BULLETIN DU CENTRE ANTIFRAUDE DU CANADA

Sophistication de la fraude 2026-03-16

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

La fraude continue de s'amplifier et de se complexifier, faisant chaque jour des victimes parmi les Canadiens. Les escrocs changent constamment de tactiques et utilisent les nouvelles technologies pour mieux leurrer et convaincre. Le Mois de la prévention de la fraude est l'occasion de sensibiliser, d'offrir des conseils pratiques et d'encourager les Canadiens à mettre la pédale douce, à vérifier l'information et à signaler les incidents de fraude afin de se protéger et de protéger les autres.

Les escrocs utilisent des technologies de pointe, dont l'intelligence artificielle (IA), l'automatisation et des outils d'aspect professionnel pour être plus difficiles à démasquer. Grâce à ces tactiques, ils parviennent à se faire passer pour des personnes, des entreprises et des plateformes de confiance, augmentant ainsi leurs chances de duper leurs victimes.

Voici quelques-uns des subterfuges utilisés :

- **Hypertrucages** – Vidéos générées par l'IA qui semblent provenir de personnes de confiance ou de personnalités publiques.
- **Faux sites Web et applications d'investissement en cryptomonnaies** conçus pour ressembler à des plateformes de négociation légitimes.
- **Fraudes à l'emploi** qui comprennent des offres d'emploi et des entrevues qui semblent réelles et des documents d'apparence officielle.
- **Messagerie automatisée et outils de communication chiffrés** utilisés pour communiquer rapidement avec un grand nombre de personnes.

Fraude à l'emploi et applications malveillantes

La fraude à l'emploi continue de se sophistiquer au point de ressembler à s'y méprendre à un véritable parcours de recrutement. Les escrocs se font passer pour des employeurs et accompagnent les victimes tout au long d'un processus d'embauche qui comprend des entrevues, des contrats et du matériel de formation.

Souvent, les victimes sont invitées à télécharger des applications malveillantes pour le « travail ». Les escrocs leur font croire que ces applications sont nécessaires pour communiquer ou effectuer des tâches ou des paiements. Or, une fois installées, elles peuvent servir à voler des renseignements personnels ou à transférer de l'argent à l'insu de la victime.

Pour mieux convaincre, les escrocs s'appuient sur une infrastructure d'apparence professionnelle, comme de faux sites Web, de fausses plateformes d'investissement dans les cryptomonnaies ou des systèmes de paiement frauduleux. Cela confère une apparence de légitimité et permet aux criminels de transférer des fonds rapidement et de façon anonyme.

Fraude à l'investissement dans les cryptomonnaies

La fraude à l'investissement dans les cryptomonnaies passe par des plateformes de négociation en ligne qui semblent légitimes. Les escrocs utilisent des sites Web ou des applications d'apparence professionnelle qui prétendent offrir des occasions d'investissement, des rendements en temps réel ou des conseils d'expert.

Pour appâter leurs victimes, les fraudeurs recourent à des vidéos hypertruquées, des publications sur les médias sociaux et des publicités en ligne commanditées qui mettent en vedette des personnes de confiance ou des personnalités connues. Ces tactiques visent à inspirer confiance et à créer un sentiment d'urgence chez les victimes.

Comme pour la fraude à l'emploi, les victimes sont amenées à télécharger des applications malveillantes ou à utiliser de fausses plateformes d'investissement qui affichent de faux rendements. Après avoir fait un « premier investissement », les victimes sont poussées à injecter davantage d'argent ou à payer des frais supplémentaires, pour finalement se rendre compte qu'elles ne peuvent pas retirer leur argent.

Signaux d'alerte – Comment vous protéger

- Méfiez-vous des offres d'emploi non sollicitées, surtout celles reçues sur des messageries de réseaux sociaux ou par textos non sollicités.
- Vérifiez l'existence de l'employeur en consultant son site Web officiel et ses coordonnées.
- Ne téléchargez jamais d'applications ou de logiciels dans le cadre d'une offre d'emploi à moins de pouvoir vous assurer de leur légitimité.
- Soyez vigilant! Si on vous demande de transférer de l'argent, d'accepter des paiements sur votre compte bancaire personnel ou d'utiliser des cryptomonnaies dans le cadre de votre travail, c'est probablement un stratagème frauduleux.
- Méfiez-vous des « occasions d'investissement » qui font miroiter des rendements garantis ou extraordinairement élevés.
- Vérifiez si la société est inscrite auprès de l'autorité en valeurs mobilières de votre province ou à l'aide de la base de données nationale d'inscription.
- Ne cédez pas aux pressions pour agir rapidement ou garder le « secret ».
- Méfiez-vous des promotions qui utilisent des photos de célébrités, des vidéos hypertruquées ou des publicités commanditées.
- Ne téléchargez jamais d'applications d'investissement inconnues et n'envoyez jamais d'argent à des plateformes dont vous ne pouvez pas vérifier l'existence par vos propres moyens.
- Quel que soit le type d'investissement, rappelez-vous que vous devriez pouvoir retirer vos fonds sans avoir à payer des frais supplémentaires.

Quiconque croit avoir été la cible d'une fraude ou de cybercriminalité devrait le signaler à son service de police local. On peut également effectuer un signalement en ligne ou par téléphone sur le site Web Signaler la cybercriminalité et la fraude ou en composant le 1-888-495-8501.