SANS SECURITY AWARENESS

OUCH!

Boletín mensual de seguridad para todos

Fraude del CEO

¿Qué es el fraude del CEO o BEC?

Los ciberdelincuentes continúan mejorando el ataque de correo electrónico llamado “el fraude del CEO”, o Compromiso de Correo Electrónico Empresarial (Business Email Compromise o BEC, por sus siglas en inglés). Estos son ataques vía correo electrónico dirigidos que engañan a sus víctimas para que realicen una acción que no deberían ejecutar. En la mayoría de los casos, los atacantes buscan dinero. Lo que hace que estos ataques sean tan peligrosos es que los ciberdelincuentes investigan a sus víctimas antes de realizar su cometido. También, es muy difícil para las tecnologías de seguridad detener estos ataques porque no hay archivos adjuntos de correo electrónico infectados ni enlaces maliciosos que se puedan detectar. Así es como funciona.

El atacante cibernético utiliza Internet para investigar a la víctima y las personas con las que interactúa. Por ejemplo, si ellos te atacan, investigarían quién es tu jefe en el trabajo o quizás quién es el agente de bienes raíces con el que estés trabajando desde tu casa. Después, el atacante escribe un correo electrónico, haciéndose pasar por una de estas personas y te lo envía. El correo electrónico tiene un tono urgente y requiere que realices una acción de inmediato, como procesar una factura, cambiar a quién se le hace un pago o convencerte de responder con documentos confidenciales. El correo electrónico pretende presionarte para que hagas lo que los atacantes quieren. Aquí hay dos ejemplos de cómo podría funcionar un ataque:

Transferencia bancaria: un ciberdelincuente busca dinero. Investiga la empresa en la que trabajas, por ejemplo, identifica quién es el responsable de realizar depósitos o cualquier persona responsable de transferir fondos. Después, los delincuentes crean y envían un correo electrónico a estas personas pretendiendo ser su jefe o un alto ejecutivo. El correo electrónico les dice que hay una emergencia y el dinero debe ser transferido de inmediato a una nueva cuenta bancaria. El correo electrónico los presiona para cometer un error y en realidad están enviando dinero al ciberdelincuente.

Fraude fiscal: los delincuentes están utilizando la información personal de las personas para utilizarla en fraudes fiscales. Una de las formas más rápidas de obtenerlo es robar la información de los empleados de una empresa. Los delincuentes cibernéticos investigan e identifican quién trabaja en Recursos Humanos. Después envían correos electrónicos falsos a estas personas, pretendiendo ser un alto ejecutivo o quizás alguien del área legal. Los correos electrónicos crean una historia de urgencia, para que la información fiscal de todos los empleados deba enviarse de inmediato. El personal de Recursos Humanos piensa que está enviando los documentos confidenciales a la alta dirección, cuando en realidad los están enviando a un delincuente cibernético.

Protégete

Entonces, ¿qué puedes hacer para protegerte? El sentido común es tu mejor defensa. Estas son las pistas más comunes para buscar.

- El correo electrónico es muy corto y urgente (a menudo solo un par de oraciones) y la firma dice que el correo electrónico se envió desde un dispositivo móvil.
- Hay un fuerte sentido de urgencia, presionándote para ignorar o pasar por alto las políticas de tu empleador. Siempre sigue las políticas y procedimientos relacionados con el trabajo, incluso si el correo electrónico parece provenir de tu jefe o incluso del director ejecutivo (Chief Executive Officer o CEO por sus siglas en inglés).
- El correo electrónico está relacionado con el trabajo, pero usa una dirección de correo electrónico personal, como @gmail.com o @hotmail.com.
- Parece que el correo electrónico proviene de un alto directivo, compañero de trabajo o proveedor que conoces o con quien trabajas, pero el tono del mensaje no se parece al de ellos.
- Se proporcionan instrucciones de pago y estas difieren de las que ya recibiste, como solicitar el pago inmediato a una cuenta bancaria diferente.

Si sospechas que has sido objetivo de los ciberdelincuentes en el trabajo, detén toda interacción con el atacante y repórtalo a tu supervisor. Si has sido atacado en tu casa o si has sido víctima y realizaste una transferencia bancaria, repórtalo inmediatamente a tu banco y luego a la policía.

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

Donald Cavender *es un exagente especial del FBI con más de 22 años en el análisis forense digital y el delito cibernético. Recientemente se enfocó en las organizaciones de delitos informáticos como coordinador del BEC en Washington DC. Cavender imparte capacitación, realiza investigaciones cibernéticas y en análisis forense digital.* @don_cavender
https://www.linkedin.com/in/donald-cavender

Recursos

Ingeniería social:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_sp.pdf
Detener el phishing:	https://www.sans.org/sites/default/files/2018-04/201804-OUCH-April-Spanish.pdf
Detener el malware:	https://www.sans.org/sites/default/files/2018-06/201806-OUCH-June-Spanish.pdf
Bloquea tu sesión:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201712_sp.pdf