

BE ON THE LOOKOUT for these common scams

Scammers will use different tactics to generate emotional responses like fear or sympathy and get you to act without thinking. Remember some may call but others use mail, text, ads or emails. Here is a list of the top ten scams that specifically target seniors.

IRS Impersonation Scams:

Scammers pretend to call from the IRS, saying you owe back taxes and you will go to jail unless you pay immediately. You are then directed to purchase gift cards (like iTunes) or complete a wire transfer. This fraud is coming through US Mail, email and phone calls. Another version is an "official" looking letter from the IRS stating that you owe taxes related to the Affordable Care Act from the 2015 tax year. This notice is labeled "CP2000" and instructs you to send payments to the IRS care of an Austin, TX post office.

Remember, the IRS will never contact you via email or phone!

Sweepstakes Scams: The basic premise is that you won the lottery or sweepstakes and need to pay taxes or "verify personal information" (i.e., social security number) before receiving the winnings.

RoboCalling/"Yes" Scam: Many people receive telemarketing and government impersonation scams

despite being registered with national and state do-not-call lists. A new approach scammers use is asking, "can you hear me?" prompting you to respond with "yes." Now, the scammer has your voice recorded and can access utility account or credit card information.

Computer Scams: Many different scams are prevalent online. One example, scammers call pretending to be from "Microsoft" or another reputable company and state that they'll need "remote access" to your computer. You are then instructed to pay by giving personal banking information or wire transfer. Another scam is a pop-up windows saying your device has been infected with a virus. Also, you may receive emails from what appear to be reputable companies like your bank, the IRS, credit card companies, or even "friends". Sometimes just opening the email can cause a virus to be introduced on your device.

Elder Financial Abuse: Typically a guardian or caretaker is taking money from an older adult who is unable to manage their own finances.

Grandparent Scams: Scammer calls pretending to be the grandchild, says they're in trouble or their parent is in

the hospital and needs money. Caller may also pretend to be police or a doctor. Another version is virtual kidnapping, where the caller states that the grandchild has been kidnapped and you need to wire money for them to be released.

Romance Scams/Confidence Fraud:

Schemers develop friendships via social media pretending to be a deployed U.S. soldier, and eventually ask you for money or favors (i.e., forwarding a package).

Government Grant Scams: Defrauders say that the victim is eligible for a government grant, but has to pay taxes first. This scam uses phones, email, social media, etc.

Counterfeit Check Scams: Fake check scams always involve someone giving you a genuine-looking check or money order and asking you to wire money in return.

Identity Theft: There are many different methods (i.e. medical, tax, social security, child identity, etc.). The common denominator is theft of personal information to benefit the scammer.

Jury Duty: Scammer says you failed to report for jury summons. If you pay or verify personal info, you'll avoid jail.

Contractor Fraud: Dishonest contractors try to scam you either by stealing your money, using shoddy work/materials or illegal permit practices.

Utility Scams: Fake employees try to gain personal or financial information by trying to say you are behind on your payment. Some also try to distract you while another scammer slips in the back door or window and steals your money, jewelry or even prescription medications.

Prescription Medication Fraud: If you are researching for cheaper medications online, this opens you up to be targeted by scammers pedaling fake prescriptions. This is dangerous because you never know what substance is in the new, cheaper medication. Scammers could also steal your personal information.



Stay Informed!

Sign up **FREE** Scam of the Month email blast: scams@coamidtn.org

**Council on Aging
of Middle Tennessee**

615-353-4235 ♦ www.coamidtn.org

Scam Prevention Checklist

- ⇒ Add your name/number to the National Do Not Call Registry. **Call 1.888.382.1222** or visit www.donotcall.gov
- ⇒ Inform yourself about scams and frauds at www.usa.gov/scams-and-frauds
- ⇒ **Avoid** isolating yourself. Take up a hobby, visit friends or family, volunteer, etc.
- ⇒ **DO NOT** allow someone to pressure you into making a snap decision.
- ⇒ **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.
- ⇒ **DO NOT** give out personal information (i.e. Social Security number, account numbers, personal identification numbers or financial information) to anyone you don't trust, online or over the phone.
- ⇒ Always **shred or tear up** financial information and billing information.
- ⇒ **Be suspicious.** If someone calls or appears at the door, **DO NOT** give them personal information.
- ⇒ **DO NOT** open emails or links that you receive from unknown sources. Double check the source by calling the company or looking at the sender address.
- ⇒ **DO NOT** announce when your home may be empty. Forego the note on the door to the delivery persons and wait until you return to post your photos on social media.

You've Been Scammed!

What Now?

- Step 1:** Notify law enforcement immediately.
- 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:
1. You show them that you are capable of managing your affairs because you are taking the proper steps to protect yourself.
 2. 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 the scammer used a legitimate company, you should contact the business so they are aware and able to warn other clients.

Scam Prevention for Older Adults: Safeguard Your Money and Identity



Developed by:
Council on Aging of
Middle Tennessee

with support from:

the
**Women's
Fund**
of The Community Foundation
of Middle Tennessee



Senior Scam Statistics

- ◆ **1 in 5** Americans 65+ have been financially exploited
- ◆ Annually, scammers cause older adults to lose over **\$36 billion**
- ◆ **1 in 23** senior fraud cases are reported
- ◆ **1 in 10** scammed seniors will turn to Medicaid as a direct result of being defrauded
- ◆ In 2015, **57%** of all fraud complaints were from adults 50+



Why are Seniors Targeted?

- ◆ It is widely assumed that older adults have a "nest egg", own their own home and have excellent credit.
- ◆ Older adults were generally taught to be polite and trusting, making it difficult to say "no" or even hang up the phone.
- ◆ Seniors are less likely to report the crime and are more likely to be home during the day.
- ◆ Older adults are perceived to be more vulnerable, especially those isolated, lonely, disabled or grief-stricken.
- ◆ Seniors are less familiar with technology and protecting themselves online.