

Emploi

De nombreuses fraudes ciblent et exploitent les personnes qui sont à la recherche d'un emploi.

Voici quelques variantes de cette fraude qui nous ont été signalées :

- Agent financier
- Client mystère
- Emplois rémunérés en cryptomonnaie, promotion de produits, ou tâches en ligne
- Faux chèque
- Habillage de voiture
- Emplois liés à des sondages en ligne, à des boutiques en ligne ou au commerce électronique
- Indices
- Comment vous protéger

Agent financier

Un fraudeur tente de vous recruter au moyen d'une offre d'emploi :

- envoyée par texto ou courriel non sollicité;
- publiée dans des petites annonces en ligne;
- figurant sur des sites Web de possibilités d'emploi.

Il peut s'agir d'un emploi d'« agent financier » ou de « gestionnaire des relations avec la clientèle ». Si vous répondez à l'offre, le fraudeur vous embauche pour traiter les paiements au nom de la compagnie. Votre travail consiste à recevoir les paiements des clients de la compagnie. Vous recevez des virements électroniques ou bancaires dans votre compte de banque, puis le fraudeur vous demande d'envoyer l'argent en bitcoins à un représentant de la compagnie. L'argent reçu vient de comptes compromis ou d'autres victimes de fraude. Le fraudeur a fait de vous une mule. Vous pourriez vous faire arrêter pour blanchiment d'argent.

Client mystère

Vous recevez un avis vous informant que vous avez été choisi pour être :

- un client mystère;
- un préposé au contrôle de la qualité;
- un conseiller en stratégie de service à la clientèle;
- un adjoint personnel.

L'avis comprend un chèque et des directives. Le fraudeur vous demande de déposer l'argent dans votre compte bancaire personnel et de transférer une grande partie de l'argent dans un compte bancaire précis.

Le fraudeur peut aussi vous demander de faire de petits achats, comme des cartes-cadeaux, et de lui fournir les numéros pour confirmer qu'elles fonctionnent.

À chaque étape, le fraudeur vous demande de remplir et de soumettre un sondage sur le service à la clientèle en fonction de vos expériences. Les sondages sont un moyen de vous convaincre que l'emploi est réel. Vous découvrez par la suite que le chèque que vous avez déposé est faux et que vous devez maintenant de l'argent à la banque.

Emplois rémunérés en cryptomonnaie, promotion de produits, ou tâches en ligne

Les fraudeurs communiqueront avec vous par texto, WhatsApp, courriel ou Messenger après que vous avez fourni votre curriculum vitae et vos coordonnées sur des sites Web de recrutement.

En se servant de noms d'entreprises qui existent au Canada, les fraudeurs vous offrent des emplois à la pige visant à faire la « promotion » de produits, d'applications ou de vidéos à l'aide d'un logiciel qu'ils ont créé. Après avoir installé le logiciel et créé un compte, vous recevrez des « commandes » ou des « tâches » à effectuer.

Vous pourriez recevoir un petit montant d'argent ou une commission pour vous convaincre qu'il s'agit d'un emploi légitime. Les fraudeurs vous informeront ensuite que vous pouvez toucher une commission plus élevée ou « passer à un niveau supérieur » si vous faites la promotion d'un plus grand nombre de produits ou de vidéos, mais que vous devez payer des frais pour obtenir plus de travail.

Les fonds sont déposés dans des comptes ou des portefeuilles de cryptomonnaies. Vous verrez les fonds gagnés dans votre compte de cryptomonnaies, mais vous ne pourrez pas les retirer.

N'acceptez jamais d'encaisser des fonds dans votre compte bancaire personnel pour les transférer ailleurs, car il y a de fortes chances que vous serviez de mule et contribuiez à du blanchiment d'argent.

On peut aussi vous demander de recruter d'autres personnes afin d'augmenter vos revenus. Il s'agit de vente pyramidale, une pratique illégale au Canada. Quiconque fait la promotion d'un système de vente pyramidale commet une infraction criminelle.

Faux chèque

Un fraudeur envoie un courriel ou un texto pour offrir un emploi à des personnes qui affichent leur curriculum vitae en ligne. Les offres peuvent varier :

- Fournisseur de soins
- Adjoint administratif
- Commis à la saisie de données
- Client mystère

Le fraudeur vous envoie un chèque contrefait et vous explique pourquoi il a besoin d'aide pour l'encaisser. Il vous demande de le déposer, puis de lui remettre une partie des fonds.

