Security Awareness

Fraud Alert - Scams

- How scams work
- Technical support scams
- Internal Revenue Service scams
- Prevention and protection

Often criminals impersonate personnel from legitimate, well-known companies or government agencies to trick people into handing over personal financial information, account numbers, user identification and passwords. The goal is account fraud and theft. Don't underestimate them — they are very convincing, sophisticated con artists.

How the scam works

The scammer contacts a person to report an urgent security problem or some suspicious activity with an internet device that needs immediate attention. Then they ask to verify personal information or to allow them access to computer files. Often, they direct a person to a website that looks authentic — but it is not. The page was set up to phish for personal information. These scammers need one thing; that is, to get account information and account access — without it — they can't steal.

Technical support scams

If you get an unexpected pop-up, telephone call, email or other urgent message about a problem with your computer or other device, stop right there! Technology companies will never call you to offer a solution to a random computer problem. This call is likely a technical support scam and the goal is to convince you that your computer or other device has a serious, urgent problem — and only they can provide the fix.

Internal Revenue Service scams

IRS scams occur when a scammer contacts you pretending to work for the Internal Revenue Service. The initial contact may be by telephone, email, mail, or even a text message. The two most common types of this fraud are:

- Tax collection scam – You receive a phone call or letter claiming that you owe taxes. They will demand that you pay immediately, often with a prepaid debit card or wire transfer. They threaten serious consequences if you don't pay.
- Verification scam – You receive an email or text message that requires you to verify your personal information. The message often includes a link to a phishing website that collects the data and imbeds malware.

SCAM PREVENTION AND PROTECTION

- Hang up if you get a telephone call from someone who claims to be from computer tech support or a government agency asking for personal information.
- Ignore it if you get a pop-up message, email or text that directs you to call a specific telephone number or go to a website for technical support or government agency.
- Never use the phone number in the pop-up or on caller ID. Instead, find the real contact information online.
- Never give control of your computer or other device to anyone who contacts you by telephone, e-mail, pop-up or text message.
- Remember the IRS doesn't initiate contact with taxpayers by telephone, email, text messages, or social media channels to request payments or personal information. Call 800-366-4484 to report it.

Resources

- Federal Trade Commission - www.ftc.gov
- Federal Deposit Insurance Corporation - www.fdic.gov
- National Credit Union Association - www.ncua.gov
- Financial Fraud Enforcement Task Force - www.stopfraud.gov