Octubre 19, 2020

FEDERAL DEPOSIT INSURANCE CORPORATION

consumer **news**

¡Cuidado, es una estafa!

Evite el phishing, smishing, vishing, y otras estafas

Los delincuentes intentan constantemente robar los datos personales de los consumidores mediante correos electrónicos, sitios web, llamadas telefónicas e incluso mensajes de texto falsos. Utilizan una variedad de formas de intentar engañar a las personas para que proporcionen números de seguro social, números de cuentas bancarias y otra información valiosa. En muchos casos, su objetivo es robarte dinero. Este artículo define algunos términos utilizados para diferentes estafas en línea y cómo funcionan, para que pueda proteger su dinero.

¿Cómo se comunican los estafadores con sus víctimas?

Phishing es un término para las estafas que se usa comúnmente cuando un delincuente usa el correo electrónico para pedirle que proporcione información financiera personal. El remitente pretende ser de un banco, una tienda minorista o una agencia gubernamental y hace que el correo electrónico parezca legítimo. Los delincuentes a menudo intentan amenazar, incluso asustar a las personas diciendo "usted es víctima de un fraude" o algún otro mensaje que suene urgente para engañarlo y que proporcione información sin pensar. No lo hagas.

Smishing es similar al phishing, pero en lugar de usar el correo electrónico, el delincuente usa mensajes de texto para comunicarse contigo. Con la misma idea, fingen que pertenecen a una organización que quizás conozcas y en la que confíes (como un banco o el IRS) y tratan de obtener tu información personal.

Vishing, similar al phishing y smishing, es cuando los estafadores usan servicios telefónicos como una llamada telefónica en vivo, una "llamada automática" o un correo de voz para tratar de engañarlo para que proporcione información personal pareciendo un funcionario comercial o gubernamental legítimo.

¿Cuáles son los diferentes tipos de estafas?

Las estafas de impostores gubernamentales ocurren cuando los estafadores fingen ser empleados de la FDIC u otra agencia gubernamental, a veces incluso usando nombres de personas reales. La edición de marzo de 2020 de FDIC Consumer News tiene más información sobre cómo evitar ser estafado por impostores del gobierno.

Recuerde, la FDIC no envía correspondencia no solicitada solicitando dinero o información personal confidencial, y nunca lo amenazaremos. Además, ninguna agencia gubernamental le exigirá que pague con tarjeta de regalo, transferencia de dinero o moneda digital. La FDIC nunca se comunicaría con usted para pedirle detalles personales, como información de cuenta bancaria, números de tarjetas de crédito y débito, números de seguro social o contraseñas.

Loterías y estafas de riquezas repentinas son cuando le dicen que ganó una lotería, quizás en un país extranjero, o que tiene derecho a recibir una herencia. Se le dice que para "reclamar" las ganancias de la lotería o la herencia, debe pagar "impuestos y tarifas". Es posible que le envíen un cheque de caja falso, que el estafador le pide que lo cobre y luego le devuelva los fondos para cubrir los impuestos y las tarifas. Desaparecen con sus fondos y no obtiene nada, pero el delincuente se aprovecha de ellos cuando el cheque es encontrado fraudulento y su banco lo responsabiliza por la pérdida.

Las subastas en línea, los sitios de anuncios clasificados y las estafas de pago excesivo implican una subasta en línea o un sitio de anuncios clasificados. El estafador ofrece comprar un artículo en venta, pagar un servicio por adelantado o alquilar un apartamento. La pista de que se trata de una estafa es que le envían un cheque de caja por un monto superior al precio de venta. Cuando les comunique esto, se disculparán por el descuido y le pedirán que devuelva rápidamente los fondos adicionales. El motivo del estafador es hacer que usted cobre o deposite el cheque y envíe dinero legítimo antes de que usted o su banco se den cuenta de que el cheque que depositó es falso.

Las estafas del abuelo ocurren cuando un estafador hackea la cuenta de correo electrónico de alguien y envía correos electrónicos falsos a amigos y familiares, quizás alegando que el propietario real de la cuenta está varado en el extranjero y podría necesitar la información de su tarjeta de crédito para regresar a casa. Si recibe un correo electrónico de este tipo, asegúrese de comunicarse con el remitente por otros medios antes de enviar dinero o información personal.

Las estafas de empleo de compradores secretos o misteriosos implican anuncios falsos de oportunidades laborales que afirman estar "contratando" personas para trabajar desde casa. Como nuevo "empleado" potencial, es posible que reciba un cheque oficial como bonificación inicial y se le solicite que cubra el costo de la "activación de la cuenta". El estafador espera recibir estos fondos antes de que se acredite el cheque oficial y usted se dé cuenta de que ha sido estafado. Otro escenario implica una oferta para trabajar desde casa como comprador secreto para "evaluar la calidad" de las empresas locales de transferencia de dinero. Se le envía un cheque de caja y se le indica que lo deposite en su cuenta bancaria y retire la cantidad en efectivo. A continuación, se le indica que utilice una empresa de transferencia de dinero local para enviar los fondos al "empleador" y "evaluar" el servicio proporcionado por la empresa de transferencia de dinero.

Asegúrese de leer el artículo de *FDIC Consumer News* de Agosto 2019: Cuidado con los cheques falsos - PDF para obtener más información sobre las estafas que involucran cheques.

¿Cómo puedo evitar las estafas?

Sospeche si alguien se comunica con usted inesperadamente en línea y le pide su información personal. No importa qué tan legítimo pueda parecer el correo electrónico o el sitio web. Solo abra correos electrónicos, responda a mensajes de texto, correos de voz o personas que llaman que provengan de personas u organizaciones que conoce, e incluso entonces, tenga cuidado si parecen cuestionables.

Si cree que un correo electrónico, mensaje de texto o cuadro emergente puede ser legítimo, aún debe verificarlo antes de proporcionar información personal. Si desea verificar algo, comuníquese de forma independiente con la supuesta fuente (tal vez un banco u organización) utilizando una dirección de correo electrónico o un número de teléfono que sepa que es válido, como su sitio web o un extracto bancario.

Tenga especial cuidado con los correos electrónicos o sitios web que tengan errores tipográficos u otros errores obvios.

Recursos adicionales:

Comisión Federal de Comercio (FTC): *Cómo reconocer y denunciar mensajes de texto no deseados*, https://www.consumidor.ftc.gov/articulos/como-reconocer-y-reportar-los-mensajes-de-texto-spam

FTC: *Cómo reconocer y evitar las estafas de phishing*, https://www.consumidor.ftc.gov/articulos/como-reconocer-y-evitar-las-estafas-de-phishing

FTC: *Cómo detectar, evitar y denunciar estafas con cheques falsos*, https://www.consumidor.ftc.gov/articulos/como-detectar-evitar-y-reportar-las-estafas-de-cheques-falsos-0

Oficina de Protección Financiera del Consumidor (CFPB): *Estafas de impostores*, https://www.consumerfinance.gov/about-us/blog/warning-lottery-scam-using-cfpb-employees-name/

FTC: *las estafas del abuelo en la era del coronavirus*, https://www.consumidor.ftc.gov/blog/2020/04/las-estafas-del-abuelo-en-la-epoca-del-coronavirus

Para obtener más ayuda o información, vaya a **www.fdic.gov** o llame a la FDIC gratis al **1-877-ASK-FDIC (1-877-275-3342)**. Envíe sus ideas para historias o comentarios a Asuntos del Consumidor a **consumeraffairsmailbox@fdic.gov**

FDIC