La lettre d'information mensuelle de sensibilisation à la sécurité

Les belles paroles et les porte-monnaies vides : les arnaques à l'investissement fondées sur la romance

Une histoire dont il faut se rappeler : l'expérience de Lisa

Lisa, une professionnelle de la gestion sympathique et prospère, avait une vie bien remplie et un travail très prenant. Mais comme son travail devenait envahissant, elle se sentait de plus en plus isolée et s'est donc tournée vers les réseaux sociaux pour rencontrer de nouvelles personnes. C'est à ce moment-là qu'elle a rencontré "Ryan", un homme qui est rapidement devenu un ami et un compagnon de confiance, bien que virtuel comme il vivait de l'autre côté de la planète. Il semblait attentionné, ils partageaient la même passion pour le voyage, la cuisine, et même l'investissement.

Pendant plusieurs mois, alors que leur relation évoluait, Ryan lui a suggéré d'investir dans une plateforme de crypto-monnaie dans laquelle il avait investi et qui connaissait une croissance rapide. La plateforme semblait légitime pour Lisa et elle a commencé à investir une petite somme. En voyant son investissement fructifier, et avec les encouragements de Ryan, elle a investi encore plus d'argent les mois suivants. Après six mois de relation, Lisa a essayé de retirer son argent, mais la plateforme avait "gelé" son compte et Ryan avait disparu. Lisa a découvert avoir perdu plus de 175,000$ à cause d'une arnaque à l'investissement et la romance connue sous le nom de "l'arnaque à l'abattage du cochon". La perte financière était dévastatrice mais la trahison émotionnelle l'était encore plus.

Qu'est-ce que l'arnaque à l'abattage du cochon ?

"L'arnaque à l'abattage du cochon" est une arnaque élaborée qui combine la romance et les escroqueries à l'investissement. Elle suit quelques étapes prévisibles, bien que les détails puissent varier :

1. **Contact initial** : L'escroc prend contact avec la victime, souvent via des applications de messagerie ou les réseaux sociaux, en engageant une conversation légère, faisant des compliments et s'intéressant à la vie de la victime.
2. **Construire une relation** : Avec le temps, l'escroc construit la confiance. Il partage des histoires personnelles, entame des discussions agréables, et construit souvent une relation romantique pour renforcer le lien.
3. **Présenter des opportunités d'investissement** : Une fois que la confiance est établie, l'escroc parle d'un investissement "sûr et lucratif", souvent dans la crypto. Il prétend avoir une connaissance d'initié ou de la réussite avec cet investissement et montre des résultats falsifiés avec rendements financiers incroyables.
4. **Encourager les petits investissements** : L'escroc encourage la victime à faire de petits investissements. Dans un premier temps, la victime voit ce qui est en réalité de faux "bénéfices" ou de fausses recettes, que l'escroc utilise pour asseoir sa crédibilité. L'escroc peut même autoriser de petits retraits au début de la relation afin d'ajouter une façade légitime.
5. **Augmenter les enjeux** : Lorsque la victime voit ses "gains", l'escroc la presse à investir encore plus, avec un sentiment d'urgence comme celui-ci : "Agis maintenant, ou tu risques de passer à côté !"
6. **La coupure** : Quand l'escroc estime avoir pris tout ce qu'elle pouvait à sa victime, il "gèle" le compte ou disparaît. La plateforme devient inaccessible, laissant la victime sans rien.

Quels sont les signaux d'alertes pour détecter les "arnaques à l'abattage du cochon" ?

1. **Trop beau pour être vrai** : Méfiez-vous des personnes qui promettent des rendements garantis ou qui affirment ne courir aucun risque. Les investissements légitimes comportent toujours un certain risque, et des gains rapides et réguliers sont souvent un indicateur de danger.
2. **Un contact inattendu** : Méfiez-vous des personnes inconnues qui prennent contact avec vous sans raison claire. Avez-vous déjà reçu un "Salut" d'une personne que vous ne connaissiez pas sans savoir pourquoi elle vous contactait ? C'est le début d'une arnaque. Ne répondez sous aucun prétexte et envisagez de bloquer l'expéditeur.
3. **La relation tourne rapidement autour de l'argent** : Si quelqu'un que vous avez récemment rencontré en ligne commence à vous parler d'investissement, c'est un signal d'alerte. Les escrocs mêlent les relations avec la finance pour manipuler la confiance.
4. **Une pression pour investir rapidement** : Les escrocs créent souvent un sentiment d'urgence pour que les victimes investissent beaucoup d'argent très vite. Ils affirment que la "fenêtre" pour cette opportunité va se fermer, ou que c'est une offre "à durée limitée.
5. **Les fausses plateformes d'investissement** : Beaucoup d'escrocs utilisent de faux sites ou des applications d'investissement d'apparence légitime qui affichent des chiffres fabriqués. Méfiez-vous de toutes les plateformes qui ne sont pas largement reconnues ou recommandées par des conseillers financiers de confiance.
6. **Une difficulté à retirer les fonds** : Le dernier signal d'alerte est que lorsque vous essayez de retirer l'argent, vous êtes confrontés à des retards, des excuses ou des frais supplémentaires. Tout investissement légitime doit vous permettre d'accéder à vos fonds sans entrave.

Comment se protéger

Les escrocs qui se cachent derrière ces systèmes sont d'habiles manipulateurs. Vous êtes votre meilleure défense.

- **Se méfier** : Lorsque des inconnus établissent une connexion avec vous, soyez très méfiants. En outre, plus l'opération financière est importante et plus la pression pour investir est forte, plus il y a de chances qu'il s'agisse d'une escroquerie.
- **Faire des recherches approfondies sur les plates-formes** : Tenez-vous en à des plateformes d'investissement bien connues et évitez toute plateforme dont l'actionnariat n'est pas clair ou qui ne dispose pas d'informations réglementaires.
- **Protéger ses informations personnelles** : N'en dites pas trop sur vos finances ou votre vie personnelle en ligne, surtout avec des personnes que vous n'avez jamais rencontrées en personne.

Rédacteur invité

Karen Nemani est responsable de la sécurité commerciale des services professionnels canadiens d'AWS et présidente de l'affilié ontarien de WiCyS. Elle se passionne pour l'évolution de la culture de la cybersécurité afin de créer une main-d'œuvre inclusive où la diversité des mentalités, des compétences et des points de vue s'épanouit. https://www.linkedin.com/in/karenbnemani/

Ressources

Déclencheurs émotionnels : comment les escrocs vous piégent : https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Ne laissez pas les cybercriminels s'emparer de vos économies : verrouillez vos comptes financiers : https://www.sans.org/newsletters/ouch/dont-let-cybercriminals-swipe-your-savings-lock-down-your-financial-accounts/
Protégez votre cœur (et votre portefeuille) contre les arnaques à la romance : https://www.sans.org/newsletters/ouch/guard-your-heart-wallet-against-romance-scams/

Traduit pour la Communauté par : Juliette Busson