# Fraude du courriel d'entreprise compromis

**Ce que vous devez savoir et comment vous protéger**

**Aperçu**

Les criminels cherchent toujours des façons de cibler votre entreprise, et la fraude du courriel d'entreprise compromis est un autre type d'attaque dont vous devez vous méfier. Selon le Centre antifraude du Canada, des pertes de plus de 14,5 millions de dollars ont été enregistrées en 2020 à cause du harponnage et du courriel d'entreprise compromis. Ces pratiques ont fait près de 500 victimes[1]. Découvrez comment réduire au minimum leur impact sur votre chiffre d'affaires et empêcher vos employés d'être victimes de la fraude du courriel d'entreprise compromis.

**La Fraude du courriel d'entreprise compromis** est un type d'hameçonnage qui consiste à se faire passer pour quelqu'un d'autre afin d'obtenir l'accès à des fonds. Les criminels se font couramment passer pour des membres de la direction, des employés et même des représentants d'autres entreprises comme les fournisseurs par exemple. Ce type d'escroquerie n'est pas nouveau, mais notre présence accrue en ligne pour les affaires l'a fait évoluer au fil du temps.

**Comment ça fonctionne?**

Les criminels tentent de se faire passer pour des fournisseurs, des collègues ou votre chef d'entreprise et essaient de vous convaincre de leur envoyer de l'argent ou des renseignements confidentiels. Ils tentent aussi de vous tromper en ayant recours à différentes techniques, comme celle des noms de domaine ou d'adresse courriel semblables qui visent à vous faire croire qu'il s'agit de sources fiables ou reconnaissables. Par exemple, l'adresse courriel comptes.fournisseurs@1nterac.ca pourrait facilement passer inaperçue et avoir l'air d'une adresse légitime appartenant à Interac. Le criminel se faisant passer pour un fournisseur pourrait tenter de convaincre l'employé qu'il a besoin qu'on lui envoie un paiement à cette nouvelle adresse, tout comme le paiement de toutes les prochaines factures.

La fraude du courriel d'entreprise compromis peut prendre plusieurs formes. Voici les plus fréquentes :

- **La fraude du PDG :** Dans ce cas, les criminels se présentent comme le chef ou un membre de la direction d'une entreprise et envoient généralement des courriels à un employé responsable d'effectuer les paiements, lui demandant d'envoyer des fonds de façon urgente et confidentielle à un bénéficiaire précis.

- **Compte de courriel compromis :** Le compte de courriel d'un employé a été infiltré et le criminel envoie des fonds à un compte frauduleux.

- **Fraude par fausse facture :** Souvent dans une même facture, le criminel se fait passer pour un fournisseur existant et demande au destinataire de changer son compte bancaire de fournisseur pour un autre compte qu'il contrôle.

# Fraude du courriel d'entreprise compromis

## Ce que vous devez savoir et comment vous protéger

**Comment vous protégeret protéger votre organisation :**

- **S'ARRÊTER :** Si quelqu'un vous fait une demande « hors norme » comme de lui envoyer des renseignements confidentiels ou de l'argent, prenez un moment pour réfléchir. Demandez-vous pourquoi quelqu'un voudrait changer le processus en vigueur.
- **EXAMINER :** S'agit-il d'une demande inhabituelle de changement aux processus et aux protocoles établis? Avez-vous l'intuition que quelque chose ne va pas? Vérifiez verbalement tout changement qu'on désire apporter aux renseignements sur le paiement.
- **INTERVENIR :** Posez des questions supplémentaires pour confirmer la légitimité de l'expéditeur ainsi que la nature de la demande. Validez les renseignements avec des collègues et signalez la demande aux corps policiers s'il est confirmé qu'elle est frauduleuse.

**Comment protéger votre organisation et vos employés :**

- Établissez une authentification à facteurs multiples et confiez à plus d'un employé la responsabilité d'approuver les transactions sortantes.
- Tenez régulièrement des formations pour sensibilité vos employés. Faites de la sensibilisation à la cybersécurité une priorité en tenant des formations mensuelles portant, entre autres, sur la sécurité et les pratiques exemplaires en matière de mots de passe.
- Communiquez avec votre institution financière et demandez-lui comment elle peut vous aider à protéger votre organisation.

**La protection de votre organisation, de vos employés et de vos clients doit demeurer une de vos principales priorités. Communiquez ces renseignements à votre personnel et à vos fournisseurs afin qu'ils restent vigilants face à la fraude du courriel d'entreprise compromis.**

[1] Centre antifraude du Canada, février 2021.

*Interac* et le logo *Interac* sont des marques déposées d'Interac Corp. Utilisées sous licence.