Votre publication mensuelle de conscientisation à propos de la Sécurité

Vishing - Attaques et escroqueries par appel téléphonique

Aperçu

Quand vous pensez à un cybercriminel, vous pensez probablement à un génie diabolique assis derrière un ordinateur, lançant des attaques sophistiquées sur Internet. Alors que certains des cybercriminels d'aujourd'hui utilisent des technologies avancées, plusieurs utilisent simplement le téléphone pour tromper leurs victimes. Il y a deux avantages majeurs à utiliser un téléphone: Contrairement aux autres attaques, il existe moins de technologies de sécurité capables de détecter et d'arrêter une attaque par appel téléphonique; de plus, il est beaucoup plus facile pour les criminels d'utiliser des émotions et de bâtir la confiance par téléphone, ce qui permet de tromper plus facilement leurs victimes. Apprenons à détecter et arrêter ces attaques.

Comment fonctionnent les attaques par appel téléphonique?

Tout d'abord, comprenez que ces criminels recherchent généralement votre argent, vos informations ou l'accès à votre ordinateur (ou aux trois). Ils font ceci en vous incitant à faire quelque chose que vous ne devriez pas faire, une technique appelée « ingénierie sociale ». Les cybercriminels créent souvent des situations qui semblent très urgentes et réalistes lors de l'appel. Certains des exemples les plus courants incluent:

- La personne au téléphone prétend être du gouvernement et vous informe que vous avez des impôts impayés. Ils disent que vous irez en prison si vous ne payez pas vos impôts tout de suite, puis ils vous poussent à payer vos impôts avec votre carte de crédit par téléphone. C'est une arnaque. Le gouvernement envoie des avis fiscaux officiels uniquement par la poste.
- La personne au téléphone prétend travailler pour une entreprise telle que Amazon, Apple ou le Support Technique de Microsoft et explique que votre ordinateur est infecté. Une fois qu'ils vous ont convaincu que votre ordinateur est infecté, ils vous poussent à acheter leur logiciel ou à leur donner un accès à distance à votre ordinateur.
- Un message vocal automatisé vous informe que votre compte bancaire ou votre carte de crédit a été annulé et que vous devez rappeler un numéro pour le réactiver. Lorsque vous appelez, vous tombez sur un système automatisé qui vous demande de confirmer votre identité ainsi que toutes sortes de questions privées. Il ne s'agit en aucun cas de votre banque. Ils enregistrent simplement toutes vos informations pour effectuer une fraude d'identité.

Se protéger

La meilleure défense que vous avez contre une attaque par appel téléphonique, c'est vous-même. Gardez ces choses à l'esprit:

- Chaque fois que quelqu'un vous appelle et induit un fort sentiment d'urgence ou de pression, soyez extrêmement méfiant. Ils essaient de vous pousser à commettre une erreur. Même si l'appel téléphonique semble correct au début, s'il commence à vous paraître étrange, vous pouvez arrêter et dire «non» à tout moment.
- Méfiez-vous particulièrement des gens qui vous appellent et qui insistent pour que vous achetiez des cartes-cadeaux ou des cartes de débit prépayées.
- Ne faites jamais confiance à l'afficheur. Les personnes malintentionnées usurpent souvent le numéro afin qu'il semble provenir d'une organisation légitime ou qu'il ait le même indicatif régional que votre numéro de téléphone.
- Ne permettez jamais à quelqu'un au téléphone de prendre le contrôle temporaire de votre ordinateur ou de vous inciter à télécharger un logiciel. C'est ainsi qu'ils peuvent infecter votre ordinateur.
- Sauf si vous avez passé l'appel, ne donnez jamais à l'interlocuteur les informations qu'il devrait déjà avoir. Par exemple, si la banque vous a appelé, elle ne devrait pas vous demander votre numéro de compte.
- Si vous pensez qu'un appel téléphonique est une attaque, raccrochez simplement. Si vous souhaitez confirmer que l'appel téléphonique était légitime, accédez au site Web de l'organisation (par exemple, votre banque) et appelez directement vous-même le numéro de téléphone du service client. De cette façon, vous savez vraiment que vous parlez à la vraie organisation.
- Si un appel téléphonique provient d'une personne que vous ne connaissez pas personnellement, laissez l'appel passer directement à la messagerie vocale. De cette façon, vous pouvez consulter les appels inconnus à votre rythme. Mieux encore, sur de nombreux téléphones, vous pouvez l'activer par défaut avec la fonction «Ne pas déranger».

Les escroqueries et les attaques par téléphone sont en augmentation. Vous êtes la meilleure défense pour les détecter et les arrêter.

Rédacteur invité

Jen Fox est titulaire de l'insigne noir DEF CON 23 pour l'ingénierie sociale et fournit une éducation de sensibilisation à la sécurité en tant que spécialiste des programmes de sécurité chez Domino's. Vous pouvez rejoindre Jen sur Twitter en tant que @j_fox.

Ressources

Ingénierie sociale: https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
Attaques de messagerie/smishing: https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks
Escroqueries Personnalisées: https://www.sans.org/security-awareness-training/resources/personalized-scams
Signaler une arnaque téléphonique (aux États-Unis): https://www.reportfraud.ftc.gov

Traduit pour la communauté par: Jérôme Boutin et Sebastien Kierszka