VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Julio 2016

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- ¿Qué es la estafa del CEO?
- ¿Cómo protegerte?

Estafa del CEO

¿Qué es la estafa del CEO?

Los ciberatacantes son sigilosos y están constantemente desarrollando nuevas formas de conseguir lo que quieren. Uno de sus métodos más eficaces es elegir a gente como tú. Ellos han aprendido que las personas desprevenidas son el eslabón más débil en cualquier organización, pero se han olvidado que la gente bien informada como los lectores del boletín OUCH! pueden ser la mejor defensa de una organización.

Editor Invitado

Angela Pappas es directora de formación y concienciación en seguridad de la información en Thomson Reuters. Ella es responsable del programa de embajadores, e-Learning y la educación de los empleados sobre el phishing.

Los ciberdelincuentes han desarrollado un nuevo ataque llamado estafa del CEO, también conocido como correo electrónico empresarial comprometido (BEC, por sus siglas en inglés). En estos ataques, un criminal cibernético se hace pasar por un director ejecutivo u otro alto cargo de una organización y envían a su nombre un correo electrónico al personal tratando de engañarlos para que hagan algo que no deberían hacer. Este tipo de ataques son extremadamente eficaces ya que los delincuentes hacen su investigación. Ellos buscan la página web de la organización para obtener información, por ejemplo, dónde se encuentra, quiénes son sus ejecutivos y otras organizaciones con las que trabaja. Los cibercriminales aprenden todo lo que pueden acerca de los trabajadores en sitios como LinkedIn, Facebook o Twitter. Una vez que conocen la estructura de la organización, comienzan a investigar y a seleccionar empleados específicos. Ellos escogen a sus víctimas con base en sus objetivos: si los cibercriminales están en busca de dinero, puede que su blanco sea el personal del departamento de finanzas; si están buscando información fiscal, se dirigirán a recursos humanos; y si quieren tener acceso a los servidores de base de datos, podrían escoger a alguien en TI.

Una vez que determinan lo que quieren y cuál es su objetivo, comienzan a elaborar su ataque; es frecuente que utilicen el spear phishing. Phishing es cuando un atacante envía un correo electrónico a millones de personas con el objetivo de engañarlos para que hagan algo, por ejemplo, la apertura de un archivo adjunto infectado o visitar un sitio web malicioso. Spear phishing es similar al phishing, sin embargo, en lugar de enviar un correo genérico de forma masiva, envían un correo electrónico personalizado dirigido a un muy pequeño y selecto número de personas. Los correos de spear phishing son extremadamente realistas a la vista y difícil de detectar; a menudo parecen provenir de alguien que conoces o con quien

Estafa del CEO

trabajas, por ejemplo, un compañero de trabajo o incluso tu jefe. Los correos parecen auténticos ya que pueden usar la misma jerga que utilizan tus compañeros del trabajo, el logotipo de tu organización o incluso la firma oficial de un ejecutivo. Estos mensajes de correo electrónico a menudo crean una sensación de urgencia, exigiendo que tomes una acción inmediata y no lo comentes con nadie. El objetivo del ciberdelincuente es apresurarte a cometer un error. Estos son los tres escenarios comunes:

La estafa del CEO es un poderoso ataque que puede evadir la mayoría de las defensas de seguridad. Tú eres nuestra mejor forma de defensa.

- **Transferencia bancaria**: El atacante está tras el dinero. Esto significa que investigan y aprenden quién trabaja en cuentas de nómina o el equipo que se encarga de las finanzas de tu organización. Después, los criminales diseñan y envían un correo electrónico simulando ser el jefe; éste dice que hay una emergencia y que el dinero debe ser trasladado de inmediato a una cuenta determinada.

- **Fraude fiscal**: Los cibercriminales quieren robar información acerca de tus compañeros de trabajo para que puedan hacerse pasar por empleados y cometer fraude fiscal. Ellos investigan tu organización y determinan quién maneja la información de los empleados, por ejemplo, alguien en recursos humanos. A partir de ahí envían correos falsos haciéndose pasar por un alto ejecutivo o tal vez algún abogado, exigiendo que proporcionen ciertos documentos inmediatamente.

- **Suplantación fiscal**: No todos los ataques de estafa del CEO implican un correo electrónico; otros métodos pueden ser utilizados, como una llamada telefónica. En este escenario, los delincuentes comienzan enviando un correo en el cual fingen ser un líder de alto rango, notificando que un abogado llamará para tratar un asunto urgente. El criminal llamará haciéndose pasar por el abogado y creando una sensación de urgencia, ya que habla sobre asuntos confidenciales y plazos de tiempo. Este sentido de urgencia te engaña para que actúes de forma inmediata.

¿Cómo protegerte?

Entonces, ¿qué se puede hacer para protegerte a ti y a tu organización? El sentido común es tu mejor defensa. Si recibes un mensaje sospechoso o raro de tu jefe o un colega, puede ser un ataque. Las pistas pueden incluir una sensación de urgencia, una firma que no parece estar bien, un cierto tono que nunca esperarías, o el nombre usado en el correo

Estafa del CEO

electrónico puede ser diferente al de la persona que realmente te llama. Otro indicio es que el atacante está utilizando un número de teléfono o dirección de correo que nunca has visto antes, o tal vez está utilizando una dirección de correo muy similar pero no exactamente la misma que la de tu compañero de trabajo o jefe. En caso de tener dudas, llama a la persona a través de un número de teléfono de confianza o reúnanse en persona (no respondas a través de correo) y confirma el envío de este. Nunca evadas las políticas o procedimientos de seguridad. Tu organización puede tener políticas que definan los procedimientos adecuados para autorizar la transferencia de fondos o la divulgación de información confidencial. Las solicitudes que derivan de eludir esas políticas, independientemente de su aparente fuente, deben ser consideradas sospechosas y tendrán que ser verificadas antes de tomar cualquier acción. Si recibes una solicitud de este tipo y no estás seguro de qué hacer, ponte en contacto con tu supervisor, la mesa de ayuda o el equipo de seguridad de la información de forma inmediata.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: securingthehuman.sans.org/ouch/archives

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

Recursos

Correo Electrónico Empresarial Comprometido:
http://blog.la.trendmicro.com/seguridad-basica-esquemas-del-correo-electronico-empresarial-comprometido/#.V1teqtThCt8

FBI advierte sobre estafa del CEO: http://www.seguridad.unam.mx/noticia/?noti=2915

Ingeniería Social: http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

Spear phishing: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201307_sp.pdf

Evitando ataques de ingeniería social y de phishing: http://www.seguridad.unam.mx/documento/?id=36

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traducción: Xocoyotzin Carlos Zamora, Katia Rodríguez, Raúl González

