Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

Phishing por correo electrónico

EDITOR INVITADO

El editor invitado para esta publicación es Pieter Danhieux. Él trabaja para BAE Systems Detica en Australia (www.baesystemsdetica.com.au) y es instructor de los cursos de pruebas de penetración en el instituto SANS.

RESUMEN

El correo electrónico es uno de los principales medios en donde podemos comunicarnos. No solo lo usamos todos los días para trabajar, sino también para estar en contacto con nuestros amigos y familiares. Además, el correo electrónico es el medio por el cual las compañías ofrecen muchos productos o servicios, como la confirmación de una compra en línea o la disponibilidad de tus estados de cuenta. Desde que mucha gente alrededor del mundo depende del uso del correo electrónico, los ataques a este servicio se han convertido en uno de los principales métodos utilizados por los delincuentes cibernéticos. En este boletín explicamos los ataques a correo electrónico más comunes y los pasos que puedes seguir para protegerte.

ATAQUES PHISHING

Phishing es un término utilizado originalmente para describir ataques de correo electrónico diseñados para robar tu nombre de usuario y contraseña de algún servicio bancario. Sin embargo, el término ha evolucionado y ahora se refiere a casi cualquier ataque basado en correo electrónico. El phishing utiliza ingeniería social, una técnica en la que los atacantes cibernéticos tratan de engañarte para que realices alguna acción. A menudo, estos ataques comienzan con un criminal cibernético que envía un correo electrónico pretendiendo ser alguien o algo que conoces o en lo que confías, como un amigo, tu banco o tu tienda en línea favorita. Estos mensajes de correo electrónico te motivan a realizar alguna acción, como hacer clic en un enlace, abrir un archivo adjunto o responder a un mensaje. Los criminales cibernéticos crean estos mensajes de correo electrónico a modo de parecer convincentes, enviándolos, literalmente, a millones de personas alrededor de todo el mundo. Los delincuentes no tienen un objetivo específico en mente, ni saben exactamente quién caerá víctima de su engaño. Solamente saben que entre más correos envíen, existe la posibilidad de que más personas pueden ser engañadas. Los ataques phishing funcionan de 4 formas.

- **Recolección de información:** El objetivo del atacante cibernético es engañarte para hacer clic en un enlace que te llevará a una página web que pide tu nombre de usuario y contraseña o, tal vez, tu número de tarjeta de crédito o tu PIN para usar el cajero automático. Estos

Phishing por correo electrónico

sitios web tienen el mismo aspecto que los sitios legítimos, poseen las mismas imágenes y dan la sensación de ser páginas de bancos o tiendas, pero son sitios falsos diseñados por el criminal para robar tu información.

- **Infectar tu computadora con enlaces maliciosos:** Una vez más, el objetivo del atacante es que tú hagas clic en un enlace. Sin embargo, en lugar de recolectar tu información, su objetivo es infectar tu computadora. Si haces clic en el enlace, te redirige a un sitio web que de forma silenciosa lanza un ataque contra tu equipo y, si tiene éxito, infectará tu sistema.

- **Infectar tu computadora con archivos adjuntos maliciosos**: Estos son correos electrónicos phishing que contienen archivos adjuntos maliciosos, tales como archivos PDF o documentos de Microsoft Office infectados. Si los abres atacarán tu computadora y si tienen éxito, le darán al atacante control total sobre tu equipo.

- **Estafas:** Son intentos hechos por delincuentes para estafarte. Ejemplos clásicos incluyen: noticias como que has ganado la lotería, solicitudes de donaciones de caridad después de un desastre reciente o un dignatario que necesita transferir millones de dólares a tu país y está dispuesto a pagarte por ayudarle con la transferencia. No te dejes engañar, estas son estafas creadas por criminales que están detrás de tu dinero.

PROTÉGETE

En la mayoría de los casos, solo abrir un correo electrónico es seguro. Para que la mayor parte de los ataques funcionen, tienes que hacer algo después de leer el correo (por ejemplo, abrir el archivo adjunto, dar clic en un enlace o responder la solicitud de información). Aquí te presentamos algunos tips para reconocer un ataque por correo electrónico.

Usa el sentido común, si un correo electrónico te parece extraño o demasiado bueno para ser verdad, muy probablemente se trata de un ataque.

- Sospecha de cualquier correo que requiera de “acción inmediata” o cree un sentido de urgencia. Esta es una técnica común usada por los criminales para apresurar a la gente a cometer un error.
- Sospecha de correos electrónicos dirigidos a “Estimado cliente” o algún otro saludo genérico. Si es tu banco, seguramente sabrá tu nombre.
- Sospecha de errores gramaticales o de ortografía, la mayoría de los negocios corrigen sus mensajes cuidadosamente antes de enviarlos.
- No des clics en los enlaces. En lugar de eso, copia la

Phishing por correo electrónico

URL del correo y pégala en tu navegador web. Aún mejor, puedes escribir el nombre del destino en tu navegador.

- Sitúa el ratón sobre el enlace. Esto te mostrará el verdadero destino al que irías si realmente hicieras clic en él. Si la dirección destino del enlace es diferente a la que se muestra en el correo, puede ser un claro indicador de fraude.
- Sospecha de los documentos adjuntos y abre solo aquellos que estés esperando.
- El hecho de recibir un correo electrónico de un amigo no quiere decir que realmente fue él quien lo envió. La computadora de tu amigo podría estar infectada o su cuenta de correo electrónico probablemente comprometida y el malware está enviando ese correo a todos los contactos de tu amigo. Si recibes un correo sospechoso de una fuente confiable o un amigo, háblales para confirmar que efectivamente ellos lo enviaron. Siempre usa un número telefónico que conozcas o puedas verificar de forma independiente, no uno incluido en el cuerpo del correo.

Si después de leer un correo te parece que se trata de un ataque phishing o una estafa, elimínalo. Realmente, utilizar el correo electrónico de forma segura es solo cuestión de sentido común. Si algo parece sospechoso o demasiado bueno para ser verdad, lo más probable es que se trate de un ataque o de una estafa. Simplemente borra el correo electrónico.

RECURSOS

Algunos de los enlaces mostrados a continuación se redujeron para mejorar la legibilidad a través del servicio TinyURL. Con el fin de mitigar problemas de seguridad, OUCH! siempre utiliza la característica de vista previa de TinyURL (preview), la cual muestra el enlace destino, solicitando tu permiso antes de abrirlo.

Manual para identificar y notificar correo fraudulento:
http://preview.tinyurl.com/ago98mz

Alerta en línea
http://preview.tinyurl.com/bb333zq

Términos comunes de seguridad:
http://preview.tinyurl.com/6wkpae5

Consejo del día SSI UNAM-CERT:
http://preview.tinyurl.com/8fpbhtw

MÁS INFORMACIÓN

Suscríbete al boletín mensual OUCH!, el boletín de consejos sobre seguridad. Accede a los archivos de OUCH! y aprende más acerca de las soluciones preventivas de seguridad que SANS tiene para ti.
Visítanos en http://www.securingthehuman.org

VERSIÓN EN ESPAÑOL

UNAM-CERT, Equipo de Respuesta a Incidentes en México reconocido ante FIRST, es una referencia en seguridad de la información en este país.

Sitio web http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Versión en español a cargo de UNAM-CERT: Sandra Atonal, Carlos Colio, Célica Martínez, Jazmín López, Andrea Méndez, Gustavo Villafán