Votre bulletin mensuel sur la sensibilisation à la sécurité

Les escroqueries liées aux associations caritatives et aux crises

Les cyber-criminels savent qu'une des meilleures manières de piéger les gens est de créer un fort sentiment d'urgence. Et l'un des meilleurs moyens de créer un sentiment d'urgence est de profiter d'une crise. C'est pour cette raison que les cyber-criminels adorent lorsqu'un événement traumatisant a un impact mondial. Ce que la plupart d'entre nous voient comme une tragédie, les cyber-criminels le voient comme une opportunité, tel que le déclenchement d'une guerre, une catastrophe naturelle comme l'éruption d'un volcan, et bien sûr le déclenchement de maladies infectieuses comme le COVID-19. Les cybercriminels savent que c'est le moment de frapper lorsqu'un événement est largement couvert par les réseaux sociaux et l'actualité.

Ils en profitent pour créer des e-mails d'hameçonnage ou des escroqueries à propos de l'événement, puis envoient cet e-mail ou lancent l'escroquerie à des millions de personnes dans le monde. Par exemple, lors d'une catastrophe naturelle, ils peuvent se faire passer pour une association caritative et vous demander des dons pour sauver les enfants dans le besoin. Les cyber-criminels peuvent souvent agir dans les heures qui suivent une crise puisqu'ils disposent de toute l'infrastructure technique nécessaire et sont prêts à l'avance. Comment pouvons-nous nous protéger la prochaine fois qu'il y a une grosse crise et que les cyber-criminels prévoient de l'exploiter ?

Comment détecter et comment se défendre contre ces attaques

La clé pour éviter ces escroqueries est de se méfier de toute personne qui essaie de vous contacter. Par exemple, ne faites pas confiance à un e-mail urgent qui affirme venir d'une association caritative qui a besoin de dons, même si le mail vient d'une marque que vous connaissez. Ne faites pas confiance à un appel qui prétend venir d'une banque alimentaire et qui insiste pour que vous fassiez un don. Plus vous avez une impression d'urgence, plus vous avez de chance que ce soit une arnaque. Voici les indices les plus fréquents d'une attaque :

- Méfiez-vous de toute organisation caritative qui vous demande de faire un don via crypto-monnaie, Western Union, des transferts d'argent ou des cartes-cadeaux.
- Les cyber-criminels peuvent changer leur numéro de téléphone de sorte à faire croire qu'ils appellent depuis un endroit que vous connaissez. On ne peut plus se fier à l'identificateur d'appels de nos jours.
- Certains cyber-criminels utiliseront des noms et des logos qui ressemblent vraiment à une véritable organisation caritative. C'est pour cela qu'il faut faire des recherches avant de faire des dons.
- Les cybercriminels font souvent des déclarations vagues et sentimentales sur ce qu'ils feront de votre argent, mais ne donnent aucune précision sur l'utilisation de votre don.

- Ne supposez pas que les appels à l'aide sur les sites de financements participatifs comme GoFundMe ou les sites de réseaux sociaux comme TikTok sont légitimes, surtout à la suite d'une crise ou d'une tragédie.
- Certains cyber-criminels peuvent essayer de vous piéger en vous remerciant pour un don que vous avez effectué dans le passé, alors qu'en réalité vous ne leur avez jamais donné.
- Ne donnez pas d'informations personnelles ou financières en réponse à une demande non sollicitée.

Comment faire la différence en toute sécurité

Pour faire un don en cas de besoin ou pour aider les personnes touchées par une catastrophe, ne donnez qu'à des organisations connues et de confiance. C'est vous qui initiez les connexions et décidez des personnes à contacter, en choisissant par exemple les sites web à visiter ou les organisations à appeler. Lorsque vous voulez faire un don, faites des recherches sur l'association caritative en tapant son nom sur internet suivi des termes « plaintes », « avis » ou « arnaque ». Vous ne savez pas à quelle association vous pouvez faire confiance ? Commencez par faire des recherches sur des sites gouvernementaux auxquels vous faites confiance, ou peut-être sur des liens fournis par un organisme d'information connu et très fiable. Faire un don en cas de besoin est un moyen fantastique de faire la différence, mais assurez-vous que vous donnez à des organisations légitimes.

Rédacteur Invité

Dr Jessica Barker (@drjessicabarker) est la leader du côté humain de la cybersécurité. Elle est co-PDG de Cygenta et auteur de best-sellers. Jessica est membre du comité consultatif du SANS Security Awareness Summit.

Ressources

FTC Fraude à la charité : https://consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams
Ingénierie sociale: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Top trois des arnaques: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Hameçonnage par message: https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks
Arnaques et escroqueries vocales: https://www.sans.org/newsletters/ouch/vishing/
Navigateur des associations caritatives : https://www.charitynavigator.org/

Traduit pour la communauté par : Juliette Busson