Scam Prevention Checklist

- **Register** with the National Do Not Call Registry at 888.382.1222 or visit donotcall.gov & the TN Do Not Call Program at 877.872.7030
- **Track scam**s at bbb.org/scamtracker
- **Avoid** isolating yourself
- **Use** a trusted antivirus & malware software on all devices
- **DO NOT** be pressured into making a snap decision based on an emotional response.
- **Don't trust** your Caller ID
- **Never** click on a link sent in an unsolicited email or text message—type in the web address yourself. Only provide information on secure websites
- **Be skeptical**. If it sounds too good to be true, it probably is
- **Read** all documents that you sign. If you don't understand, seek advice.
- **Never** give out your personal or financial information in response to an unsolicited call or message
- Always **shred** financial and billing information
- **Be suspicious!** If someone calls or appears at the door, DO NOT give them personal information.
- **DO NOT** announce when your home may be empty. Forego the note on the door to the delivery persons, wait to post your photos on social media & put your mail on hold
- **Never** access personal accounts like bank institutions on public Wi-Fi
- **Check** your credit report for free at annualcreditreport.com
- Create **different passwords** for your online accounts with at least 12 characters
- Enable **2-step authentication** for your accounts
- **Never** use gift cards, wire money or cryptocurrency as payment

You've Been Scammed! What Now?

Step 1: Notify the local police department.

Step 2: Notify your financial institution and close the accounts or debit/credit cards.

Step 3: Contact all three credit bureaus and set up a free 90-day fraud alert. You can also set up a credit freeze.

Step 4: Tell a family member or loved one. You may think by telling your family that they will think you are unfit to manage your affairs but remember that is what scammers want you to think. By telling your family you accomplish two goals:

- You show them that you are capable of managing your affairs because you are taking the proper steps to protect yourself.
- You are protecting them from being scammed.

Step 5: If your social security number was exposed, please call the Social Security Administration at 1-800-772-1213.

Step 6: The Federal Trade Commission creates public warnings and tracks scam data. Call FTC at 1-877-FTC-HELP.

Step 7: The State Attorney's Office keeps track of fraud in your state and helps create public notices. To find your local SAO, visit www.justice.gov/usao/us-attorneys-listing.

Step 8: If you were a victim of a cyber scam, file a report at ic3.gov, which is operated by the FBI.

Step 9: For identity theft victims, visit identitytheft.gov for resources and forms.

Step 10: If the scammer used a legitimate company, you should contact the business so they are aware and able to warn other clients.

Step 11: Call AgeWell at 615-353-4235 for help finding victim services & support.

SCAM PREVENTION FOR OLDER ADULTS

Safeguard Your Money & Identity

Developed by

AgeWell MIDDLE TENNESSEE

with support from

The Community Foundation of Middle Tennessee

The Memorial Foundation

The West End Home Foundation

Printing by

JACKSON®

Senior Scam Statistics

- 1 in 5 Americans 65+ has been financially exploited
- Annually, scammers cause older adults to lose over **$3 billion**
- People 80+ reported median losses of **$1,674**, which is more than all other age demographics
- 1 in 10 scammed older adults will turn to Medicaid as a direct result of being defrauded
- In 2022, **49%** of all fraud reports were from older adults 50+

Why Are Older Adults Targeted?

- It is widely assumed that older adults have a "nest egg", own their homes and have excellent credit
- They were generally taught to be polite and trusting, making it difficult to say "no" or hang up the phone
- Older adults are less likely to report and are more likely to be home during the day.
- Older adults may be less familiar and comfortable with technology and protecting themselves online.

Common Scams

Every day a new scam surfaces that is aimed at older adults. The best defensive strategy is knowledge and awareness of criminal behavior.

Scammers will use different tactics to generate emotional responses like fear or sympathy to get you to act without thinking. Remember some may call but others use mail, text, ads or emails.

