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