FDIC

October 8, 2021

FEDERAL DEPOSIT INSURANCE CORPORATION
consumer news

Avoiding Scams and Scammers

Cybersecurity is key

When cybersecurity is inadequate, it can lead to stolen identity and financial loss. Most scams and scammers have two main goals—to steal your money and your identity. You should know what to look for, how they work, and what to do, so you can protect yourself and your finances.

Maintaining cybersecurity is very important, even for consumers. It is not simply something that concerns large corporations and other businesses. Here are some steps you can take:

- **Do not open email from people you don't know.** If you are unsure whether an email you received is legitimate, try contacting the sender directly via other means. Do not click on any links in an email unless you are sure it is safe.
- **Be careful with links and new website addresses.** Malicious website addresses may appear almost identical to legitimate sites. Scammers often use a slight variation in spelling or logo to lure you. Malicious links can also come from friends whose email has unknowingly been compromised, so be careful.
- **Secure your personal information.** Before providing any personal information, such as your date of birth, Social Security number, account numbers, and passwords, be sure the website is secure.
- **Stay informed on the latest cyber threats.** Keep yourself up to date on current scams. The Cybersecurity and Infrastructure Security Agency (CISA) can provide you with Alerts.
- **Use Strong Passwords.** Strong passwords are critical to online security. Review CISA guidance on Choosing and Protecting Passwords.
- **Keep your software up to date and maintain preventative software programs.** Keep all of your software applications up to date on your computers and mobile devices. Install software that provides antivirus, firewall, and email filter services.
- **Update the operating systems on your electronic devices.** Make sure your operating systems (OSs) and applications are up to date on all of your electronic devices. Older and unpatched versions of OSs and software are the target of many hacks. Read the CISA security tip on Understanding Patches and Software Updates for more information.

Here are some trending scams to look out for:

Money Mules

Scammers use people as "money mules" to receive or move money obtained from victims of fraudulent activities. Scammers proactively recruit people to be part of fraudulent activity without their knowing it. If a stranger asks you to open a bank account, or asks for access to your bank account or debit card, be extremely guarded. A scammer may ask you to move

money and direct you to deposit funds into your bank account, or ask you to purchase virtual currency or gift cards for someone else's benefit. In these scenarios, you may be unknowingly hiding someone else's money for them. Be very cautious if a stranger asks you to receive or forward packages containing money or goods, which may also be part of a similar fraudulent scheme.

If you believe you have engaged in, or contributed to, money mule activities, stop transferring money or merchandise, and stop communicating with the person giving you direction. Then, immediately report your concern to your bank. Your banker can assist you with the appropriate steps toward protecting your bank account and money. You should also report the suspected activity to law enforcement. Visit the U.S. Department of Justice webpage on money mules for more information.

Online Dating

Romance scammers, as they are often called, create fake profiles and try to develop relationships with their targeted victims through online dating apps or social networking websites. Once the relationship develops and they have earned your trust, the scammer makes up a story and asks for your money. Be aware that scammers are lurking in these areas, so you can keep yourself and your money safe. The Federal Trade Commission (FTC) has additional information on romance scams.

Impostors

Impostor scams are when a scammer pretends to be someone you know or trust to convince you to send them money. They may even claim they are with the FDIC or another government agency. These scams are communicated through emails, phone calls, letters, text messages, faxes, and social media. The messages might ask you to "confirm" or "update" confidential personal financial information, such as bank account numbers. In other cases, the communication might be an offer to help victims of current or previous frauds with an investigation or to recover losses. Some scams request that you file official looking forms, such as insurance claims, or pay taxes on prize winnings. They might claim that you have an unpaid debt and threaten you with a lawsuit or arrest if you don't pay. Other recent examples include check endorsements, bankruptcy claimant verification forms, stock confirmations, and investment purchases.

The FDIC or other government agencies do not send unsolicited correspondence asking for money or sensitive personal information, and we will never threaten you, or demand that you pay by gift card, wiring money, or digital currency. FDIC Consumer News: Scammers Pretending to be the FDIC has more information on impostor scams.

Mortgage and Foreclosure Scams

Watch out for scammers who falsely claim to be lenders, loan servicers, financial counselors, or representatives of government agencies who can help with your mortgage. These criminals prey on vulnerable, desperate homeowners. For more on mortgage scams and how to protect yourself, visit the FTC Mortgage Relief Scams.

Foreclosure scams usually come from multiple advertisements stating that a company wants to save you from foreclosure. This scam allows fraudsters to take the equity out of your home. They may even try to evict you from your home and sell it. Learn more at Common Foreclosure Rescue and Loan Modification Scams under the FDIC Consumer Assistance Topics.

Ransomware

One cyber threat often discussed in the news is ransomware. Typically, this scam targets businesses, not individuals. Ransomware is a type of malware created to lock or encrypt files on an electronic device like a smart phone or computer. The sender of the ransomware then demands a ransom in exchange for unlocking or decrypting the information on your electronic device. The scammer typically threatens to publically disclose or sell the compromised information, if the ransom is not paid.

If you believe your business is a victim of a ransomware attack, contact law enforcement immediately. You can also contact a local field office of the Federal Bureau of Investigation (FBI) or U.S. Secret Service to report a ransomware attack and ask for assistance.

Maintaining your cybersecurity will help prevent you from being a victim of identity theft and potential financial loss. Staying current on the latest types of scams can help you to identify the risks and learn how avoid them, so you can protect yourself and your finances.

Additional Resources

FDIC Podcast, Banking on Innovation: Building a More Resilient Banking System

FDIC Consumer News: Beware It's a Scam

FDIC Video #FDICExplains: Phishing

CISA Ransomware 101

Online Dating Scams

Auto Warranty Scams

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 **consumeraffairs3@fdic.gov**

FDIC