

Avoiding *Scams & Fraud*

How to Spot Scams and Where to Get Help

Compliments of

Insert Your Business Card
in This Clear Holder...
**Seen Every Time Seniors
Use Their Booklets!**

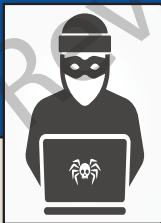
Your Quick Reference Guide

Fraud Targeting Older Americans is a Growing Problem

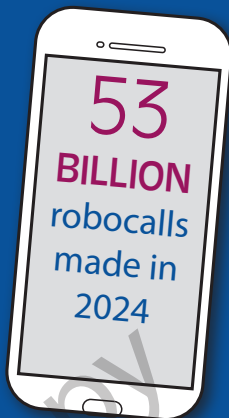
>300%

Increase in total losses from 2020 to 2023

The average loss per victim was
\$33,915



The most common types of fraud reported were **Tech Support** and **Confidence/Romance** scams.



60+

Age group with fraud losses of

3.4

billion dollars in 2023

Victims of fraud ages 60+ who actually report fraud is less than

25%

Section One

For quick reference, this section is highlighted with blue bars. You'll find pages about the common scams and fraud that target older adults, tips to avoid these scams and where to get help.

Common Scams and Fraud 2-3

Tips for Avoiding Scams and Fraud 4-5

Where to Find Help 6

Contacting Credit Bureaus & Three Tips to Prevent Medicare Fraud 7

Fraud Vocabulary & Hang Up on Gift Card Scams 8

Common Scams and Fraud

These two pages describe the most common scams and fraud as reported by local, state and federal officials.

- **Government Impersonation Scams:** Scammers pretend to be from the IRS, Social Security or Medicare, and tell the victim they will be arrested, deported or lose benefits. They then ask for personal identifying information or payment.
- **Sweepstakes/Lottery Scams:** You receive calls or mailings claiming you have won a substantial amount of money, but must first pay a fee or taxes to collect your winnings. These winnings don't exist.
- **Tech Support Scams:** Scammers contact you, posing as tech support representatives. They claim your computer has a virus or other issues. Then they request remote access to your device to steal information or demand payment for "fixing" the problem.
- **The Grandparent Scam:** Fraudsters impersonate grandchildren or other relatives in distress, sometimes using AI to sound realistic. They claim they need immediate financial help due to an emergency, such as an accident or legal trouble.

- **Romance Scams:** Scammers create fake online profiles, often on dating websites, and establish romantic relationships. They exploit emotions and trust to request money.
- **Investment Fraud:** Retirees are targeted with promises of high returns or guaranteed income in either non-existent or high-risk investment schemes.
- **Robocall/Phone Scams:** Fraudsters often "spoof" a number, making it appear as if a call is coming from a legitimate organization. There are many variations of this scam, most ending with the caller requesting money.
- **Medicare Fraud:** Scammers pose as healthcare providers, offering unnecessary services or equipment. They bill Medicare for these fraudulent claims.
- **Digital Fraud:** Scammers use e-mails, text messages and fake websites that look like those of trusted companies to steal your personal information. These fake messages trick people into clicking harmful links or sharing private details with criminals.
- **Cryptocurrency Scams:** Fraudsters may urge you to invest in digital money (like Bitcoin), promising quick and high returns.

Sources: FBI, National Council on Aging, AARP.

Tips for Avoiding Scams and Fraud

Experts recommend reviewing the following points to help you avoid becoming a victim.

- Scammers create a sense of urgency, so resist pressure to act quickly. Call the police if you feel there is a danger to yourself or a loved one.
- Always be cautious when you receive a phone call, text, e-mail, mailing or in-person visit from someone you do not know. If they ask for personal information (like a Social Security number or log-in information) or money, it is most likely a scam.
- Be suspicious if anyone demands payment by cryptocurrency, prepaid gift cards, gold, wire transfers or mailing cash. Never use a cryptocurrency ATM.
- If you suspect you are the victim of a fraud, immediately contact your financial institution to place protections on your accounts.
- Seek advice from trusted sources, such as family members, friends or professionals, before making major financial decisions.
- Use strong and unique passwords for online accounts, and shred documents with personal information before discarding them.

