Se protéger contre les fraudes par compte de courriel d'entreprise compromis

La fraude par compte de courriel d'entreprise compromis est l'une des arnaques les plus courantes. Des employés de tous les échelons sont dupés et poussés à envoyer des fonds, à dévoiler des renseignements confidentiels ou à fournir des accès non autorisés à des fraudeurs. Ne tombez pas dans le piège. Servez-vous du présent guide pour assurer votre sécurité.

SECTION 1

Fraudes par compte de courriel d'entreprise compromis

Renseignez-vous sur les fraudes par compte de courriel d'entreprise compromis pour pouvoir les éviter.

Fraude du président

«Virez immédiatement les fonds vers mon compte.»

Dans ce type d'arnaque par courriel, des fraudeurs prétendront être le chef de la direction ou un haut dirigeant de votre entreprise. Ils affirmeront avoir besoin de fonds pour une occasion d'affaires, une urgence ou tout autre enjeu pressant. Ils vous demanderont de transférer immédiatement les fonds nécessaires vers un compte inconnu.

Compte de courriel de fournisseur compromis

«Voici la facture pour nos derniers services.»

Des fraudeurs piratent le compte de courriel de votre fournisseur et vous envoient une facture. Celle-ci semble légitime, mais le numéro de compte est différent. Si vous payez cette facture, vos fonds seront virés aux fraudeurs.

Changement de bénéficiaire

«Veuillez verser le paiement dans notre nouveau compte.»

Vous recevez un courriel qui semble provenir de l'un de vos fournisseurs, mais qui vient en fait de fraudeurs. Ils vous informeront que leurs renseignements bancaires ont changé et que vous devez leur verser vos paiements dans un nouveau compte.

Vol de données

«Veuillez me transmettre vos relevés fiscaux.»

Les cybercriminels ciblent souvent les entreprises afin d'obtenir les relevés fiscaux d'employés ou d'autres renseignements confidentiels. Les fraudeurs se serviront de ces données pour mener des attaques futures comme des tentatives d'hameçonnage, de fraude du président ou de falsification de factures ou de comptes.

Banque Scotia

SECTION 2

Signaux d'alerte

Si vous remarquez l'un de ces signes, soyez sur vos gardes : il se pourrait que vous soyez aux prises avec un fraudeur.

Quelque chose cloche sur la forme

- **Variations mineures** de l'adresse électronique ou du nom de domaine.
- **Différences** dans le modèle de facture, de papier à en-tête, de télécopie ou de modèle de courriel.
- **Fournisseur inconnu.**
- **Renseignements** sur le bénéficiaire et les opérations modifiés.
- **Fautes de grammaire** ou d'orthographe.

Quelque chose cloche sur le fond

- Fort sentiment d'urgence : ***«Il faut agir sur-le-champ.»***
- Entente secrète : ***«Gardons les détails du paiement confidentiel.»***
- Obstacles à la communication : ***«Je ne peux pas vous parler, je ne peux communiquer que par courriel.»***
- Les coordonnées fournies ne correspondent pas à celles dans les dossiers.
- Volonté de contourner le processus d'approbation habituel.

Vous aimeriez en savoir plus?

Évitez les fraudes
Découvrez comment prévenir les fraudes par chèque et par carte de crédit.

Pensez cybersécurité
Découvrez comment améliorer la cybersécurité à la maison et au travail.

Centre antifraude du Canada
Restez au fait des derniers types de fraudes pour éviter d'en être victime.

SECTION 3

Conseils de prévention

Ne vous laissez pas faire : suivez ces conseils simples pour protéger votre entreprise des escroqueries.

1 Avant de donner suite à une demande

- **Prenez le temps de réfléchir** à la demande qui vous est adressée. Vous semble-t-elle étrange de quelque manière que ce soit?
- **Passez un coup de fil à une personne-ressource** connue pour confirmer la demande.
- **Faites part de vos préoccupations** à votre supérieur.
- **Validez les changements** de renseignements bancaires en communiquant par écrit avec une personne-ressource connue.
- Rappelez-vous que **la Banque Scotia ne vous demandera jamais de divulguer vos mots de passe**, la valeur de jetons ou tout autre renseignement confidentiel.

2 Politiques et procédures à mettre en œuvre

- **Faites approuver les paiements** par plus d'une personne.
- **Vérifiez régulièrement** si les registres des opérations sont conformes aux relevés de paiement.
- Tenez à jour un répertoire détaillé des fournisseurs et des bénéficiaires **et consultez-le régulièrement.**
- **Établissez un processus** pour amorcer une demande de rappel de paiement en cas de soupçon de fraude.