Votre bulletin mensuel sur la sensibilisation à la sécurité

Les trois principales arnaques sur les réseaux sociaux

Aperçu

Si les réseaux sociaux sont un moyen fantastique de communiquer, de partager et de s'amuser avec d'autres personnes, ils constituent également un moyen peu coûteux pour les cybercriminels de piéger et de profiter de millions de personnes. Ne vous faites pas avoir par les trois escroqueries les plus courantes sur les réseaux sociaux.

Escroqueries en matière d'investissement

Avez-vous déjà vu un article sur une opportunité d'investissement qui promet un rendement énorme dans un laps de temps extrêmement court, avec un risque prétendument faible ou nul ? En réalité, ces garanties sont en fait des escroqueries à l'investissement. Les fraudeurs volent simplement votre argent après que vous les avez payés. Ces escroqueries incluent souvent des publicités ou des histoires de réussite d'anciens clients pour promouvoir les investissements, mais il ne s'agit que de faux témoignages destinés à accroître votre confiance. Souvent, ces escroqueries à l'investissement portent sur l'investissement dans des crypto-monnaies ou des biens immobiliers, et le paiement est souvent effectué en crypto-monnaies ou par d'autres méthodes de paiement non standard. Si un investissement semble trop beau pour être vrai, il l'est très probablement. N'oubliez pas qu'il n'existe pas d'investissement à rendement élevé garanti. N'investissez votre argent que dans des ressources fiables et connues, et non à des inconnus que vous rencontrez en ligne et qui vous proposent un système d'enrichissement rapide.

Escroqueries à l'amour

Lorsque des criminels établissent une relation en ligne avec une personne qu'ils ont identifiée comme solitaire ou vulnérable pour lui soutirer de l'argent, on parle d'escroquerie à l'amour. Le criminel utilisera toutes les tactiques possibles pour établir une confiance, y compris l'échange de fausses photos ou l'envoi de cadeaux, puis racontera une histoire tragique dans laquelle il a besoin d'argent pour payer des dépenses telles que des factures d'hôpital ou des frais de déplacement pour rendre visite à la victime en personne. Pour éviter de vous rencontrer en personne, ces criminels peuvent dire qu'ils travaillent dans un secteur qui les en empêche, comme la construction, la médecine internationale ou l'armée. Ils demandent souvent de l'argent sous forme de virement bancaire ou de cartes-cadeaux pour obtenir de l'argent rapidement et rester anonyme. Ces types d'escroquerie ne sont pas seulement courants sur les réseaux sociaux, mais aussi sur les applications de rencontre en ligne. Soyez prudent avec les personnes que vous rencontrez en ligne, allez-y doucement et n'envoyez jamais d'argent à une personne avec laquelle vous n'avez communiqué qu'en ligne.

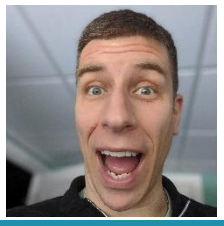
En outre, si vous pensez qu'une personne de votre entourage peut être vulnérable à une telle arnaque ou qu'elle est engagée dans une relation en ligne qui coche ces cases, proposez-lui votre aide. Parfois, il peut être très difficile pour une personne absorbée par un lien émotionnel de voir à quel point la situation est devenue dangereuse.

Escroqueries en matière d'achats en ligne

Les arnaques au shopping en ligne se produisent lorsque vous achetez des articles en ligne à des prix extrêmement bas mais que vous ne les recevez jamais. Des publicités alléchantes sur les réseaux sociaux vantent des prix incroyables et proposent des liens vers des sites qui semblent légitimes et vendent des marques connues, mais ces sites sont souvent faux. Méfiez-vous des sites web qui n'ont pas d'informations de contact, dont les formulaires de contact ne fonctionnent pas ou qui utilisent des adresses électroniques personnelles. Tapez le nom de la boutique en ligne ou son adresse web dans un moteur de recherche pour voir ce que d'autres personnes ont dit à son sujet. Recherchez des termes tels que "fraude", "escroquerie", "plus jamais" et "faux". Méfiez-vous des promotions ou des offres en ligne qui semblent trop belles pour être vraies. Il est beaucoup plus sûr d'acheter des articles qui peuvent coûter un peu plus cher, mais sur des sites de confiance que vous ou vos amis avez déjà utilisés.

La bonne nouvelle est : Vous êtes votre propre meilleure défense. Vous avez le contrôle. Il suffit d'être attentif aux escroqueries de ce type pour pouvoir profiter pleinement des réseaux sociaux en toute sécurité.

Rédacteur Invité



Chris Elgee (@chriselgee) est testeur d'intrusion et concepteur de défis pour @CounterHackSec, commandant de bataillon cybernétique dans la Garde nationale de l'armée, et instructeur certifié SANS. Il aime apprendre les détails techniques, les intégrer dans une compréhension plus large et organisationnelle et les partager avec les étudiants et les clients.

Ressources

Suivi des escroqueries du Better Business Bureau: https://www.bbb.org/ScamTracker
Ingénierie sociale: https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering
Acheter en ligne en toute sécurité: https://www.sans.org/newsletters/ouch/shopping-online-securely-nov-21/
Arnaques et escroqueries vocales: https://www.sans.org/newsletters/ouch/vishing/

Traduit pour la communauté par: Juliette Busson