October 19, 2020

FEDERAL DEPOSIT INSURANCE CORPORATION

consumer **news**

Beware, It's a Scam!

Avoid phishing, smishing, vishing, and other scams

Criminals are constantly trying to steal consumers' personal data using fake emails, websites, phone calls, and even text messages. They use a variety of ways to try to trick people into providing Social Security numbers, bank account numbers, and other valuable information. In many cases, their goal is to steal money from you. This article defines some terms used for different online scams and how they work, so you can protect your money.

How do scammers contact their victims?

Phishing is a term for scams commonly used when a criminal uses email to ask you to provide personal financial information. The sender pretends to be from a bank, a retail store, or government agency and makes the email appear legitimate. Criminals often try to threaten, even frighten people by stating "you're a victim of fraud" or some other urgent-sounding message to trick you into providing information without thinking. Don't do it.

Smishing is similar to phishing, but instead of using email, the criminal uses text messaging to reach you. Same idea, they pretend they are from an organization you might know and trust (such as a bank or the IRS) and try to get your personal information.

Vishing, similar to phishing and smishing, is when scammers use phone services such as a live phone call, a "robocall," or a voicemail to try to trick you into providing personal information by sounding like a legitimate business or government official.

What are the different types of scams?

Government Impostor Scams are when fraudsters pretend to be an employee of the FDIC or other government agency, sometimes even using the names of real people. The March 2020 FDIC Consumer News issue has more on how to avoid being scammed by government impostors.

Remember, the FDIC does not send unsolicited correspondence asking for money or sensitive personal information, and we'll never threaten you. Also, no government agency will ever demand that you pay by gift card, wiring money, or digital currency. The FDIC would never contact you asking for personal details, such as bank account information, credit and debit card numbers, social security numbers, or passwords.

Lotteries and Sudden Riches Scams are when you are told that you won a lottery, perhaps in a foreign country, or that you are entitled to receive an inheritance. You are told that in order to "claim" the lottery winnings or inheritance, you must pay "taxes and fees." A fake cashier's check might be sent to you, which the scammer asks you to cash and then wire back the funds to cover the taxes and fees.

They disappear with your funds and you get nothing but taken advantage of by the criminal when the check is found to be fraudulent and your bank holds you responsible for the loss.

Online Auctions, Classified Listing Sites, and Overpayment Scams involve an online auction or classified listing site. The scammer offers to buy an item for sale, pay for a service in advance, or rent an apartment. The clue that it is a scam is that they send you a cashier's check for an amount that is higher than your asking price. When you bring this to their attention, they will apologize for the oversight and ask you to quickly return the extra funds. The scammer's motive is to get you to cash or deposit the check and send back legitimate money before you or your bank realize that the check you deposited is fake.

Grandparent Scams happen when a fraudster hacks into someone's email account and sends out fake emails to friends and relatives, perhaps claiming that the real account owner is stranded abroad and might need your credit card information to return home. If you receive such an email, make sure you contact the sender through other means before sending any money or personal information.

Secret or Mystery Shopper Employment Scams involve fake advertisements for job opportunities that claim to be "hiring" people to work from home. As the potential new "employee," you might receive an official check as a starting bonus, and are asked to cover the cost of "account activation." The scammer hopes to receive these funds before the official check clears and you realize you have been scammed. Another scenario involves an offer to work from home as a secret shopper to "assess the quality" of local money transfer businesses. You are sent a cashier's check and instructed to deposit it into your bank account and withdraw the amount in cash. You are then instructed to use a local money transfer business to send the funds back to the "employer" and "evaluate" the service provided by the money transfer business.

Be sure to read the FDIC Consumer News on check fraud to learn more about scams involving checks. FDIC Consumer News: *Beware of Fake Checks*, https://www.fdic.gov/consumers/consumer/news/august2019.html

How can I avoid scams?

Be suspicious if someone contacts you unexpectedly online and asks for your personal information. It doesn't matter how legitimate the email or website may look. Only open emails, respond to text messages, voice mails, or callers that are from people or organizations you know, and even then, be cautious if they look questionable.

If you think an email, text message, or pop-up box might be legitimate, you should still verify it before providing personal information. If you want to check something out, independently contact the supposed source (perhaps a bank or organization) by using an email address or telephone number that you know is valid, such as from their website or a bank statement.

Be especially wary of emails or websites that have typos or other obvious mistakes.

Additional Resources:

FDIC Video #FDICExplains: *Phishing,* https://www.youtube.com/watch?v=titE2f8rhfs

Federal Trade Commission (FTC): *How to Recognize and Report Spam Text Messages*, https://www.consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages

FTC: *How to Recognize and Avoid Phishing Scams*, https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

FTC: *How to Spot, Avoid and Report Fake Check Scams*, https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-fake-check-scams

Consumer Financial Protection Bureau (CFPB): *Impostor Scams*, https://www.consumerfinance.gov/about-us/blog/warning-lottery-scam-using-cfpb-employees-name/

FTC: *Grandparent scams in the age of Coronavirus*, https://www.consumer.ftc.gov/blog/2020/04/grandparent-scams-age-coronavirus

For more help or information, go to **www.fdic.gov** or call the FDIC toll-free at **1-877-ASK-FDIC (1-877-275-3342)**. Please send your story ideas or comments to Consumer Affairs at **consumeraffairsmailbox@fdic.gov**

FDIC

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