- Stay informed. Seek information on frauds and scams from AARP, the FBI or other trusted websites.
- Government or law enforcement will never contact you by phone to say that you are under investigation.
- If someone you don't know contacts you and asks for remote access to your computer, it's a scam. Contact someone you trust.
- Be careful what you post online. Scammers can use information from social media to better understand and target you.
- Establish a family "safe word" or unique phrase that only you and your loved ones know. If someone claiming to be family calls with an emergency request for money, ask for this code word to verify their identity.
- Use antivirus software from a reputable company and keep it up-to-date.
- Check fraud is on the rise. If you can, mail checks at the post office or hand deliver them.
- Be careful of pop-up windows on your computer, tablet or cell phone. Shut down your device and disconnect from the Internet if a pop-up message locks your screen.

Sources: FBI, CFPB, FTC.

Where to Find Help

Here are resources that may be helpful.

- **FBI Internet Crime Complaint Center (IC3)**
ic3.gov
*This is the federal hub for reporting cyber crime.
Fraud specialists provide free support and guidance.*
- **AARP Fraud Watch Network**
1-877-908-3360, aarp.org/money/scams-fraud/
Get guidance from fraud specialists.
- **Department of Justice National Elder Fraud Hotline**
1-833 FRAUD-11 (1-833-372-8311),
ovc.ojp.gov/program/stop-elder-fraud
Case managers are available to assist you.
- **Federal Trade Commission (FTC)**
1-877-FTC-HELP (1-877-382-4357),
reportfraud.ftc.gov
*You can report anything you think is a fraud, scam
or bad business practice.*
- **National Council on Aging (NCOA)**
1-571-527-3900, ncoa.org
Find tips on avoiding scams and frauds.
- **Eldercare Locator**
1-800-677-1116, eldercare.acl.gov
*Find services for older adults through this public
service from the U.S. government.*

Contact Information for the Top Credit Reporting Companies

- **Equifax:** **equifax.com**
Place security freeze or fraud alert **1-888-378-4329**
- **Experian:** **experian.com**
Place security freeze or fraud alert **1-888-397-3742**
- **TransUnion:** **transunion.com**
Place security freeze or fraud alert **1-800-916-8800**




Tips to Prevent Medicare Fraud

- 1 If you get a call, text or e-mail asking for your Medicare Number, don't respond. Don't give your Medicare card or Medicare number to anyone except your doctor or people you know should have it.
- 2 Check your Medicare Summary Notices (MSNs) or claims statements carefully. If you see a charge for a service you didn't get or a product you didn't order, it may be fraud. If you suspect fraud, report it at **1-800-633-4227.**
- 3 Guard your Medicare card. Treat it like a credit card!

Fraud Vocabulary: Words to Know

- **Strong Password:** A password that uses a mix of uppercase and lowercase letters, numbers, and symbols, and is not based on personal information or common words.
- **Phishing:** Fake messages or websites that look like they're from trusted companies or organizations designed to trick you into revealing personal information.
- **Security Freeze:** A tool that restricts access to your credit report, making it harder for identity thieves to open accounts in your name.

Hang Up on Gift Card Scams

-  Were you asked to buy a gift card to pay someone?
-  STOP. It's a scam!
-  Gift cards are for gifts, not for payments.

Report the scams to the Federal Trade Commission: **ReportFraud.ftc.gov**

For more information on gift card scams:
ftc.gov/giftcards

Adapted from the Federal Trade Commission.

Section Two

This section has green bars for quick reference. You'll find space to record information, useful checklists and a true/false, multiple choice quiz.

Steps to Get Help	10
Scam Report Log	11
Fraud Prevention Checklist	12
Suspicious Activity Checklist	13
True/False Multiple Choice Quiz ..	14-15
Quiz Answers	16

Steps to Get Help

If you, a loved one or a friend feel you are a victim of fraud, follow these initial steps.

1 Save Proof

Keep e-mails, texts, receipts and any screenshots related to the scam in case investigators need them.

2 Contact Your Financial Institution Immediately

Place protections on your account.

Financial institution contact:

3 Contact Local Law Enforcement

Contact your local police department or sheriff's office for assistance.

Law enforcement contact:

4 File a Report with the FBI's Internet Complaint Center (IC3)

Visit **ic3.gov** to file a report. Ask someone you trust to help you fill out the form.

For more detailed advice, see the FTC's website:
consumer.ftc.gov/articles/what-do-if-you-were-scammed.

Scam Report Log

Make notes here if you think you may be a target of a scam or fraud.

Date and Time: _____

Description of Incident: _____

Amount of Money Involved: _____

Actions Taken: _____

Additional Notes: _____

Date and Time: _____

Description of Incident: _____

Amount of Money Involved: _____

Actions Taken: _____

Additional Notes: _____

Fraud Prevention Checklist

Here's a checklist of things to do to help prevent scams and fraud.

