SANS SECURITY AWARENESS

OUCH!

Boletín mensual de seguridad para todos

Evita el phishing

Resumen

Los servicios de mensajería y correo electrónico (como Skype, Twitter o Snapchat) son algunos de los principales medios de comunicación que utilizamos. No solo usamos estas tecnologías cada día para trabajar, sino también para mantenernos en contacto con amigos y familiares. Dado que muchas personas alrededor del mundo dependen de estas tecnologías, se han convertido en uno de los principales métodos de ataque usado por cibercriminales, un método de ataque llamado phishing. Aprende qué es el phishing y cómo puedes identificarlo para detener esta amenaza, sin importar si estás en el trabajo o en casa.

¿Qué es el phishing?

El phishing es un tipo de ataque que aprovecha el correo electrónico o los servicios de mensajería para engañarte con la intención de que realices alguna acción que no deberías hacer, como hacer clic en un vínculo malicioso, compartir tu contraseña o abrir un archivo adjunto malicioso en algún correo. Los atacantes se empeñan en hacer que estos mensajes parezcan convincentes y activar tu lado emocional, como el sentimiento de apremio o tu curiosidad. Pueden lograr que parezca que el mensaje provino de alguien conocido, como un amigo o una compañía de confianza que usas a menudo. Quizás añadan logos de tu banco o falsifiquen la dirección de correo para que el mensaje parezca legítimo. Los atacantes envían estos mensajes a millones de personas. No saben quién morderá el anzuelo, lo único que saben es que entre más envíen, más gente caerá víctima.

Protégete

En casi todos los casos, abrir y leer un correo electrónico o mensaje no es un peligro. Para que un ataque de phishing funcione, los actores maliciosos necesitan engañarte para hacer algo. Afortunadamente hay pistas de que un mensaje es un ataque, aquí se enlistan los más comunes:

- El correo tiene un sentido de urgencia, exige “acción inmediata” antes de que algo malo suceda, como la amenaza de que tu cuenta será cerrada o que serás enviado a prisión. El atacante quiere que te apresures para que cometas un error.
- Presionan para que pases por alto las políticas o procedimientos en el trabajo.
- Explotan un fuerte sentido de curiosidad o el mensaje es muy bueno para ser cierto (no, no ganaste la lotería).
- Contienen un saludo genérico, como “Estimado cliente”. La mayoría de las compañías o amigos que te contactan saben tu nombre.

- Requieren información muy sensible, como tu número de tarjeta de crédito o tu contraseña o cualquier otra información que el remitente legítimo debe saber.
- El mensaje dice que proviene de una organización oficial, pero tiene una gramática u ortografía pobre o usa una dirección de correo personal como @gmail.com.
- El mensaje viene de un correo oficial (como el de tu jefe), pero tiene una dirección para contestar que se dirige a otra cuenta personal de correo electrónico.
- Recibiste un mensaje de alguien que conoces, pero el tono o las expresiones no suenan a él o ella. Si sospechas, llama al remitente para verificar que lo ha enviado. Es fácil para un ciberatacante crear un mensaje que parece venir de un amigo o compañero de trabajo.

Al final, el sentido común es tu mejor defensa. Si un correo o mensaje parece extraño, sospechoso o demasiado bueno para ser verdad, puede tratarse de un ataque de phishing.

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

Tonia Dudley ha desarrollado y dirigido programas de concientización de seguridad desde 2011, incluyendo un programa galardonado de entrenamiento para detectar phishing. Puedes encontrarla en www.linkedin.com/in/toniadudley.

Recursos

Ingeniería social: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_sp.pdf
Ayuda a otros a asegurarse: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201710_sp.pdf
Qué hacer y qué no hacer con tu correo electrónico:
https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201609_sp.pdf
Estafa del CEO: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201607_sp.pdf
Boletín OUCH!: https://www.sans.org/u/Cbq

Licencia