FALCON
WEALTH ADVISORS

Elderly Financial Fraud

4 Tactics Commonly Used to Steal Sensitive Information

Financial scams are detrimental to everyone affected but they pose an even greater risk for older individuals who often own valuable assets such as homes and life insurance policies and may rely on fixed incomes from retirement savings. The elderly have become regular targets of fraudsters due to their increased vulnerability to cognitive disorders and disabilities, as well as their lack of awareness in identifying suspicious online content.

In November 2023, the Federal Trade Commission (FTC) reported that three out of four adults aged 50-80 had been victims of financial fraud over the previous two years.[1] These scams were carried out by phone, text, email, or social media.

Here are some of the most common scams targeting seniors, along with guidance on how to protect yourself or a loved one from falling victim to them.

01 | Government Impersonators

A type of fraud that seniors often become victims of is government official impersonator scams. These impersonators claim to work for various government agencies such as the Social Security Administration, the Internal Revenue Service, and the Centers for Medicare and Medicaid Services, and they attempt to gather personal information to use for stealing the senior's identity or bank account information. They may claim that there is an urgent issue that requires immediate attention. To avoid being caught, they ask for payment through wire transfers, cryptocurrency, gift cards, or payment apps like Zelle, Cash App, and Venmo.

If you receive a suspicious call like this, hang up and do not engage. If you're unsure about the legitimacy of the call, directly contact the agency using the official number provided in your mail or past communications. Keep in mind that government agencies like the IRS do not reach out via email, text, or social media. If you receive a message through these channels, report it to the Federal Trade Commission, Office of the Inspector General, or your state's Attorney General's office.

02 | Internet Ads & Phish

When scrolling online or playing games on your phone or laptop, you may come across pop-up ads that encourage you to click on them. These ads can promise things like a gift card for filling out a survey, or they may say your computer has a virus that can be removed by clicking the ad.[2] While not all online ads are malicious, it is best to avoid clicking on any ads that hint at the immediacy of the offer or sound too good to be true. Clicking on pop-up ads can allow hackers to download malware onto your devices, potentially compromising your personal information. In some cases, the ad may even download ransomware, which can lock you out of your computer files and allow hackers to demand a ransom for you to regain access.

Another common tactic criminals use to get ahold of your information is to send phishing emails. Phishing involves creating emails or websites that appear to be from legitimate

companies and including links or buttons for you to click. These lead you to a fake webpage where you're prompted to update or provide personal information.

If you are unsure of the legitimacy of an email, you can click on the sender's email address to see if it matches the address listed on the company's website. If it does not match, report the email and mark it as spam. Additionally, you can hover over links to see if they direct you to the claimed destination.

03 | Friendship and Romance Swindlers

Many older adults go online to find companionship, especially after the death of a spouse. But like anyone who is active online, there is a risk of becoming the victim of another type of scam, called a "pig butchering scam".[3] With these, fraudsters use fake pictures and names to develop a profile to initiate conversations with victims. The scammer may spend weeks or months developing a relationship and building trust with the victims before asking them to send money or sending the victims a link to sign up for online investments, such as cryptocurrency. In this example, the link wouldn't lead the victims to a website for a legitimate cryptocurrency exchange, rather it directs any money sent directly to the scammer's account, all unbeknownst to the victims.

Scammers tend to target older, widowed adults who are grieving and seeking an emotional connection with someone. This vulnerability can make the victim unmindful of warning signs. It is important to be cautious and reserved when interacting with strangers online. Avoid sharing personal financial information and do not send money or engage in investment opportunities with individuals met online.

04 | AI Cloning

A concerning new scam involves the AI cloning of a loved one's voice. Scammers achieve this by using a short video clip of their loved ones speaking, which is then processed through an AI platform to make the voice say whatever the scammer wants.[4] The voice often sounds distressed, claiming that someone is harming the person and demanding ransom money.

As of now, there are no laws preventing the use of AI impersonation, which makes this fraud particularly dangerous. To protect yourself and your family, consider establishing a password or phrase to use in situations like this. Such an agreed-upon phrase will help you verify the validity of the call and determine whether your loved one is actually on the other end.

There are numerous tactics that scammers use to deceive people into giving them money. A financial advisor can serve as a valuable resource in educating older individuals about the latest scams and how to engage safely online. They can also provide guidance on selecting investments that align with one's stage of life and age. If you or a loved one falls victim to fraud, seek advice from your advisor to ascertain the most appropriate actions to safeguard your accounts and pursue recovering your funds.

1900 SHAWNEE MISSION PKWY, SUITE 210
MISSION WOODS, KS 66205
FALCONWEALTHADVISORS.COM
913-326-1900

[1] Facts about fraud from the FTC – and what it means for your business. (2024, April 4). Federal Trade Commission. https://www.ftc.gov/business-guidance/blog/2024/02/facts-about-fraud-ftc-what-it-means-your-business

[2] Identifying and avoiding fraudulent Pop-Ups. (n.d.). Schwab Brokerage. https://www.aboutschwab.com/identifying-and-avoiding-fraudulent-pop-ups

[3] How to stay safe when having conversations online. (2024, May 7). https://www.ncoa.org/article/how-to-stay-safe-when-having-conversations-online/

[4] Bethea, C. (2024, March 7). The terrifying A.I. scam that uses your loved one's voice. The New Yorker. https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice