Esté ciberseguro: protéjase de las estafas de soporte técnico

El fraude de soporte técnico ocurre cuando un ciberdelincuente se hace pasar por un representante de servicio o soporte técnico para resolver problemas tecnológicos como virus, correo electrónico o cuenta bancaria comprometidos, o una renovación de licencia de software. Una vez que los ciberdelincuentes obtienen acceso remoto a dispositivos o cuentas, pueden exponer sus datos y finanzas a riesgo.

Con el acceso a su cuenta, los ciberdelincuentes pueden:

- **Crear una identidad falsa** con parte de su información y usarla para abrir una nueva tarjeta de crédito o solicitar un préstamo.
- **Transferir fondos** desde sus cuentas o cargar compras a ellas.
- **Robar su identidad** y reclamar su reembolso de impuestos o beneficios gubernamentales.
- **Enviar mensajes de "phishing" o suplantación de identidad** a sus contactos usando su cuenta de correo electrónico y convencerlos de que compartan información confidencial.

Sea proactivo:

- **Invierta en software antivirus** y otros programas de ciberseguridad capaces de reducir las ventanas emergentes y detectar correos electrónicos y sitios web sospechosos. Asegúrese de que todo software antivirus y de ciberseguridad se mantenga actualizado.
- **Nunca confíe en personas desconocidas.** Verifique todo lo que afirman y no envíe información sensible a personas cuya identidad no pueda verificar.
- **No responda ni haga clic en fuentes desconocidas,** ni haga clic en sus enlaces o archivos adjuntos. Las empresas legítimas de seguridad o soporte técnico no se comunicarán con usted a menos que usted lo solicite.
- **Si tiene dudas, espere.** Tómese el tiempo para investigar con quién está hablando. Las compañías legítimas le darán tiempo para que responda y haga preguntas.

Si sospecha que ha sido atacado:

- **No demore.** Una respuesta rápida después de haber sufrido un ataque puede minimizar los daños.
- **Llame a su banco,** congele las cuentas financieras que puedan haber sido afectadas e informe a las agencias de informes de crédito.
- **Cambie todas las contraseñas** que puedan haber sido vulneradas.
- **Llame a la policía** y presente denuncias ante las autoridades locales pertinentes.
- **Documente todo** lo relacionado con el suceso. Cuanta más información tenga, mejor preparado estará para asistir en una investigación y también estará mejor preparado para protegerse contra futuros ataques.

Los ciberdelincuentes pueden contactarle de las siguientes maneras:

- **Llamadas telefónicas no solicitadas** de un ciberdelincuente que se hace pasar por compañías de computadoras, bancos y servicios públicos.
- **La publicidad en motores de búsqueda** ocurre cuando una persona busca en línea para encontrar números de soporte telefónico. Los ciberdelincuentes pagan para tener un enlace fraudulento en la parte superior de la lista de búsqueda.
- **Mensaje emergente** que indica que se ha encontrado un virus en la computadora. La solicitud del mensaje le indica que llame a un número de teléfono que está vinculado con el ciberdelincuente.
- **Un correo electrónico** que afirma que tiene usted una suscripción de software que vence o un posible cargo fraudulento en su cuenta bancaria. Luego, se le recomendará que se comunique con el ciberdelincuente por teléfono.

INFORMACION IMPORTANTE

Ni Bank of America ni sus afiliadas proporcionan servicios de asesoría sobre seguridad de la información o tecnología de la información (information technology, o IT). Este material se proporciona "tal como está", sin garantía de integridad, exactitud, puntualidad o de los resultados obtenidos del uso de este material, y sin garantía de ninguna clase, expresa o implícita, incluyendo, sin limitación las garantías de desempeño, calidad y aptitud para un fin específico. Este material debe ser considerado como información general sobre seguridad de la información y consideraciones de IT y no tiene el propósito de proveer información específica de seguridad o asesoría sobre IT ni es un sustituto de sus propias investigaciones independientes. Si tiene preguntas con respecto a su sistema de IT en particular o problemas de seguridad de la información, por favor póngase en contacto con su asesor de IT o de seguridad de la información.

"Bank of America" y "BofA Securities" son los nombres de mercadeo utilizados por las divisiones de Banca Global y Mercados Globales de Bank of America Corporation. Los préstamos, otras actividades de banca comercial y la compraventa de ciertos instrumentos financieros son llevados a cabo de forma global por afiliadas bancarias de Bank of America Corporation, entre las que se incluye Bank of America, N.A., Miembro de FDIC. La compraventa de valores e instrumentos financieros, la asesoría estratégica y otras actividades de banca de inversión son llevadas a cabo de forma global por afiliadas de banca de inversión de Bank of America Corporation ("Afiliadas de Banca de Inversión") entre las que se incluyen, en los Estados Unidos, BofA Securities, Inc. y Merrill Lynch Professional Clearing Corp., ambos agentes corredores de bolsa registrados y miembros de SIPC y, en otras jurisdicciones, entidades registradas a nivel local. BofA Securities, Inc. y Merrill Lynch Professional Clearing Corp. están registradas como comisionistas de futuros ante la Comisión de Compraventa Futura de Productos Básicos (Commodity Futures Trading Commission, o CFTC) y son miembros de la Asociación Nacional de Futuros (National Futures Association, o NFA).

Los productos de inversión ofrecidos por las Afiliadas de Banca de Inversión:

No Están Asegurados por FDIC	No Tienen Garantía Bancaria	Pueden Perder Valor