TRONA VALLEY
FEDERAL CREDIT UNION

Tips to Protect Seniors from Being Scammed

Each year, millions of seniors fall victim to some type of financial fraud or confidence scheme. Financial abuse targeting seniors is a widespread issue affecting lots of people. The FBI estimates that seniors lose more than $3 billion each year to fraudsters.

One of the best ways to protect yourself from scams at any age is to familiarize yourself with some of the most common schemes that scammers use to steal money, bank information, and other personal details.

Fake Lottery - Seniors get a call saying they've won millions of dollars and need to pay administrative fees or taxes to receive money.

Grandparent Scam - A call or email to the grandparent posing as law enforcement or medical professionals claiming to represent a family member in distress (overdue rent, payment for car repairs, etc.). They might also pose as the "grandchild" directly asking the grandparent to guess who is calling. Scammers ask for money to be wired to pay for medical bills or legal fees.

Fake Virus or Ransomware - Pop-up browser windows simulating virus-scanning software will fool victims into either downloading a fake anti-virus program (at a substantial cost) or an actual virus that will allow scammers direct access to the computer. Also, popups claim that the computer has been locked and requires payment within a very short time or the files will be deleted.

Tech Support Scam - Scammers claiming to be from legitimate companies demand payment for unnecessary tech support services, or to fix a problem that doesn't exist. Sometimes scammers will create fake websites with a number to call to receive support.

Email/Phishing - A senior receives email messages that appear to be from a legitimate company or institution, asking them to "update" or "verify" their personal information. Scammers also use LinkedIn and other social media networks like Facebook to gather information. They can then use the victim's connections to trick the victim into thinking their contact is messaging them.

False Online Shopping - Scammers set up websites that seem like legitimate storefronts but only exist to collect your payment information or sell stolen goods. These sites can look surprisingly real and might be found on social media or in websites' comments sections.

Romance Scam - Using a fake online identity, a scammer will gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim. This type of scam can occur on dating and social media sites.

Crime Scam - A senior gets a scary phone call saying their name or social security number was used in a crime such as a stolen car or illegal drug purchase.

Social Security Scam - Scammers pretend they represent Social Security Administration (SSA) and need money to adjust a senior's Cost of Living Adjustment (COLA).

IRS Scam - A senior receives a phone call or voice message claiming to be the IRS. The scammer will say that the senior owes taxes and could be sent to jail if they don't receive payment right away.

Medicare Impersonator - Scammers try to steal personal information and identity by calling and asking for information in order to issue the senior a new Medicare card or offer you discounted additional coverage.

Deals on Prescriptions - Preying on the high cost of medical care, scammers offer discounted medications. They might even send a sample drug that could be harmful if taken.

False Investment Opportunities - An unsolicited call or email from a financial advisor offering a once-in-a-lifetime investment opportunity. If it's too good to be true, it probably is.

Refund Scam - Scammers will claim that the senior has been given too much money due to an accounting mistake and demand the money back.

Fake Insurance - Scammers offer deals on different types of insurance such as home, auto, and life in order to obtain personal information from seniors.

Here are some tips:

1. Don't act quickly - Scams are based on fear and urgency. Always take a little extra time to think it through and evaluate the legitimacy of what you are being asked to do.

2. Avoid odd payment types - Scammers will often ask you to send them money with a wire transfer, money order, cryptocurrency, payment app, or gift card. Legitimate businesses will accept credit cards. Be suspicious of excuses for alternative forms of payment.

3. Notice threatening behavior - Often scams are presented as urgent situations requiring immediate action. If you receive threats or hostility for asking questions that's a sign they are a scammer.

4. Be suspicious of fake caller IDs - Using computer software, scammers can make phone calls and emails that look like they're coming from legitimate companies, government organizations, or your local area code. Often it is best to ignore people that contact you uninitiated. At the very least avoid sharing private information. Looking up the organization's contact information and contacting them yourself is a safer option.

5. Be cautious of impersonation - Con artists can sometimes pretend to be the government. Before making investments or online payments, be sure that you have confirmed that the organization is a legitimate business by asking for information about the company and checking that they are registered with the Better Business Bureau.

6. Do not reveal personal information - Con artists can try to get you to provide them with personal information like your Social Security number, account numbers, passwords, credit cards, or other identifying information which can be sold to fraudsters.

7. Avoid suspicious links - Don't click on links in unsolicited emails, texts, or social media messages.

8. Ask a friend or family member - Before giving out your credit card number or money, ask a friend or family member if the request or situation seems suspicious—particularly if you've been told by someone you don't know that the person needs help.

9. Add extra security to your accounts - Many online accounts let you turn on multifactor authentication. You may then need to enter a code that's sent to your phone or email, or that you generate with an app, before accessing your account. Enabling this extra security measure can keep scammers out of your accounts even if they get hold of your username and password.

10. Call the Hotline - If you feel that you or someone you know may be a victim of elder abuse, there's no need to be ashamed - it can happen to anyone. The faster you report the crime, the better chance you have of minimizing the consequences. Call the National Elder Fraud Hotline at 1-833-FRAUD.

Above all else, listen to your gut. If something feels off about a stranger's request, it's okay to be skeptical and investigate further before taking action. At Trona Valley FCU, we are committed to bringing attention to the issue of elder abuse. Working together to recognize the signs and symptoms and act, we can help seniors stay safe.