SANS SECURITY AWARENESS

Attaques de messagerie / Smishing

Aperçu

L'un des moyens les plus employés par les cyber-attaquants pour tromper les gens consiste à vous escroquer lors d'attaques par e-mail (souvent appelées phishing) ou à tenter de vous piéger par téléphone. Cependant, plus la technologie avance, plus les criminels essaient de nouvelles méthodes, y compris des technologies de messagerie telles que le SMS, iMessage / Facetime, WhatsApp, Slack ou Skype. Voici des étapes simples pour vous protéger ou repérer / arrêter ces attaques.

Quelles sont les attaques de messagerie ?

Les attaques de messagerie (parfois appelées Smishing, un jeu sur le mot Phishing) se produisent lorsque des cyber-attaquants utilisent des technologies de SMS ou autres types de messageries pour vous contacter et tenter de vous pousser à faire quelque chose que vous ne devriez pas faire. Peut-être vont-ils vous pousser à cliquer sur un lien malveillant ou vous demander d'appeler un numéro de téléphone pour obtenir vos coordonnées bancaires. Comme pour les attaques de hameçonnage traditionnelles, les criminels jouent souvent avec vos émotions pour agir. Cependant, ce qui rend les attaques par messagerie si dangereuses, c'est qu'elles sont souvent plus informelles ou personnelles que les e-mails, ce qui augmente le risque d'en être victime. De plus, avec les attaques de messagerie, il y a moins d'informations et / ou d'indices pour que vous puissiez voir que quelque chose semble suspect. Lorsque vous recevez un message qui semble étrange ou suspect, commencez par vous demander si ce message a un sens et pourquoi vous le recevez. Voici les indices les plus fréquents d'une attaque.

Un sentiment d'urgence très fort, lorsque quelqu'un tente de vous pousser à agir.

Ce message demande-t-il des informations personnelles, des mots de passe ou autres informations sensibles auxquelles ils ne devraient pas avoir accès ?

Le message semble-t-il trop beau pour être vrai ? Non, vous n'avez pas gagné au Loto, surtout si vous n'avez pas joué !

Un message qui semble provenir d'un compte ou d'un numéro de téléphone d'un collègue ou d'un ami, mais dont la tournure ne lui ressemble pas. Leur compte a peut-être été compromis et repris par un criminel, ou bien le criminel tente de se faire passer pour eux et vous incite à prendre des mesures.

Si vous recevez un message qui vous a fait réagir fortement, attendez un moment et prenez le temps de vous calmer et de réfléchir avant de répondre.

Parfois, les criminels combinent même des attaques par e-mail et par messagerie. Par exemple, les escroqueries par cartes cadeaux peuvent fonctionner de cette façon. Un cyber-attaquant vous enverra un e-mail urgent prétendant être un ami ou un collègue, puis vous demandera votre numéro de téléphone portable. Ils peuvent ensuite envoyer des textos à répétition, vous incitant à acheter des cartes cadeaux. Une fois achetées, les criminels vous demandent de gratter le code au dos des cartes et de leur envoyer une photo des codes. Une autre attaque courante vous pousse à regarder une vidéo ou une image (« vous n'y croirez pas ! »). Cela attise votre curiosité. Si le message semble provenir de quelqu'un que vous connaissez, appelez peut-être la personne au téléphone pour vérifier avant d'agir.

Si vous recevez un message d'alerte d'un organisme officiel, vérifiez directement auprès d'eux. Par exemple, si vous recevez un SMS de votre banque indiquant qu'il y a un problème avec votre compte ou votre carte de crédit, contactez directement votre banque en visitant leur site web ou en l'appelant directement à l'aide du numéro situé à l'arrière de votre carte bancaire. N'oubliez pas que la plupart des administrations, telles que les impôts ou la sécurité sociale, ne vous contacteront pas par SMS.

En ce qui concerne les attaques de messagerie, vous êtes votre meilleure défense.

Rédacteur Invité

Jen Fox *détient le badge noir DEF CON 23 pour l'ingénierie sociale et dispense des cours de sensibilisation à la sécurité en tant que spécialiste des programmes de sécurité chez Domino's. Vous pouvez la suivre sur Twitter :* @j_fox.

Ressources

Ingénierie sociale :	http://www.sans.org/u/XAQ
Stop au hameçonnage :	http://www.sans.org/u/XAV
Arnaque téléphonique :	http://www.sans.org/u/XB0
Signaler des textos frauduleux :	https://www.consumer.ftc.gov/articles/0350-text-message-spam