

OUCH!

EN ESTA EDICIÓN

- Phishing
- Scams
- ¿Cómo protegerse?

Phishing y Scams en el Correo Electrónico

EDITOR INVITADO

Pieter Danhieux es el editor invitado para esta edición. Trabaja para BAE Systems stratsec en Australia (www.stratsec.net), y es instructor de cursos de pruebas de penetración en el SANS Institute.

RESUMEN

El correo electrónico es una de las principales formas de comunicación. No sólo lo utilizamos todos los días en el trabajo, sino también para mantenernos en contacto con amigos y familiares. Además, el correo electrónico es la forma en que las compañías proveen muchos de sus productos o servicios; por ejemplo, confirmaciones de compras en línea o actualizaciones para nuestras cuentas bancarias. Por ello, muchas personas alrededor del mundo dependen del correo electrónico, esto lo convierte en uno de los principales métodos que los cibercriminales utilizan para realizar ataques. En esta entrega explicamos los peligros y pasos que puedes seguir para protegerte.

PHISHING

El phishing es uno de los ataques más comunes presentes en el correo electrónico. Utiliza ingeniería social, una técnica en la que los ciberatacantes intentan engañarte para que realices alguna acción determinada. El phishing es un término originalmente utilizado para describir un ataque diseñado para robar información de tus credenciales de banca en línea. Sin embargo, el término ha

evolucionado, y ahora se refiere a casi cualquier ciberataque enviado por correo electrónico.

Un ataque de phishing comienza con un correo electrónico que pretende proceder de alguna persona u organización que conoces y en quien confías, como tu banco o tienda favorita en línea. Estos correos electrónicos tratan de convencerte para realizar una acción, como dar clic sobre un enlace, abrir un archivo adjunto, o responder a un mensaje. Los cibercriminales elaboran estos correos electrónicos de manera convincente, después los envían a miles, si no es que a millones de personas alrededor del mundo. Los criminales no tienen un objetivo específico en mente, ni saben exactamente quienes serán las víctimas. Simplemente, saben que entre más correos electrónicos envíen, más gente podrá ser engañada. Comúnmente, los ataques de phishing tienen uno de los siguientes objetivos:

- **Recolección de información:** El objetivo de estos atacantes es convencerte de dar clic en un enlace y llevarte a un sitio web que solicite tu usuario y contraseña, o quizás tu color favorito o el nombre de soltera de tu mamá. Estos sitios web pueden parecer legítimos y tener exactamente el mismo aspecto de tu banca en línea, pero están diseñados para robar información que podría darles acceso a tu cuenta.
- **Control de tu computadora a través de enlaces maliciosos:** Una vez más, el objetivo de los ciberatacantes es que des clic en un enlace. Sin

Phishing y Scams en el Correo Electrónico

embargo, en lugar de obtener tu información, su objetivo es infectar tu computadora. Si das clic en el enlace, serás dirigido a un sitio web que, de manera silenciosa, lanza un ataque contra tu navegador y, si es exitoso, obtendrán el control completo de tu equipo.

- **Control de tu computadora a través de adjuntos maliciosos:** Estos correos electrónicos de phishing vienen acompañados de archivos adjuntos infectados, como archivos PDF o documentos de Microsoft Office (Word, Excel o PowerPoint). Si abres estos adjuntos pueden atacar tu computadora, y si resulta exitoso, dar al atacante control sobre tu equipo.

SCAM

El scam (estafa) no es nada nuevo, son intentos fraudulentos realizados por los criminales. Algunos ejemplos clásicos incluyen avisos que te indican que has ganado la lotería (cuando ni siquiera has participado), o que alguien necesita transferir millones de dólares a tu país y le gustaría pagarte para que lo ayudes con la transferencia. Entonces, te dirán que tienes que pagar primero una tarifa de procesamiento antes de poder obtener tu dinero. Después de pagar estos honorarios, los criminales desaparecen y nunca más vuelves a saber de ellos.

¿CÓMO PROTEGERSE?

En la mayoría de los casos, abrir un correo electrónico es seguro. Para que la mayoría de los ataques funcionen, tienes que hacer algo después de leer el correo electrónico (por ejemplo, abrir un archivo adjunto, hacer clic en un enlace, o responder a una solicitud para obtener información). Si después de leer un correo electrónico piensas que es un ataque o una estafa, simplemente elimínalo.



Usa el sentido común, si un correo electrónico parece extraño o demasiado bueno para ser verdad lo más probable es que se trate de un ataque.

A continuación, te presentamos algunos puntos que podrían indicar si un correo electrónico es en realidad un ataque.

- Sospecha de cualquier correo electrónico que requiera “una acción inmediata” o que cree una sensación de urgencia. Este es un método muy común que se utiliza para engañar a la gente.
- Sospecha de direcciones de correo que digan “Estimado Cliente” o algún otro saludo genérico.
- Sospecha de errores gramaticales u ortográficos. La mayoría de las empresas deben revisar sus mensajes con mucho cuidado.
- Si el enlace en un correo electrónico es sospechoso, pasa el ratón sobre el enlace. Esto te mostrará el destino al que te llevará si haces clic.

Phishing y Scams en el Correo Electrónico

El enlace que está escrito en el correo electrónico probablemente puede ser muy diferente al lugar donde realmente te enviará.

- No des clic en enlaces. Lo recomendable es copiar la URL del correo electrónico y pegarlo en el navegador. Aun mejor, es escribir el nombre en el navegador. Por ejemplo, si tienes un correo electrónico de UPS diciéndote que tu paquete está listo para ser entregado, no debes de hacer clic en el enlace. En lugar de eso, dirígete al sitio web de UPS, y copia y pega el número de seguimiento.
- Sospecha de archivos adjuntos. Solo se deben abrir archivos adjuntos que estés esperando.
- Si recibiste un correo electrónico de tus amigos, esto no significa que precisamente ellos lo enviaron. Las computadoras de tus amigos podrían estar infectadas, o sus cuentas probablemente comprometidas, en cuyo caso un código malicioso estaría enviando correos electrónicos a todos sus contactos. Si recibes correo electrónico sospechoso de la cuenta de un amigo o un colega confiable, comunícate o confirma con ellos la veracidad del envío.

Finalmente, el uso seguro del correo electrónico se reduce al sentido común. Si algo te parece sospechoso o muy bueno para ser verdad, lo más probable es que se trate de un ataque. Lo que debes hacer es simplemente eliminar ese correo electrónico.

RECURSOS

Algunos de los enlaces mostrados a continuación, se redujeron para mejorar la legibilidad a través del servicio de

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 permiso antes de abrirlo.

Usuario Casero UNAM/CERT - Phishing Scam:

<http://preview.tinyurl.com/7a9brgw>

Alerta en línea – Evite estafas:

<http://preview.tinyurl.com/82wdbgu>

Anti-Phishing Working Group:

<http://preview.tinyurl.com/7qoqfew>

OSI – Fraude e Ingeniería Social:

<http://preview.tinyurl.com/6v27dz3>

Clic Seguro ¿Qué es? Diccionario de Términos:

<http://preview.tinyurl.com/89z2r79>

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](https://twitter.com/unamcert).

OUCH! es publicado bajo el programa Securing The Human de SANS y es distribuido bajo la licencia [Creative Commons BY-NC-ND 3.0](https://creativecommons.org/licenses/by-nc-nd/3.0/). Se concede el permiso para distribuir este boletín siempre y cuando se referencie la fuente, la distribución no sea modificada ni usada con fines comerciales. Para traducción o más información, por favor contacte a: ouch@securingthehuman.org.

Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy
Versión en español a cargo de UNAM-CERT: Mayra Villeda, Francisco Martínez, Galvy Cruz, Iván Alvarado