BULLETIN DU CENTRE ANTIFRAUDE DU CANADA

Fraudes à l'emploi – Nouvelle variante 2025-12-16

LA FRAUDE : IDENTIFIEZ-LA, SIGNALEZ-LA, ENRAYEZ-LA

Le Centre antifraude du Canada (CAFC) continue de recevoir des signalements sur les fraudes à l'emploi. Les victimes reçoivent des offres d'emploi frauduleuses par messagerie texte, WhatsApp, par courriel, par Messenger ou elles les voient dans des publicités sur les réseaux sociaux. Ces offres d'emploi pourraient porter le nom de vraies entreprises, mais elles sont en fait frauduleuses. Les victimes se font convaincre par la ruse de faire des dépôts ou d'envoyer de la cryptomonnaie et sont ensuite incapables de récupérer leur argent.

Les pertes totales signalées attribuables à ces fraudes ont monté en flèche ces dernières années. En 2022, les Canadiens ont signalé des pertes de plus de 7,3 millions de dollars. Cette somme est passée à 49 millions de dollars en 2024. Malheureusement, la tendance se poursuit en 2025. Au cours des neuf premiers mois de 2025 inclusivement, les victimes ont déjà signalé des pertes de 46,5 millions de dollars. On peut donc affirmer que la fraude à l'emploi connaît une hausse fulgurante, et que les fraudes ciblent plus de Canadiens que jamais auparavant.

*****Nouvelle variante*** 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 des 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.

Variante « promotion de produits » ou « tâches en ligne »
En utilisant les noms de vraies entreprises canadiennes, les fraudeurs offrent aux victimes des emplois à la pige visant à faire la « promotion » de produits, d'applications ou de vidéos au moyen d'un logiciel qu'ils ont créé. Après avoir installé le logiciel et créé un compte, les victimes reçoivent des « commandes » ou des « tâches » à effectuer. Elles peuvent recevoir un petit montant d'argent ou une commission pour ce travail, ce qui les convainc qu'il s'agit d'un emploi légitime. Il est aussi possible pour elles de toucher une commission plus élevée ou de « passer à un niveau supérieur » si elles font la promotion d'un plus grand nombre de produits ou de vidéos, mais elles doivent payer des frais pour obtenir plus de travail.

Les victimes déposent leurs fonds dans des comptes ou des portefeuilles de cryptomonnaies. Il est également possible qu'on leur demande de recruter d'autres personnes afin d'augmenter leurs revenus. Comme dans le cas d'arnaques d'investissements dans les cryptomonnaies, les victimes voient les fonds qu'elles ont gagnés dans leur compte de cryptomonnaies, mais elles ne peuvent pas les retirer.

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.