BULLETIN DU CENTRE ANTIFRAUDE DU CANADA

Fraude liée aux médias sociaux 2024-10-15

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

Plus que jamais, les gens communiquent et interagissent socialement en ligne, et le CAFC tient à vous éviter d'être victimes de fraude dans les médias sociaux dans le cadre du Mois de la sensibilisation à la cybersécurité. Avoir un compte compromis ou se laisser prendre par une fraude liée aux investissements peut se révéler coûteux si vous ne faites pas preuve de vigilance.

Fraudes courantes liées aux médias sociaux

Compromission de comptes

Avez-vous reçu une offre d'un ami pour des billets de concert de Taylor Swift à bon prix ou des demandes d'aide d'un membre de votre famille qui a perdu son téléphone, ou avez-vous répondu à des offres d'immigration appuyées par des députés canadiens?

Prenez garde, les fraudeurs compromettent de plus en plus de profils sur les plateformes comme Facebook. Ces comptes sont alors utilisés pour faciliter des fraudes liées aux marchandises, au besoin urgent d'argent, et même à l'immigration.

Fraudes liées aux investissements

Il est important de connaître deux fraudes liées aux investissements qui se produisent couramment en ligne :

- Dans le cas des fraudes liées aux investissements qui semblent appuyées par des célébrités, les fraudeurs créent et affichent des articles de fausses nouvelles contenant des vidéos hypertruquées mettant en vedette des personnalités en vue bien connues pour encourager leurs victimes à investir dans la cryptomonnaie.

- Dans le cas des fraudes sentimentales liées aux investissements, les fraudeurs vous contactent par l'entremise de sites de rencontre en ligne, de plateformes de médias sociaux ou même par texto pour tenter de nouer une relation avec vous et de gagner votre confiance. Ils prétendent habituellement être des investisseurs en cryptomonnaie qui connaissent le succès, et vous persuadent d'investir en vous promettant un haut rendement.

Extorsion sexuelle (sextorsion)

Les fraudeurs créent de faux profils sur des sites de réseautage social, de pornographie et de rencontre. Ils utilisent ces profils pour vous séduire et vous contraindre à vous livrer à des actes sexuels devant une caméra. L'extorsion sexuelle, ou l'exploitation sexuelle en ligne, c'est du chantage. Elle se produit quand des criminels menacent d'envoyer une image ou une vidéo à caractère sexuel existante (ou fabriquée) à vous ou à d'autres personnes à moins que vous les payiez ou que vous leur fournissiez plus de matériel à caractère sexuel. Elle peut aussi se produire quand une personne est encouragée à observer des situations à caractère sexuel en ligne, ou à y participer. Ces rencontres peuvent être enregistrées à l'insu des

victimes. Les fraudeurs menacent alors d'envoyer ces enregistrements à des amis, à des membres de la famille, ou à des collègues de travail si la personne n'envoie pas d'argent ou d'autres images.

Signes avertisseurs pour tous les types de fraude

• Quelqu'un que vous n'avez jamais rencontré en personne vous déclare son amour.
• Vous recevez des textos non sollicités de la part d'inconnus.
• Une personne tente de changer de moyen de communication ou de passer à un moyen de communication privé (WhatsApp, Signal, Discord, etc.).
• Les rencontres en personne que vous tentez d'organiser sont toujours annulées ou la personne a toujours une excuse pour ne pas vous rencontrer.
• La personne joue la carte de la détresse ou de la colère pour vous forcer à lui envoyer de l'argent.
• Demandes d'amis de personnes que vous ne connaissez pas ou profils qui semblent trop parfaits.
• Demandes d'accès à distance à votre ordinateur ou appareil électronique pour vous montrer comment investir.
• Possibilités d'investissement offrant un rendement supérieur à la normale.
• Demandes de virement de placements en cryptomonnaie vers un autre portefeuille de cryptomonnaie.
• Annonces pour des investissements provenant de personnes très en vue qui promettent un haut rendement.

Comment vous protéger de tous ces types de fraudes?

• N'acceptez pas de demandes d'amis de personnes que vous ne connaissez pas.
• Faites attention à qui vous transmettez des photos. Les suspects utilisent souvent des photos explicites pour extorquer plus d'argent à leurs victimes.
• Apprenez comment vous protéger de la sextorsion.
• N'envoyez jamais d'argent à une personne que vous n'avez jamais rencontrée.
• Ne divulguez pas vos renseignements personnels (nom, adresse, date de naissance, numéro d'assurance sociale, justificatifs bancaires).
• Ne scannez jamais un code QR provenant d'une source inconnue. Il pourrait contenir un virus et infecter votre appareil.
• Ne donnez jamais accès à distance à votre ordinateur ou appareil électronique (à l'aide d'AnyDesk, de TeamViewer, etc.).
• Faites preuve de vigilance au moment d'envoyer de la cryptomonnaie : les virements sont pratiquement toujours irréversibles.
• Vérifiez si les entreprises de placement sont enregistrées à l'aide du moteur de recherche national (http://www.sontilsinscrits.ca/).
• Méfiez-vous des personnes qui vous incitent à ouvrir des comptes de cryptomonnaie et à y verser de l'argent. Elles vous orienteront vers des portefeuilles qu'elles contrôlent. Ne le faites pas!
• Méfiez-vous des offres qui vous promettent un haut rendement. Si c'est trop beau pour être vrai, méfiez-vous.
• Obtenez d'autres trucs et conseils pour vous protéger.

Si vous croyez être victime de fraude ou si vous connaissez une personne qui en a été la cible, signalez-le au Centre antifraude du Canada, au 1-888-495-8501 ou en ligne au http://www.centreantifraude.ca/.