Les prises de contrôle de comptes : les prédateurs émotionnels

Prise par surprise : l'histoire d'Emma

Emma défilait les actualités Facebook lorsqu'elle a vu une publication prenante de sa cousine Sarah. La publication annonçait que le père de Sarah avait déménagé dans une maison de retraite et qu'il vendait ses biens pour pouvoir payer les frais médicaux. On y trouvait des photos d'objets tels que sa voiture, des bijoux et des meubles anciens à des prix incroyablement bas.

Désireuse d'aider et de faire une bonne affaire, Emma a rapidement contacté Sarah via Facebook Messenger pour la première fois depuis des années. Sarah était heureuse d'avoir des nouvelles de sa cousine et a tenu Emma au courant de l'état de santé de son père. Sarah a rapidement poussé Emma à passer au paiement car de nombreux articles se vendaient très vite. Emma s'est empressée d'envoyer l'argent, pour découvrir plus tard que l'ensemble du message était une escroquerie.

Emma n'avait jamais été en contact avec sa cousine. Le compte Facebook de Sarah avait été piraté et contrôlé par un escroc. Après avoir obtenu un accès complet, l'escroc a publié de fausses nouvelles sur le père de Sarah, puis a exploité le réseau d'amis et de membres de la famille de Sarah en prétendant vendre ses articles. En pensant acheter des articles à Sarah (et soutenir son père), les gens payaient en réalité un escroc qui s'en allait tout simplement avec leur argent.

Que se passe-t-il ?

Les escrocs détournent les comptes de réseaux sociaux sur des plateformes comme Facebook ou Instagram, souvent en découvrant les noms d'utilisateur et les mots de passe. Une fois qu'ils ont l'accès, ils se font passer pour le propriétaire du compte pour partager de faux messages qui incluent souvent des détails émotionnels pour créer un sentiment d'urgence et pousser les gens à agit. Ces escroqueries consistent souvent à raconter qu'on s'est fait agresser dans une ville et qu'on a besoin d'aide, qu'on a eu un accident de voiture et qu'on a besoin d'argent, ou qu'un être cher est décédé et que ses biens sont en train d'être vendus.

Les victimes sont attirées, croyant que le message provient d'une personne qu'elles connaissent et en qui elles ont confiance. Elles envoient de l'argent, souvent par le biais de méthodes de paiement intraçables telles que les applications peer-to-peer ou les virements électroniques, pour se rendre compte plus tard qu'ils n'ont pas réellement interagit avec leur famille ou leurs amis et que leur argent s'est envolé.

Qu'est-ce qui fait que ces arnaques sont si dangereuses ?

- **Une confiance détournée** : Les escrocs profitent du réseau de confiance des comptes de réseaux sociaux qu'ils prennent en charge. Les messages semblent provenir d'un ami de confiance ou d'un membre de la famille, ce qui les rend plus crédibles.

- **Une manipulation émotionnelle** : Les escrocs utilisent des sujets personnels et émotionnels qui créent souvent un fort sentiment d'urgence ou d'opportunité, poussant les gens à commettre une erreur.
- **Une diffusion rapide** : Une fois que le compte d'une victime est compromis, l'escroc peut rapidement atteindre des centaines, voire des milliers de personnes. En outre, de nombreuses personnes utilisent le même mot de passe pour plusieurs comptes en ligne, de sorte qu'une fois qu'un compte est sous contrôle, le même mot de passe peut être utilisé pour prendre le contrôle des autres comptes de réseaux sociaux de la victime.

Comment se protéger et protéger les autres

- **Soyez sceptique à l'égard des messages émotionnels impliquant de l'argent** : Si un message semble inhabituellement émotif ou urgent et qu'il implique d'envoyer de l'argent à quelqu'un, faites une pause et vérifiez, il pourrait s'agir d'une escroquerie.
- **Vérifiez avec la personne directement** : Contactez la personne par un autre canal pour confirmer l'information. Par exemple, appelez-la au téléphone ou parlez-lui en personne. Très souvent, la victime ne sait même pas que son compte a été pris en charge ou que l'escroc a publié des messages sur son compte.
- **Vérifiez les signaux d'alerte** : Les escrocs demandent souvent d'être payés par des moyens intraçables tels que des cartes-cadeaux ou des bitcoins. Un autre signal d'alarme apparaît si l'on vous demande d'utiliser une autre plateforme pour continuer à communiquer (par exemple, passer de Facebook Messenger à WhatsApp).
- **Protégez votre compte** : Si votre compte est piraté et pris en charge, la première chose que font les cybercriminels est souvent de changer votre mot de passe, ce qui vous empêche d'accéder à votre compte. Une fois que cela se produit, il est très difficile de récupérer votre compte. Commencez par protéger chacun de vos comptes par un mot de passe long et unique. Activez ensuite l'authentification multifactorielle pour chaque compte. Ces deux mesures simples rendent vos comptes beaucoup plus sûrs, et les escrocs vous détesteront pour cela !

Gardez une longueur d'avance

Lorsqu'il s'agit d'escroqueries par vol de compte, vous êtes votre meilleure défense. Si vous pensez avoir été victime de cette escroquerie, signalez le compte et informez immédiatement votre plateforme de réseaux sociaux.

Rédacteur invité

Amie Dsouza est une professionnelle de la cybersécurité qui travaille pour une grande compagnie aérienne américaine. Elle a travaillé dans six pays et siège au conseil d'administration de Women in Cybersecurity (WiCys). Amie milite activement pour l'éducation de tous à la sécurité des données personnelles en ligne.

Ressources

Déclencheurs émotionnels : comment les escrocs vous piégent : https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Comment les cybercriminels volent vos mots de passe : https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords
Le pouvoir de la phrase de passe : https://www.sans.org/newsletters/ouch/power-passphrase/
J'ai été piraté, que faire ? : https://www.sans.org/newsletters/ouch/im-hacked-now-what/

Traduit pour la communauté par : Juliette Busson