OUCH! | Juillet, 2018

SANS SECURITY AWARENESS

OUCH!

La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

Attaques téléphoniques & escroqueries

Vue d'ensemble

Quand vous pensez aux cybercriminels, vous pensez probablement à un cerveau maléfique assis derrière un ordinateur lançant des attaques sophistiquées sur Internet. Alors que de nombreux cybercriminels utilisent des technologies telles que le courrier électronique ou la messagerie instantanée, les malfaiteurs utilisent également le téléphone pour tromper leurs victimes. Il y a deux gros avantages à utiliser un téléphone. Tout d'abord, contrairement au courrier électronique, il y a moins de technologies de sécurité qui surveillent les appels téléphoniques et qui peuvent ainsi détecter et arrêter une attaque. Deuxièmement, il est beaucoup plus facile pour les criminels de transmettre des émotions par téléphone, ce qui les rend plus susceptibles de tromper leurs victimes. Apprenons à repérer et arrêter ces attaques.

Comment fonctionnent les attaques par appel téléphonique?

D'abord, vous devez comprendre ce que ces attaquants recherchent. Ils veulent généralement votre argent, vos informations ou votre accès à votre ordinateur (ou les trois). Ils le font en vous incitant à faire ce qu'ils veulent. Les criminels appellent des gens partout dans le monde, créant des situations qui semblent très urgentes. Ils veulent vous déséquilibrer en vous effrayant afin que vous ne puissiez pas avoir les idées claires, et ensuite vous précipiter à faire une erreur. Certains des exemples les plus courants comprennent:

L'appelant prétend qu'il provient d'un service des impôts du gouvernement ou d'un service de recouvrement des impôts et que vous avez des impôts impayés. Il explique que si vous ne payez pas vos impôts tout de suite, vous irez en prison, puis vous oblige à payer vos impôts avec votre carte de crédit par téléphone. Ceci est une arnaque, de nombreux services fiscaux, y compris l'IRS, n'appellent jamais et n'envoient jamais d'emails. Toutes les notifications fiscales officielles sont envoyées par courrier postal.

L'appelant prétend qu'il s'agit du support technique Microsoft et vous explique que votre ordinateur est infecté. Une fois qu'il vous a convaincu que vous êtes infecté, il vous pousse à acheter son logiciel ou à lui donner un accès à distance à votre ordinateur. Sachez que Microsoft n'appelle pas chez vous.

Vous recevez un message vocal automatique indiquant que votre compte bancaire a été suspendu et que vous devez rappeler un numéro pour le réactiver. Lorsque vous appelez, vous obtenez un système automatisé qui vous demande de confirmer votre identité et vous pose toutes sortes de questions privées. Il ne s'agit pas de votre banque, les criminels enregistrent simplement toutes vos informations pour procéder à une fraude d'identité.

Protégez-vous

La meilleure défense dont vous disposez contre les attaques par appel téléphonique c'est vous-même. Gardez bien cela à l'esprit.

Chaque fois que quelqu'un vous appelle et crée un énorme sentiment d'urgence, vous presse de faire quelque chose, soyez extrêmement méfiant. Même si l'appel téléphonique semble pertinent au début, mais commence à devenir suspect, vous pouvez l'arrêter et dire «non» à tout moment.

Si vous croyez qu'un appel téléphonique est une attaque, raccrochez simplement. Si vous souhaitez confirmer que l'appel téléphonique était légitime, rendez-vous sur le site Web de l'organisation (par exemple, votre banque) et obtenez le numéro de téléphone du service clientèle et appelez-les directement. De cette façon, vous savez vraiment que vous parlez à la vraie organisation.

Ne croyez jamais à l'identification de l'appelant, les personnes malveillantes usurpent souvent le numéro de l'appelant pour 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 un appelant de prendre le contrôle temporaire de votre ordinateur ou de vous inciter à télécharger un logiciel. C'est ainsi que les criminels peuvent infecter votre ordinateur.

Si un appel provient d'une personne que vous ne connaissez pas personnellement, laissez l'appel passer directement sur la messagerie vocale. De cette façon, vous pouvez prendre le temps de passer en revue les appels inconnus. Encore mieux, sur de nombreux téléphones, vous pouvez activer cette option par défaut avec la fonction "Ne pas déranger".

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

Version Française

La société Pélissier & Partners spécialiste en Intelligence économique a été fondée sur une expérience de plus de quinze ans dans le domaine de la recherche d'information et de la cybersécurité dédiées aux dirigeants d'entreprises suisses.

Editeur invité

Jen Fox *offre des services de sensibilisation à la sécurité, d'ingénierie sociale et d'évaluation des risques en tant que conseillère principale en sécurité chez All Covered. Trouvez Jen sur Twitter en tant que* @j_fox.

Sources

Information du consommateur sur l'identité, la confidentialité et la sécurité en ligne:
https://www.consumer.ftc.gov/topics/privacy-identity-online-security
Signalez une arnaque téléphonique (aux États-Unis): https://www.ftccomplaintassistant.gov/#crnt
Ingénierie sociale: https://www.sans.org/u/Fi5

Comité de rédaction : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Traduit par : Marilyn Combet