Habillage de voiture

Un fraudeur vous envoie un message non sollicité vous informant que vous pouvez gagner de 300 \$ à 500 \$ par semaine si vous habillez votre voiture, camion, véhicule utilitaire sport ou vélo avec le logo d'une « compagnie ». Si vous répondez, vous recevez des instructions et un contrat, suivis d'un chèque par la poste.

Le fraudeur vous demande de déposer le chèque dans votre compte et de retirer une partie des fonds. Vous devez ensuite déposer l'argent dans un compte bancaire afin de payer une compagnie de graphisme ou d'autres frais. C'est alors que vous apprenez que le chèque est contrefait et que vous êtes responsable des fonds retirés.

Emplois liés à des sondages en ligne, à des boutiques en ligne ou au commerce électronique

Les fraudeurs proposent de faux emplois en télétravail qui exigent de gérer des boutiques en ligne ou de remplir des sondages en ligne. Ces offres se trouvent souvent dans des publicités sur les réseaux sociaux, des messages textes ou des messages envoyés sur WhatsApp, Telegram, Instagram, Messenger ou TikTok.

Les fraudeurs promettent aux victimes des revenus faciles, des petites commissions et des horaires de travail flexibles. Dans un premier temps, les tâches semblent faciles, et la plateforme affiche de faux profits pour instaurer la confiance. Il est même possible que les victimes reçoivent un petit paiement au début. Éventuellement, on leur demande de faire des dépôts pour continuer.

Emplois dans une boutique en ligne : Les victimes doivent s'inscrire à une fausse boutique en ligne ou à une fausse plateforme de commerce électronique. On leur demande de traiter des commandes, d'approuver les transactions ou de gérer l'inventaire. Elles se font promettre des commissions pour chaque commande exécutée. Alors que les victimes continuent leur travail, le système commence à demander des dépôts de plus en plus gros pour « mettre le compte à niveau », « corriger des erreurs dans les commandes » ou « accéder à de meilleures commissions ».

Emplois liés à des sondages sur le Web : Les victimes sont rémunérées pour remplir des sondages en ligne. Après avoir rempli quelques sondages simples, la plateforme indique qu'elle éprouve des problèmes et demande des dépôts pour poursuivre. Les victimes voient un faux solde qui augmente à l'écran, mais sont incapables de retirer des fonds. Elles subissent des pressions pour remplir plus de sondages et payer pour déverrouiller le prochain niveau.

Les victimes se rendent souvent compte qu'il s'agit d'une fraude uniquement lorsque les montants déposés deviennent trop importants ou que la plateforme bloque les retraits.

Indices

- Une entreprise utilise une adresse de courriel sur le Web plutôt qu'une adresse de domaine officiel.
- Vous recevez une offre d'emploi alors que vous n'avez pas posé votre candidature.
- On vous demande de rejoindre une plateforme, de télécharger des logiciels ou d'effectuer des tâches simples pour gagner de l'argent rapidement.
- Les tâches consistent à effectuer des dépôts à l'avance, « à optimiser les frais » ou « à déverrouiller les paiements ».
- Vous voyez un solde sur le site Web ou l'application, mais ne pouvez pas retirer d'argent.
- On vous demande de recruter d'autres personnes.
- On vous demande de recevoir ou de transférer des fonds au moyen de votre compte bancaire.
- L'offre promet une rémunération élevée pour peu de travail.

Comment vous protéger

- Prenez du temps avant de répondre à des messages d'offres d'emploi dont vous ne connaissez pas la provenance.
- Vérifiez le site Web officiel de l'entreprise et appelez leur numéro de téléphone officiel.
- N'envoyez jamais de dépôts et ne payez jamais de frais pour un emploi.
- Évitez de télécharger des logiciels ou des applications provenant d'une source inconnue.
- Ne divulguez pas de renseignements personnels ou de pièces d'identité à des contacts non vérifiés.
- Soyez vigilant·e au moment d'envoyer de la cryptomonnaie; dans la plupart des cas, la transaction ne peut pas être annulée.

Si vous croyez avoir été la cible de fraude ou de cybercriminalité, signalez-le à votre service de police local. Consultez également le site Web [Signaler la cybercriminalité et la fraude](#) pour les signalements en ligne ou par téléphone au 1-888-495-8501.

Source : Centre antifraude du Canada.