Boletín mensual de concientización en seguridad para ti

Estafas personalizadas

Resumen

Los cibercriminales continúan creando nuevas y creativas formas de engañar a la gente. Una nueva forma de estafa está ganando popularidad: las estafas personalizadas. Los cibercriminales encuentran o compran información de millones de personas y luego utilizan esa información para personalizar los ataques. A continuación, te mostramos cómo funcionan estas estafas y te guiamos a través de un ejemplo común. Mientras más sepas sobre estas estafas será más fácil para ti detectarlas y evitarlas.

¿Cómo funcionan?

Las estafas por correo electrónico y por teléfono no son nuevas, los cibercriminales han intentado engañar a las personas por años. Algunos ejemplos son: "Ganaste la lotería" o las estafas del Príncipe de Nigeria; sin embargo, en estos engaños tradicionales los cibercriminales no saben a quién se están dirigiendo, simplemente crean un mensaje genérico y lo envían a millones de personas. Debido a que estas estafas son tan genéricas, usualmente son fáciles de detectar. Una estafa personalizada es diferente, primero los cibercriminales realizan una investigación y luego crean un mensaje específico para cada víctima, esto lo hacen buscando o comprando bases de datos de nombres de personas, contraseñas, teléfonos u otros detalles. Este tipo de información fácilmente está disponible debido a todos los sitios que ya han sido hackeados, también está disponible en las redes sociales y en los registros públicos del gobierno. Una vez que cuentan con esta información, los cibercriminales dirigen sus ataques a las personas de las que han obtenido sus datos.

Un truco común que los cibercriminales utilizan es el miedo y la extorsión para obligarte a pagarles dinero. Ellos encuentran o compran una base de datos que incluye usuarios y contraseñas, los cuales obtienen de sitios web hackeados. Encuentran la información de tu cuenta en dicha base de datos y te envían a ti (y a todos los demás en esa base) un correo electrónico con algunos de tus datos personales, incluyendo la contraseña original que utilizas en el sitio web que fue vulnerado. En el mensaje el criminal se refiere a tu contraseña como "prueba" de que han hackeado tu computadora o dispositivo, lo cual, por supuesto, no es cierto. También afirma que mientras hackeaban tu computadora te sorprendieron viendo pornografía. Finalmente, te amenazan con el pago de una tarifa, la cual debes liquidar o de lo contrario compartirán con tu familia y amigos evidencia de tus actividades embarazosas en línea.

El problema es que, en casi todas las situaciones como esta, el ciberdelincuente nunca hackeo tu sistema ni siquiera saben quién eres o qué sitios web has visitado. El estafador simplemente está tratando de usar los pocos datos personales que

tiene de ti para asustarte y hacerte creer que hackearon tu computadora o dispositivo y engañarte para que pagues el dinero. Recuerda, que los cibercriminales también pueden usar las mismas técnicas para estafas por teléfono.

¿Qué tengo que hacer?

Identifica los correos electrónicos y llamadas telefónicas que como esta son una estafa. Es natural sentir miedo cuando alguien tiene información personal sobre ti. Sin embargo, recuerda que el remitente está mintiendo. El ataque es parte de una campaña automatizada a gran escala, no es un intento para dirigirse solo a ti. Hoy en día es mucho más fácil para los delincuentes cibernéticos encontrar o comprar información personal, por lo que puedes esperar estafas como esta, posiblemente, cada vez más personalizadas en el futuro. Algunas pistas para identificarlas son:

- **Cada vez que recibas un correo, mensaje o llamada telefónica con un alto sentido de urgencia, sospecha.**
- **Cuando alguien exige un pago en Bitcoins, tarjetas de regalo u otros métodos no rastreables.**
- **Cuando recibes un correo electrónico sospechoso, busca en Google si otras personas han reportado ataques similares.**

Por último, el sentido común es tu mayor defensa. También, te recordamos que utilices una contraseña larga y única para cada una de tus cuentas en línea. ¿No puedes recordar todas tus contraseñas? Utiliza un gestor de contraseñas. Además, habilita la verificación en dos pasos siempre que sea posible.

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Editor Invitado

Lenny Zeltser *es veterano en ciberseguridad, desarrolla soluciones anti-malware en Minerva Labs y enseña ciberseguridad en el SANS Institute. Su experiencia también incluye la gestión de servicios de seguridad y consultoría. Síguelo en* zeltser.com/blog *y en Twitter* @lennyzeltser.

Recursos

Ingeniería social:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_sp.pdf
Evita el phishing:	https://www.sans.org/sites/default/files/2018-04/201804-OUCH-April-Spanish.pdf
¿Qué es el phishing?:	https://www.seguridad.unam.mx/que-es-el-phishing-2
Búscate a ti mismo en línea:	https://www.sans.org/sites/default/files/2019-01/201901-OUCH-January-Spanish.pdf
Gestores de contraseñas:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201709_sp.pdf