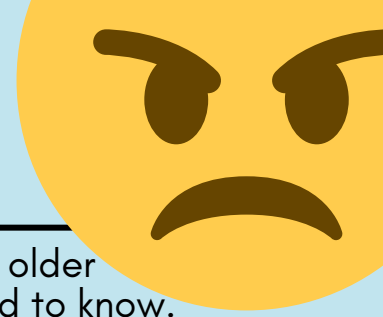


# Let's Prevent It Together!

## SCAMS & FRAUD



There are thousands of scams and fraud hits daily, especially targeting older adults. And the initiators are becoming so savvy that sometimes it's hard to know. Below are just a few examples of prevalent scams & fraud that are happening.

- ✓ **Medicare** won't call on the phone and ask you to give them personal information. They will not call and tell you they will "cancel" your insurance or that the government has canceled Medicare. If you are uncertain or would like to report a call, hang up and dial: 1-800-MEDICARE (1-800-633-4227)
- ✓ You might receive a phone call or an email where you are asked to purchase a **gift card** and then give the person the number on the card, or send it to an address. If it's an email request, it might look and sound exactly like it's coming from someone you know well. It may reference a child or other relative. **DO NOT RESPOND.**
- ✓ **Computer technical support** scams prey on lack of knowledge about computers and cybersecurity. A pop-up message or blank screen usually appears on a computer or phone, telling you that your device is compromised and needs fixing. They list a phone number and when you call for help, the scammer may either request remote access to your computer and/or that you pay a fee to have it repaired. They can take hundreds of dollars!
- ✓ **Robo-Callers:** Robo callers are those that dial hundreds of phone numbers at one time trying to get response. Often if you don't answer they leave a recorded message about an expired car warranty, credit card problem, or similar, and leave a phone number to respond. Sometimes if you answer they may ask "can you hear me?" and when you respond they record your voice to use maliciously. If you don't recognize a phone number, don't answer it. If you do answer, and you recognize a robo-call or you don't recognize the caller, don't say anything and hang up. Do not respond to recorded voicemail messages.
- ✓ **Romance scammers** create elaborate fake profiles, often on social media, and exploit loneliness for money. In some cases, romance scammers may (or pretend to) be overseas, and request money to pay for visas, medical emergencies, and travel expenses to come visit the U.S. Because they drag on for a long time, romance scammers can get a lot of money from a senior—the Federal Trade Commission found that in 2019 alone, seniors lost nearly \$84 million to romance scams. (source: ncoa.org)

**RED FLAGS** that indicate a scam or fraud include: Offer seems too good; they want private information; there are grammatical errors; there is a request for fees; suspicious email domains; suspicious or no address; request for access to your computer; untraceable payment method; pressure.

*Source: Office of the Attorney General, Commonwealth of Virginia (website below)*

Who to contact if you wish to report a scam or fraud, or need help:

- Your local police department or sheriff (see county pages 13-22)
- Office of the Attorney General, Commonwealth of Virginia: [www.oag.state.va.us](http://www.oag.state.va.us)
- The Federal Trade Commission (FTC): [ReportFraud.ftc.gov](http://ReportFraud.ftc.gov) (also has S&F updates)
- AARP Fraud Watch Network Helpline: 877-908-3360 (also has S&F updates)