Boletín mensual de concientización en seguridad para ti

Estafas a través de las redes sociales

Resumen

Muchos de nosotros hemos recibido ataques de phishing por correo electrónico, ya sea en el trabajo o en casa. Estos son correos electrónicos que parecen legítimos, como los de tu banco, tu jefe o tu tienda en línea favorita. Sin embargo, estos realmente son un ataque, que intentan apresurarte o engañarte para que tomes una acción que no debes tomar, como abrir un archivo adjunto de correo electrónico infectado, compartir tu contraseña o transferir dinero. El desafío es que cuanto más conocemos y detenemos estos ataques por correo electrónico, más delincuentes cibernéticos intentan otras formas de contactar y estafar a las personas.

Los intentos de estafa o engaño pueden ocurrir en casi cualquier forma de comunicación que uses, desde Skype, WhatsApp, Slack, Twitter, Facebook, Snapchat, Instagram o incluso aplicaciones de juegos. La comunicación a través de estas plataformas o canales puede parecer más informal o confiable, razón por la cual los atacantes los están utilizando para engañar a otros. Además, con las tecnologías actuales, se ha vuelto mucho más fácil para cualquier atacante en cualquier parte del mundo pretender ser lo que quiera. Es importante recordar que cualquier comunicación que se presente en tu camino puede no ser lo que parece y que las personas no siempre son lo que aparentan ser.

Conclusiones clave

Estas son las pistas más comunes para detectar que el mensaje que acabas de recibir o la publicación que acabas de leer puede ser un ataque.

Urgencia: un mensaje que tiene un sentido de urgencia que exige “acción inmediata” antes de que ocurra algo malo, como amenazar con cerrar una de tus cuentas o enviarte a la cárcel. El atacante quiere apresurarte a cometer un error.

Presión: ejerce presión para que omitas o ignores las políticas o procedimientos en el trabajo.

Curiosidad: un fuerte sentido de curiosidad o algo que es demasiado bueno para ser verdad. No, no ganaste la lotería.

Información sensible: una solicitud de información altamente sensible, como el número o la contraseña de tu tarjeta de crédito, o cualquier información que simplemente no te sientas cómodo compartiendo.

Mensajes oficiales: el mensaje dice provenir de una organización oficial, pero tiene una gramática u ortografía deficientes. La mayoría de las organizaciones gubernamentales no utilizarán las redes sociales para las comunicaciones oficiales directamente contigo. Si no estás seguro de si el mensaje es legítimo, vuelve a llamar a la organización, pero usa un número de teléfono confiable, como uno de su sitio web.

Suplantación: recibes un mensaje de un amigo o compañero de trabajo, pero el tono o la redacción simplemente no suena como ellos. Si sospechas, llama al remitente por teléfono para verificar que envió el mensaje. Es fácil para un atacante cibernético crear mensajes que parecen ser de alguien que conoces. En algunos casos, pueden tomar el control de una cuenta de un amigo, luego pretender ser él y comunicarse contigo. Ten especial cuidado con los mensajes de texto, como Twitter y otros formatos de mensajes cortos, que es más difícil tener una idea de la personalidad del remitente.

Eres la mejor defensa contra estafas y ataques como estos. Si una publicación o mensaje parece extraño o sospechoso, simplemente ignóralo o elimínalo, o si es de alguien que conoces personalmente, llama a la persona por teléfono para confirmar si realmente lo envió.

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

La Dra. Jessica Barker *(@drjessicabarker) es líder en el enfoque humano de la ciberseguridad. Es co-CEO de Cygenta, donde sigue su pasión de influir positivamente en la conciencia, los comportamientos y la cultura de ciberseguridad en todo el mundo. Es la presidenta de ClubCISO y una conferencista reconocida.*

Recursos

Ingeniería social:	https://www.sans.org/u/Uz6
Ataques telefónicos y engaños:	https://www.sans.org/u/Uzb
Evita el phishing:	https://www.sans.org/u/Uzg
Estafas personalizadas:	https://www.sans.org/u/Uzl
¿Qué es el phishing?:	https://www.seguridad.unam.mx/que-es-el-phishing-2