Scamming Tactics

What is Scamming?

A scam is a scheme performed by an individual or a company in an attempt to obtain money or something else of value. Scam artists on the telephone and on computers use lies, deception, and fear tactics to steal personal information and financial security.

What is Phishing and Spoofing?

Phishing is authentic-looking emails, text messages, and web pages that are used to trick users into revealing personal information. Spoofing is using a fake email address to make users think they know who is contacting them.

Warning Signs of Scams

Watch for communications from any individual or company you don't actively interact with regularly. Warning signs include:

- Telephone calls, emails, or letters regarding lotteries, drawings, or sweepstakes
- Any notice/communication beginning with "You Have Won"
- Language such as:
    - "We suspect an unauthorized transaction on your account"
    - "…please click the link below to verify your identity"
    - "I need to send my niece money right away"
- Authentic-looking claim checks
- Suspicious-looking links in emails or text
- Sweepstakes recovery calls
- Someone pretending to act as one of your family members

Steps to Minimize the Risk of Scams

- **Guard your personal information closely.** If someone asks for your Social Security number or other personal information, ask why. Ask how it will be used, how it will be protected, and what happens if it's not shared.
- **Don't respond to unknown requests.** This includes text messages, emails, or phone calls asking for sensitive information.
- **Beware of disaster-related scams.** Con artists take advantage of people after disasters. They claim to be from legitimate charitable organizations.
- **Read scam alerts.** The Federal Trade Commission (FTC) keeps a running list of scams (https://consumer.ftc.gov/scams). You can report scams on the FTC site, too.

- **Look up suspicious organizations.** If the scammer claims to be from an established organization, look up the number of the organization independently before acting.
- **Do not open messages from unfamiliar senders.** If you don't recognize the phone number or email address of the sender, don't open the message. If you do open the message, delete it. Do not click on links or call numbers listed in the message.
- **Shut down your computer when not in use.** Shutting down the computer when you aren't using it prevents hackers from getting personal information.
- **Use security software.** Downloading a trusted security software and keeping it updated will prevent unwanted viruses from getting into the computer.

Getting Help If You've Been Scammed

If you have been scammed, reach out to your banks and credit card companies to alert them of the situation. Also, reach out to the three national credit reporting agencies below and ask them to restrict access to your credit report. You may also submit a complaint to the FTC to create a personal recovery plan to help with your next steps.

- Experian (www.experian.com/fraudalert), 1-888-397-3742
- TransUnion (www.transunion.com/fraud), 1-800-680-7289
- Equifax (www.equifax.com/creditreportassistance), 1-888-766-0008

You can also place a freeze on your credit report. A freeze makes it less likely an identity thief can open a new account in your name. To learn more, visit the FTC website (https://www.ftc.gov/)and search for "fraud alerts" and "credit freeze."

This information is an excerpt from the FDIC Money Smart for Adults website. For more information, visit the FDIC Money Smart for Adults website (www.fdic.gov/consumer-resource-center/money-smart) or contact us at 1-800-257-1705 for printed materials.