OUCH! Octubre 2022

El Boletín Mensual de Concientización en Seguridad para ti

Detonantes emocionales - Cómo te engañan los ciberatacantes

Resumen

Los ciberatacantes están constantemente innovando sus formas de engañarnos para que hagamos cosas que no debemos hacer, como hacer clic en enlaces maliciosos, abrir archivos adjuntos en correos electrónicos infectados, comprar tarjetas de regalo o dar nuestras contraseñas. Además, suelen utilizar distintas tecnologías o plataformas para intentar engañarnos, como correos electrónicos, llamadas telefónicas, mensajes de texto o redes sociales. Si bien todo esto puede parecer abrumador, la mayoría de estos ataques comparten lo mismo: emociones. Al conocer los detonantes emocionales que utilizan los atacantes cibernéticos, frecuentemente puedes detectar sus ataques sin importar el método que estén utilizando.

Todo se trata sobre las emociones

Todo comienza con las emociones. Nosotros como humanos tomamos decisiones con demasiada frecuencia basadas en emociones en lugar de datos. De hecho, existe todo un campo de estudio sobre este concepto llamado “economía del comportamiento”, liderado por investigadores como Daniel Khaneman, Richard Thaler y Cass Sunstein. Afortunadamente para nosotros, si conocemos los detonantes emocionales que debemos buscar, podemos detectar y detener con éxito la mayoría de los ataques. A continuación, se enlistan los detonantes emocionales más comunes que debemos observar. A veces, los ciberatacantes usarán una combinación de estas diferentes emociones en el mismo correo electrónico, mensaje de texto, publicación en redes sociales o llamada, lo que lo hace mucho más efectivo.

Urgencia: La urgencia es uno de los detonantes emocionales más comunes, ya que es muy eficaz. Los atacantes cibernéticos a menudo usarán el miedo, la ansiedad, la escasez o la intimidación para obligarte a cometer un error. Tomemos, por ejemplo, un correo electrónico urgente de tu jefe exigiendo que se le envíen documentos confidenciales de inmediato, cuando en realidad es un ciberatacante que se hace pasar por él. O tal vez recibes un mensaje de texto de un atacante cibernético que se hace pasar por el gobierno informándote que el pago de tus impuestos está atrasado y que tienes que pagar en este momento o ir a la cárcel.

Enojo: Recibes un mensaje sobre un tema político, ambiental o social que te apasiona, algo así como "¡No creerás lo que está haciendo este grupo político o empresa!"

Sorpresa / Curiosidad: A veces los ataques que tienen más éxito dicen lo mínimo. La curiosidad se evoca con la sorpresa; queremos saber más. Es una respuesta a algo inesperado. Por ejemplo, un ciberatacante te envía un mensaje sobre un paquete que no te fue entregado para que hagas clic en un enlace y obtener más información, aunque no hayas pedido nada en línea. ¡Estamos tentados a saber más! Desafortunadamente, no hay ningún paquete, solo malas intenciones del otro lado de ese enlace.

Confianza: Los atacantes usan un nombre o una marca en la que confías para convencerte y que hagas algo. Por ejemplo, un mensaje que pretende ser de tu banco, una organización benéfica conocida, una entidad gubernamental de confianza o incluso una persona que conozcas. Solo porque un correo electrónico o mensaje de texto contenga el nombre de una organización que conoces y su logotipo no significa que el mensaje realmente provenga de ellos.

Emoción: Recibes un mensaje de texto de tu banco o proveedor de servicios agradeciéndote por realizar tus pagos a tiempo. Luego, el mensaje de texto proporciona un enlace donde puedes reclamar una recompensa. Un nuevo iPad, ¡qué emocionante! El enlace te lleva a un sitio web que parece oficial, pero te solicita toda tu información personal o dice que debes proporcionar la información de tu tarjeta de crédito para cubrir los pequeños costos de envío/manejo. Se trata de un ciberatacante que simplemente está robando tu dinero o tu identidad.

Empatía / Compasión: Los atacantes cibernéticos se aprovechan de tu buena voluntad. Por ejemplo, después de que un desastre aparece en las noticias, enviarán millones de correos electrónicos falsos donde pretenden ser una organización benéfica que atiende a las víctimas y pidiéndote dinero.

Al comprender mejor estos detonantes emocionales, estarás mucho mejor preparado para detectar y detener a los ciberatacantes, independientemente del engaño, la tecnología o la plataforma que utilicen.

Editor invitado

My-Ngoc Nguyen es CEO de Secured IT Solutions. Con 20 años de experiencia, tiene una amplia experiencia en la gestión y desarrollo de programas de gestión de riesgos y seguridad cibernética tanto para el gobierno federal como para el sector privado. Ella comparte su experiencia como instructora certificada enseñando regularmente MGT512 https://www.linkedin.com/in/menop, My-Ngoc Nguyen | Instituto SANS @MenopN

Recursos

Ingeniería social: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Ataques a través de llamadas telefónicas: https://www.sans.org/newsletters/ouch/vishing/
Estafas en redes sociales: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Smishing- Ataques a través de mensajería instantánea: https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
Ataques de phishing: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

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