OUCH! Mayo 2021

El Boletín Mensual de Concientización en Seguridad para ti

Vishing - Ataques y estafas a través de llamadas telefónicas

Resumen

Cuando piensas en un ciberdelincuente, probablemente pienses en una mente maestra malvada sentada detrás de una computadora, lanzando ataques sofisticados a través de Internet. Si bien algunos de los ciberdelincuentes actuales utilizan tecnologías avanzadas, muchos simplemente usan el teléfono para engañar a sus víctimas. Hay dos grandes ventajas de usar un teléfono: A diferencia de otros ataques, hay menos tecnologías de seguridad que pueden detectar y detener un ataque a través de una llamada telefónica. Además, es mucho más fácil para los delincuentes transmitir emociones y generar confianza por teléfono, lo que facilita engañar a sus víctimas. Aprendamos a detectar y detener estos ataques.

¿Cómo funcionan los ataques a través de llamadas telefónicas?

Primero, comprende que estos criminales usualmente buscan tu dinero, información o acceso a tu computadora (o los tres). Lo hacen engañándote para que hagas algo que no debes hacer, una técnica llamada "ingeniería social". Los ciberdelincuentes a menudo crean situaciones con sentido de urgencia y que parecieran reales durante la llamada. Algunos de los ejemplos más comunes incluyen:

- La persona que llama finge que es del gobierno y te informa que tienes impuestos sin pagar. Te explican que si no pagas tus impuestos de inmediato, irás a la cárcel y luego te presionarán para que los pagues con tu tarjeta de crédito por teléfono. Ésto es un fraude. El gobierno enviará notificaciones fiscales oficiales solo por correo ordinario.
- La persona que llama pretende ser de una empresa como Amazon, Apple o Microsoft Tech Support y te explica que tu computadora está infectada. Una vez que te convence de que tu computadora está infectada, te presiona para que compres su software o le des acceso remoto a tu computadora.
- Un correo de voz automatizado te informa que tu cuenta bancaria o tarjeta de crédito ha sido cancelada, y debes volver a llamar a un número para reactivarlo. Cuando llamas, ingresas a un sistema automatizado que te pide confirmar tu identidad, así como contestar varias preguntas privadas. Este no es realmente tu banco. Simplemente están registrando toda tu información para robar tu identidad.

Protegiéndote a ti mismo

La mayor defensa que tienes contra un ataque de llamada telefónica eres tú mismo. Ten en cuenta estas cosas:

© SANS Institute 2021

- Siempre que alguien te llame y cree una sensación enorme de urgencia o presión, se extremadamente desconfiado. Los atacantes intentan apresurarte a cometer un error. Incluso si la llamada telefónica parece estar bien al principio, si comienzas a sentirte extraño, puedes detenerte y decir "no" en cualquier momento
- Ten especial cuidado con las personas que llaman que insisten en que compres tarjetas de regalo o tarjetas de prepago.
- Nunca confíes en el identificador de llamadas. Los malos suelen falsificar el número de origen de la llamada, por lo que parece que proviene de una organización legítima o tiene el mismo código de área que tu número de teléfono.
- Nunca permitas que una persona que llama tome el control temporal de tu computadora o te engañe para que descargues software. Así es como pueden infectar tu computadora.
- A menos que tú hayas realizado la llamada, nunca le des a la otra persona información que ya debería tener. Por ejemplo, si el banco te llamó, no deberían pedirte tu número de cuenta.
- Si crees que una llamada telefónica es un ataque, simplemente cuelga. Si deseas confirmar que la llamada telefónica fue legítima, ve al sitio web de la organización (como tu banco) y llama directamente al número de teléfono de atención al cliente. De esa manera, realmente sabrás que estás hablando con la organización real.
- Si una llamada telefónica proviene de alguien que no conoces personalmente, deja que la llamada vaya directamente al correo de voz. De esta forma, puedes revisar las llamadas desconocidas en cuanto tengas tiempo. Aún mejor, en muchos teléfonos puedes habilitar esto de forma predeterminada con la función "No molestar".

Las estafas y los ataques por teléfono van en aumento. Eres la mejor defensa para detectarlos y detenerlos.

Editor invitado

Jen Fox tiene la insignia negra de DEF CON 23 por Ingeniería social y enseña concientización en seguridad como Especialista del Programa de Seguridad en Domino's. Encuentra a Jen en Twitter como @j_fox.

Recursos

Ingeniería social: https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
Ataques a través de mensajería instantánea: https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks
Estafas personalizadas: https://www.sans.org/security-awareness-training/resources/personalized-scams
Reporta estafas telefónicas (en EE.UU.): https://www.reportfraud.ftc.gov

Traducido para la comunidad por: Célica Martínez Aponte, UNAM-CERT

OUCH! Es publicado por SANS Security Awareness y distribuido bajo la licencia Creative Commons BY-NC-ND 4.0. Puedes distribuir y compartir este boletín, siempre y cuando no lo vendas o modifiques. Consejo editorial: Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.