Call Center Fraud: Illegal call centers victimize thousands every year. The majority of these scams reported include **Government Impersonation and Tech/Customer Support Scams**. Call center scammers take advantage of older adults' unfamiliarity with technology, online banking, etc. With tech support scams, you may get a pop-up, an email or a call from a scammer, pretending to be with a well-known company, telling you that you have a problem with your computer or account. Next, the scammer may

- ask for remote access to your computer
- try to enroll you in a fake warranty program
- install malware that gives them access to your data like user names and passwords
- ask for your credit card for fake repair services
- direct you to fake websites to enter your credit card, bank account and other personal information

Government impersonator scammers pretend to work with a government agency like the IRS, Medicare, or the Social Security Administration. They typically use threats that if you don't pay or give them information, you will be arrested or lose benefits. It is important to remember that these agencies will never call you out of the blue.

Cryptocurrency: This is a digital currency that is an alternate form of payment using encryption. Some common cryptocurrencies are Bitcoin, Ethereum, etc. Some cryptocurrency scams include investment schemes, social media giveaway scams, fake crypto exchanges, etc. Crypto is also quickly becoming a preferred payment for other scams.

Spoofing: There are several spoofing techniques that scammers use including email, text message, caller ID, URL and GPS. The spoofer's entire goal is to convince you that you can trust them.

Phishing: This is a type of scam that targets people through emails, fake websites or even phone calls. All to convince you that they are from a legitimate source like a bank or mortgage company to gather your sensitive information.

Malware/Ransomware: Malicious software is called malware and it is a file or code that is delivered online through a network that can infect, explore and steal virtually through your device. **Ransomware** is a specific example of malware that prevents you from accessing your computer files and/or networks and demands that you pay a ransom to regain access. You can unknowingly download ransomware by opening an email attachment, using a link or visiting a website that is embedded with malware. Some other forms of malware are viruses, trojans and spyware.

Investment Scams: Investment fraud involves complicated financial crimes described as low risk with high rewards. These scams include advance fee fraud, pyramid schemes, and real estate investments. Older adults are pressured into accessing their retirement accounts, home equity, etc.

Lottery/Sweepstakes/Inheritance Scams: The most common example of lottery/sweepstakes scams is notifying potential victims that they won a big contest or sweepstakes but must pay fees or taxes upfront. Inheritance schemes typically start with a communication that a distant, unknown relative has left a large inheritance but the victim must pay taxes and/or fees first.

Confidence/Romance Scams: These scams start when a criminal creates a fake online identity and uses the illusion of a romantic or close relationship to manipulate or steal from the victim. **Grandparent Scams** also fall into this category where scammers impersonate a loved one like a grandchild who is in trouble or hurt and needs money immediately.

Extortion: Scammers threaten victims that if they don't pay, they will release sensitive information. These scams include email extortion, hitman schemes, government extortion and sextortion.

Non-Payment/Non-Delivery: Scammers use social media and online shopping to place fake ads. Many victims report never receiving the ordered item(s) or receiving something completely different.

"Juice Jacking": This is another cyber-theft tactic that criminals use by loading malware onto public USB charging stations to access electronic devices while they are being charged. Once inside your device, the scammer can lock your device and steal personal data and passwords.

Identity Theft: Attackers use fraud or deception to obtain personal or sensitive information. The three most common types of identity theft are financial, medical and online.

Employment Scams: Fraudsters advertise jobs the same way legitimate companies do, on social media, job sites, newspapers, etc. However, in this case, they are attempting to steal your money and/or personal information. Common job scam examples are work-from-home, caregiver/personal assistant, mystery shoppers, and government/postal jobs.

Checking Washing: These scams involve changing the names and amounts on checks and depositing the "new" forged checks. Sometimes, these checks can be stolen from your mailbox and washed in chemicals that remove pen ink.

Stay Informed

Sign up for our FREE Scam of the Month email blast:
scams@agewelltn.org

AgeWell Middle Tennessee
615-353-4235
www.agewelltn.org