BANK OF AMERICA

CIBERSEGURIDAD

Mantenga la ciberseguridad: phishing

Consejos para protegerse y cómo responder si cree que ha sido atacado.

Phishing es una técnica utilizada por los ciberdelincuentes con la intención de engañarle para que revele información confidencial o sensible de la compañía. El phishing se lleva a cabo a través de distintos canales: correo electrónico, mensajes de texto, llamadas telefónicas y redes sociales. En un intento de phishing, los ciberdelincuentes con frecuencia crearán un sentido de urgencia para engañarle y lograr que usted haga clic en un enlace o abra un archivo adjunto que invadirá sus dispositivos y/o correo electrónico para robar contraseñas e información de cuentas bancarias.

Cómo protegerse

Sea proactivo:

- **Tenga cuidado** al publicar información que le identifique en redes sociales. Cumpla con las políticas de su compañía sobre redes sociales.
- **Descargue las actualizaciones de las aplicaciones.** El software no actualizado puede exponerle a amenazas.
- **Invierta en software antivirus** y otro software de ciberseguridad capaz de detectar correos electrónicos y sitios sospechosos.
- **Verifique dos veces la información del remitente.** Revise el nombre del dominio del remitente para asegurarse de que no esté falsificando la dirección de correo electrónico.
- **Nunca confíe** en personas desconocidas. Verifique todo lo que afirman y no envíe información sensible a personas cuya identidad no pueda verificar.

Si sospecha que ha sido atacado:

- **No titubee.** Una respuesta rápida después de un suceso puede minimizar los daños para usted o su compañía.
- **Comuníquese en cuanto pueda con el centro de atención o con el personal de apoyo de su banco** para denunciar una transacción fraudulenta.
- **Conozca y siga las leyes locales** y los lineamientos para incidentes cibernéticos.
- **Denuncie la amenaza** a la plataforma donde ocurrió.
- **Documente todo** lo relacionado con el suceso. Cuanta más información tenga, mejor preparado estará para asistir en una investigación realizada por su compañía, el banco y los oficiales de cumplimiento de la ley, y también estará mejor preparado para protegerse contra futuros ataques de ciberdelincuentes.

Una amenaza creciente, en cifras

241,342

Número de incidentes informados en la categoría de phishing[1].

814%

Incremento porcentual en los incidentes informados en la categoría de phishing de 2018 a 2020[1].

$54.2 millones de dólares

Pérdidas estimadas en 2020 por incidentes en la categoría de phishing[1].

[1] FBI IC3 Report, 2020

Mantenga la ciberseguridad: phishing

Por qué es importante

Phishing es una amenaza común de ingeniería social, en la que se envían mensajes aparentemente legítimos por correo electrónico o plataformas de mensajes.

- **Vishing** es la versión telefónica de phishing, y **smishing** es la versión mediante mensajes SMS o aplicaciones de mensajes.
- **Phishing focalizado (spear phishing)**: una campaña de phishing altamente focalizada, diseñada para personas específicas.
- **Spoofing**: disfraza las comunicaciones para que parezcan provenir de alguien más, incluso de compañías o empleados legítimos. Los ciberdelincuentes pueden falsificar correos electrónicos, números de teléfono y sitios web.
- Recuerde que Bank of America, como muchas compañías, nunca le pedirá detalles de una cuenta o de CashPro®, salvo que usted nos llame primero.

Los ciberdelincuentes intentarán provocar en usted una fuerte reacción emocional para que omita los procesos y haga clic o les envíe elementos que no debería. La ingeniería social depende de la avaricia, la curiosidad, la urgencia, el afán de ayudar y el temor. Algunas maneras en las que podrían intentar el phishing son:

1. **Se comunican con usted** a través de cuentas fraudulentas, falsas o vulneradas de correo electrónico o de aplicaciones de mensajes.
2. **Le alientan a hacer clic** en un enlace que descarga software malicioso (malware) en su computadora y les da a los delincuentes acceso a su dispositivo y a la información que contiene.
3. **Presentan un pretexto urgente** por el cual debe enviar información confidencial o financiera.

Seguridad de la Información Gobal en Bank of America

El equipo de Seguridad de la Información Global (Global Information Security, o GIS) está formado por profesionales de seguridad de la información en varios centros de operaciones de seguridad en todo el mundo, quienes trabajan las 24 horas del día, los 7 días de la semana para mantener seguros los datos y la información.

Para obtener más información, visite: www.business.bofa.com/en-us/content/fraud-prevention-and-cyber-security-solutions.html