7 conseils pour prévenir la fraude par courriel

Les petites et moyennes entreprises canadiennes sont de plus en plus la cible de fraudeurs sur Internet. Ces derniers cherchent à accéder aux données d'entreprise classifiées (les vôtres et celles de vos clients), obtenir des informations bancaires ou traquer des employés pour commettre un vol d'identité.

Voici les tactiques les plus courantes :

- Pourriel : courriel envoyé sans l'autorisation de l'expéditeur.
- Hameçonnage : courriel prétendument envoyé au nom d'une entreprise, d'une institution financière ou d'une agence gouvernementale.
- Cheval de Troie : offre très attrayante cachant un contrat douteux ou un engagement financier.

Heureusement, il y a des pratiques anti-fraude simples pour diriger une #EntrepriseCybersécuritaire :

1. Méfiez-vous de tout appel téléphonique, visite ou courriel d'étrangers qui demandent de l'information sur vos employés, leur famille ou des questions sensibles liées à votre entreprise.
2. Soyez vigilant quand vous recevez des courriels :
    - Proposant des offres trop belles pour être vraies.
    - Vous demandant de cliquer sur un lien dans le message.
    - Vous demandant des informations personnelles.
3. Signalez toujours à votre superviseur toute activité suspecte.
4. Si vous recevez un courriel suspect d'une organisation reconnue ou d'un client, communiquez avec eux pour vérifier s'ils ont bel et bien envoyé ce courriel.
5. Si vous pensez que votre entreprise est aux prises avec une fuite de données sensibles, prenez des mesures pour sécuriser ces données, communiquez avec votre banque par exemple.
6. Signalez l'incident à la police (ou communiquez avec le Centre antifraude du Canada).
7. Dans le doute, demandez l'aide d'un collègue ou de votre expert informatique.

Si vous ou un autre employé recevez un courriel suspect, n'y répondez pas et ne cliquez sur aucun lien ou pièces jointes accompagnant le courriel. La meilleure chose à faire est de supprimer le courriel de votre boîte de réception. Ne transférez jamais un courriel suspect.

Obtenez plus d'informations sur comment diriger une #EntrepriseCybersécuritaire dans le guide *Pensez cybersécurité pour les petites et moyennes entreprises*, gratuit et disponible en ligne à PensezCybersecurite.ca.