BULLETIN DU CENTRE ANTIFRAUDE DU CANADA

Stratagème amoureux et stratagème de rencontre 2025-02-14

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

Chaque année autour de la Saint-Valentin, des fraudeurs tentent de trouver des victimes peu méfiantes à la recherche d'amour ou de compagnie.

Stratagème amoureux

Les arnaqueurs entrent généralement en contact avec les victimes sur des sites de rencontre ou de médias sociaux; il n'est pas rare qu'ils utilisent de vraies photos trouvées dans les médias sociaux (p. ex. des photos de gens d'affaires, de militaires, de familles, d'animaux de compagnies et de passe-temps). Les fraudeurs ne tardent pas à déclarer leur amour pour gagner la confiance et l'affection de leur victime pour ensuite lui voler de l'argent. Une fois le lien établi, ils demandent aux victimes de passer à un autre moyen de communication comme Whatsapp, Signal et d'autres. Ce type de fraude mise beaucoup sur les émotions des victimes et peut durer des mois, des années ou jusqu'à ce que la victime n'ait plus rien à donner. Les fraudeurs ne rembourseront jamais la victime et continueront de faire de vaines promesses et de demander plus d'argent.

Voici les raisons les plus fréquentes pour lesquelles les fraudeurs demandent de l'argent :

- une urgence personnelle ou familiale;
- le prétexte qu'ils n'ont pas accès aux fonds qu'ils ont déjà;
- des dépenses liées au travail, des frais juridiques ou des honoraires professionnels imprévus;
- un besoin d'aide pour investir dans une nouvelle entreprise;
- des frais de voyage pour retourner à la maison.

Parmi les plus récentes variantes, on compte notamment les attaques conversationnelles, qui consistent en l'envoi de messages textes aléatoires aux victimes par les fraudeurs. Les messages contiennent souvent des phrases comme « où es-tu? », « qu'est-ce que tu deviens? », etc. Si la victime répond, le fraudeur poursuit la conversation et tente d'établir une relation avec elle.

Stratagème de rencontre lié aux investissements

Dans ces situations, les fraudeurs développent une relation avec la victime et la convainquent d'investir dans une fausse plateforme de cryptomonnaie en lui promettant des rendements élevés. En fait, les fraudeurs laissent parfois même la victime encaisser une partie des rendements d'investissements dans le seul but de l'inciter à investir une plus grande somme. Les suspects « apprendront » aux victimes comment investir dans leurs plateformes frauduleuses de cryptomonnaie. Malheureusement, lorsque la victime demandera de retirer son investissement, ce ne sera pas possible.

Nouvelle variante

La toute dernière variante qui fait l'objet de signalements se fait souvent qualifier d'« hameçonnage par approbation » (*approval phishing*). Même si cette tactique de fraude existe depuis un certain temps maintenant, elle est utilisée depuis peu par les fraudeurs spécialisés en stratagèmes amoureux et de rencontre. Les suspects développent une relation avec les victimes et les convainquent d'investir dans la

cryptomonnaie, puis les amènent à leur donner accès à leurs comptes de cryptomonnaie en se faisant passer pour des employés de services de confiance. Après avoir appris aux victimes comment acheter de la cryptomonnaie comme Ethereum ou Tron, les fraudeurs leur envoient une fausse demande qui semble provenir du service de cryptomonnaie afin qu'elles autorisent l'accès à leur portefeuille. En cliquant sur « approuver », la personne autorise le tiers à gérer ses fonds. En apparence, les fausses demandes ressemblent fortement à celles envoyées par les applications et les services légitimes et elles paraissent donc authentiques aux yeux de l'utilisateur. Dans certains cas, il est possible que les victimes reçoivent une demande de virement à approuver en cliquant sur un lien, autorisation qui permettra au fraudeur d'accéder à leur portefeuille à leur insu.

Signes avant-coureurs

Méfiez-vous :

- des profils qui semblent trop parfaits;
- si quelqu'un que vous n'avez jamais rencontré en personne vous déclare son amour;
- si une personne tente de changer de moyen de communication ou de passer à un moyen de communication privé (courriel, texte, plateforme de médias sociaux, etc.);
- si les rencontres en personne que vous tentez d'organiser sont toujours annulées ou si la personne a toujours une excuse pour ne pas vous rencontrer;
- si la personne vous demande de ne pas parler d'elle avec vos parents et amis;
- si la personne joue la carte de la détresse ou de la colère pour vous forcer à lui envoyer de l'argent;
- si vous recevez des messages mal écrits ou adressés au mauvais nom;
- si une personne vous « présente » à sa famille sur les médias sociaux pour rendre votre relation légitime;
- si quelqu'un propose de vous apprendre comment investir dans la cryptomonnaie;
- si les courriels semblent provenir de votre fournisseur de services de cryptomonnaie et vous invitent à cliquer sur des liens;
- si vous recevez des possibilités d'enrichissement rapide;
- des personnes rencontrées sur un site de rencontre ou dans les médias sociaux qui tentent de vous convaincre d'investir dans la cryptomonnaie.

Comment vous protéger

- Ne divulguez pas vos renseignements personnels (nom, adresse, date de naissance, numéro d'assurance sociale, justificatifs bancaires).
- N'acceptez pas de demandes d'amis de personnes que vous ne connaissez pas.
- N'investissez pas votre argent dans des plateformes qui vous sont proposées par des personnes que vous ne connaissez pas.
- N'envoyez jamais d'argent à une personne que vous n'avez jamais rencontrée.
- Activez l'authentification multifactorielle (AMF) sur vos comptes.

- Méfiez-vous des personnes qui vous incitent à ouvrir des cryptocomptes et à y verser de l'argent, car elles pourraient vous orienter vers des portefeuilles qu'elles contrôlent – **Ne tombez pas dans le piège!**
- Si vous avez permis à un suspect d'accéder à votre compte de cryptomonnaie, suivez la liste de vérification de la Police provinciale de l'Ontario (OPP) pour révoquer les autorisations de jetons.
- Apprenez d'autres conseils et trucs pour vous protéger.

Si vous croyez avoir été la cible de fraude ou de cybercriminalité, signalez-le à votre service de police local et au CAFC en ligne ou en composant le 1-888-495-8501.