Frauds and Scams

Be on alert. Stay informed. Protect yourself.

Knowledge is power when it comes to fraud prevention. Arm yourself with the tools to identify a fraud or scam and what to do if you become a victim of fraud. Select a topic to learn how to keep your money safe, protect your personal information and report a scam.

Cyber Crime

Cyber crime includes more than fraudulent e-mail messages and fake websites that allow criminals to take your money. A cyber crime may involve tactics using ransomware, where criminals lock you out of your files until they receive a ransom, or phony phone calls, such as criminals pretending to represent a tech support company so they can get your information.

Protect yourself from a range of cyber crimes by taking these precautions:

- Use a firewall to protect your computer.
- Encrypt your home Wi-Fi network.
- Back up your files regularly.
- Create strong passwords and share them only when necessary.
- Don't respond to spam e-mails.
- Download with caution.
- Monitor your financial accounts regularly for fraudulent activity.
- Don't visit suspicious websites or follow links to sources you don't trust.
- Keep your computer current by updating antivirus software, antispyware, operating system, and system patches.
- Don't share your personal information with sources you don't trust, especially pop-ups.
- Have different passwords for work related and non-work related accounts.
- When you're not using your computer, turn it off.
- Don't give control of your computer to an unauthorized third party.

The Federal Bureau of Investigation maintains a list of Cyber Crime Stories. Be aware of the latest cyber scams by checking this list and searching the Internet for the most recent cyber scams.

If you are a target of cyber crime, contact your financial institution immediately. Then, report the crime to the Internet Crime Complaint Center (IC3), a joint government collaboration. The IC3 links complaints together to refer them for case consideration. It also uses data to identify emerging trends and patterns.

Government Imposter Scams

Scammers sometimes pretend to be government officials to get you to send them money. They might promise lottery winnings if you pay "taxes" or other fees, or they might threaten you with arrest or a lawsuit if you don't pay a supposed debt. Regardless of their tactics, their

goal is the same: to get you to send them money.

Don't do it. Federal government agencies and federal employees don't ask people to send money for prizes or unpaid loans. Nor are they permitted to ask you to wire money or add money to a prepaid debit card to pay for anything.

Before you get caught in this type of scam, look for indicators:

- **You've "Won" a Lottery or Sweepstakes** - Someone claiming to be a government official calls, telling you that you've won a federally supervised lottery or sweepstakes.
- **You Owe a Fake Debt** - You might get a call or an official-looking letter that has your correct name, address and Social Security number. Often, fake debt collectors say they're with a law firm or a government agency — for example, the FTC, the IRS or a sheriff's office. Then, they threaten to arrest you or take you to court if you don't pay on a debt you supposedly owe.

Five Ways to Beat a Government Imposter Scam:

1. Don't wire money.
2. Don't pay for a prize.
3. Don't give the caller your financial or other personal information.
4. Don't trust a name or number.
5. Put your number on the National Do Not Call Registry. Register your phone number at donotcall.gov.

Phishing, SMishing & Vishing

Phishing

Phishing is when Internet fraudsters impersonate a business to trick you into giving them your personal information, such as usernames, passwords and credit card details. Legitimate businesses don't ask you to send sensitive information through insecure channels.

For example, a fraudulent e-mail may state that NCUA will add money to the member's account for taking part in a survey. The link embedded in the message directs members to a counterfeit version of NCUA's website with an illicit survey that solicits credit card account numbers and confidential personal information. NCUA will never ask credit union members or the general public for personal account or personally identifiable information as part of a survey.

Tips:

- Don't select links in e-mails that ask for personal information.
- Never open unexpected attachments.
- Delete suspicious messages, even if you know the source.

SMishing

Phishing via SMS, or SMishing, uses cell phone text messages or SMS (Short Message Service) to trick you into providing personal and financial information. Smishers may use URLs or an automated voice response system to try and collect your information.

Tip: In some instances, criminals have used malicious software in their text messages solicitations. To prevent further security issues, completely remove unsolicited text messages from your phone. This may take two steps: deleting the text and then completely removing it from your device.

Vishing

Phishing by voice, or vishing, exploits a general trust in landline telephone services. The victim is often unaware that voice over Internet Protocol (VoIP) allows for caller ID spoofing, thus providing anonymity for the criminal caller. Rather than providing any information to the caller, the consumer should verify the call by contacting the financial institution or credit card company directly, being sure to use the institution's accurate contact information (i.e., do not use contact information the caller provides).

Scams Targeting Older Adults

The elderly are the fastest growing segment of our society and they are also an important part of our country's economy. America's growing older adults population is uniquely vulnerable to a broad range of exploitation and abuse. Financial crimes in particular are targeted at older adults with alarming frequency, and are all too often successful.

Tax Fraud

Once a cybercriminal has your name and Social Security number, he or she can file a tax return in your name by making up financial information that generates a large refund. Since the IRS doesn't require W-2 forms when you file electronically, cyber criminals can commit electronic tax-refund fraud easier than paper tax fraud, especially since electronic tax-refund fraud is straightforward and hard to detect.

Tip: Be extremely protective of your personal information, and only share it with trusted sources, especially when using the Internet. Often, tax fraudsters will obtain your information through e-mail phishing, social engineering tactics, the black market, and other sources.

Tax identity thieves may use your Social Security number to get a tax refund or a job. You take steps to protect your personal information by not opening unrecognized emails and shredding important documents. But, do you know how to recognize and prevent from becoming a victim of tax identity theft?

Report a Scam

If you get a call from an imposter, file a complaint at ftc.gov/complaint. Be sure to include:

1. Date and time of the call,
2. Name the imposter used,
3. What they tell you, including the amount of money and the payment method they ask for, and
4. Phone number of the caller; although scammers may use technology to create a fake number or spoof a real one, law enforcement agents may be able to track that number to identify the caller.

Smart Shopping During the Holidays

Criminals and scammers use many techniques to fool potential victims. NCUA has put together a list of tips you can use to avoid becoming a victim of a holiday scam. Take a look at a few of the newest and most common scams you should watch for during the holiday season.

For more information visit
mycreditunion.gov