OUCH!

SANS SECURITY AWARENESS

Boletín mensual de concientización en seguridad para ti

Sí, tú eres un objetivo

Resumen

Muchas personas creen erróneamente que ellos no son un objetivo de los ciber atacantes, que sus sistemas o sus cuentas no tienen ningún valor. Esto no podría estar más lejos de la verdad. Si utilizas tecnología de algún modo, en el trabajo o en casa, confía en nosotros – tú tienes valor para los chicos malos. Pero, estas de suerte, ya tienes la mejor defensa que existe contra esos ciber ataques, tú.

¿Por qué tú eres un objetivo?

Hoy en día, en Internet existen diversos tipos de ciber atacantes con diferentes motivaciones. Entonces, ¿por qué alguno de ellos quisiera atacarte? Porque si te hackean ayudas a lograr su meta. Aquí hay dos ejemplos comunes de ciber atacantes y las razones por las que te atacarían.

⚠ **Ciber criminales:** Estos chicos están afuera para ganar tanto dinero como sea posible. Lo que hace que Internet sea tan valioso para ellos es que ahora pueden dirigirse fácilmente a cualquier persona en el mundo con tan solo presionar un botón. Hay MUCHAS formas en la que pueden ganar dinero gracias a ti, por ejemplo, robar dinero de tu cuenta bancaria o de retiro, crear una tarjeta de crédito a tu nombre y enviarte la factura, usar tu computadora para hackear otras personas, hackear tus redes sociales o cuentas de juego y venderlas a otros criminales. La lista es casi interminable de cómo los chicos malos pueden hacer dinero de ti. Hay cientos de miles de estos chicos malos que se despiertan cada mañana con la meta de hackear a la mayor cantidad de personas como sea posible todos los días, incluyéndote a ti.

☆ **Atacantes dirigidos:** Estos ciber atacantes están altamente entrenados, con frecuencia trabajan para gobiernos, sindicatos criminales o competidores, que suelen verte como un objetivo en tu trabajo. Puedes sentir que tu trabajo no atrae mucha atención, pero te sorprendería lo valioso que eres para ellos.

- La información que manejas en el trabajo tiene un tremendo valor para diferentes gobiernos o compañías.
- Puedes ser objetivo de los atacantes dirigidos en el trabajo, no porque ellos no quieran hackearte sino porque te usan para hackear a uno de tus compañeros de trabajo u otros sistemas.

- **Este tipo de ataques pueden estar dirigidos a ti en el trabajo debido a las empresas con las que trabajas o colaboras.**

Tengo antivirus, estoy seguro

Bueno, entonces soy el objetivo, no hay problema. Solo tengo que instalar un antivirus y un firewall en mi computadora y estoy protegido, ¿cierto? Desafortunadamente, no. Muchas personas sienten que si instalan algunas herramientas de seguridad entonces ellos estarán seguros. Lamentablemente, esto no es completamente cierto. Los ciber atacantes continúan mejorando y ahora muchos de sus métodos de ataque pueden fácilmente evitar tecnologías de seguridad. Por ejemplo, ellos con frecuencia crean malware especial que los antivirus no pueden detectar. Evitan filtros de correo electrónico con un ataque personalizado de phishing o te llaman por teléfono para engañarte o estafarte con tu tarjeta de crédito, dinero o contraseñas. La tecnología juega un papel muy importante en tu protección, pero al final, la mejor defensa eres tú.

Afortunadamente, estar seguro no es tan difícil, en el fondo, el sentido común y algunos comportamientos básicos son tu mejor defensa. Si recibiste un correo electrónico, mensaje o llamada telefónica que es extremadamente urgente, extraña o sospechosa puede ser un ataque. Para asegurar que tu computadora y dispositivos estén seguros, mantenlos actualizados y habilita las actualizaciones automáticas. Finalmente, usa una frase de contraseña fuerte y única para cada una de tus cuentas. Mantente ciber-consiente, es al final tu mejor defensa. ¿No estás seguro por dónde empezar? Considera suscribirte al boletín mensual OUCH! en sans.org/ouch

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

Matt Bromiley *(@mbromileyDFIR) es experto en análisis forense digital y respuesta a incidentes con más de 8 años de experiencia, ha trabajado con incidentes y organizaciones en todo el mundo. Matt también es instructor de Análisis Forense Digital y Respuesta a Incidentes (DFIR, por sus siglas en inglés) enseñando los cursos de FOR508 y FOR572 del SANS.*

Recursos

Evita el malware:	https://www.sans.org/u/L1J
Ingeniería social:	https://www.sans.org/u/L1O
Ataques telefónicos y estafas:	https://www.sans.org/u/L1T
Frases de contraseña:	https://www.sans.org/u/L1Y
Póster - You Are a Target:	https://www.sans.org/u/L23

 Consejo editorial: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Traductores: Sergio Anduin Tovar Balderas Célica Martínez Aponte