faible ou qu'il utilise pour plusieurs comptes. En protégeant vos données à l'aide d'un réseau privé virtuel et en demandant aux utilisateurs de s'identifier pour les consulter, vous pouvez éviter que vos données ne soient dévoilées au grand jour.

- **Tenez à jour votre logiciel de sécurité**
  Les logiciels de sécurité et les pare-feu ne peuvent pas bloquer les courriels malicieux, mais ils font régulièrement l'objet de mises à jour pour qu'ils puissent détecter les nouvelles menaces et campagnes d'hameçonnage. Ils sont beaucoup plus efficaces s'ils sont tenus à jour. Assurez-vous de toujours utiliser la version la plus récente de votre logiciel de sécurité et, pendant que vous y êtes, profitez-en pour faire la mise à jour de votre système d'exploitation et de vos applications.

Pour savoir comment rendre votre entreprise encore plus sécuritaire, communiquez avec le Service de prévention au **1.833.692.4112** ou rendez-vous au **www.federated.ca**.



* Source : Centre antifraude du Canada, 2019.