- ☐ **Monitor Financial Statements:** Review your bank and credit card statements regularly to detect unauthorized activity.
- ☐ **Check Your Credit Report:** You have the right to request one free copy of your credit report each year by visiting AnnualCreditReport.com.
- ☐ **Shred Sensitive Documents:** Shred financial statements, bills or other documents containing personal information.
- ☐ **Use Strong Passwords:** Use strong, unique passwords for online accounts. Consider using a password manager. This is a computer program that helps you create, store and remember passwords.
- ☐ **Stay Informed:** Read reliable sources to stay current on common scams and frauds targeting older adults.
- ☐ **Ask For Help:** Seek advice from family members, friends or trusted professionals when making significant financial decisions, or if you suspect fraudulent activity.

Suspicious Activity Checklist

If you check any of these boxes, STOP. Do not respond. Talk to a trusted friend or family member.

- ☐ **Unexpected Requests for Personal Information:** Does the communication request sensitive personal information such as Social Security numbers, bank account details or passwords?
- ☐ **Pressure to Act Quickly:** Is there a sense of urgency or pressure to respond immediately without giving time to think or verify the legitimacy of the request?
- ☐ **Too Good to Be True Offers:** Did you get an unexpected prize notification, lottery win or investment deal that seems too good to be true?
- ☐ **Unsolicited Communication:** Is the communication unsolicited, such as unexpected phone calls, e-mails or text messages from unknown individuals or organizations?
- ☐ **Requests for Payment or Money Transfers:** Is there a request for upfront payment, wire transfers, gift cards, gold or cryptocurrency as part of the offer or request?
- ☐ **Intimidation Tactics:** Does the communication include threats of legal action, arrest or harm if immediate action is not taken?

Scams Quiz

Take this quiz to find out how much you know about senior scams and fraud. Circle your answers. See the next page (p. 16) for answers.

1. Cryptocurrency scams often promise huge returns with little or no risk.
True - False
2. It's safe to click on links or download attachments in e-mails from unknown senders.
True - False
3. Scammers often use technology to make their phone numbers appear legitimate or local.
True - False
4. What is phishing?
 - A. Scams involving fake charities
 - B. Scams targeting seniors specifically
 - C. Scammers pretending to be a trusted entity in order to obtain sensitive information
 - D. Scams offering discounted products
5. It's safe to wire money to someone you've never met in person, even if they claim to be in an emergency situation. **True - False**

6. What is the best way to verify the identity of someone claiming to be from a legitimate organization?
 - A. Ask for personal information
 - B. Call back using a number from the organization's official website or statement
 - C. Give them your financial information
 - D. Trust their word
7. If you've fallen victim to a scam, there's nothing you can do to recover your money or your information. **True - False**
8. What is a common tactic used by scammers to gain trust?
 - A. Threatening language
 - B. Urgency or fear tactics
 - C. Offering something for free
 - D. All of the above
9. You can always trust online reviews and ratings when making a purchase or hiring a service.
True - False
10. It's safe to give out your credit card information to someone who calls claiming to be from your bank's fraud department.
True - False

Quiz Answers

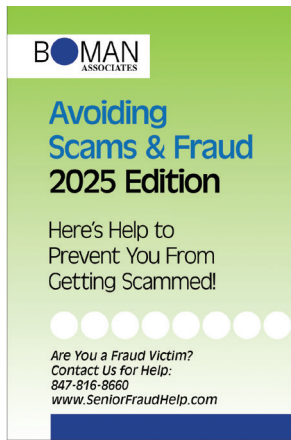
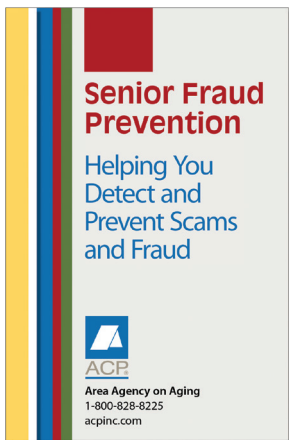
Notes

1. *True*
2. *False*. Clicking on links or downloading attachments from unknown senders can lead to serious problems. When in doubt, don't click a link or open an attachment.
3. *True*
4. *C*
5. *False*
6. *B*
7. *False*. While it can be challenging, there are often steps that victims can take to report the scam, recover lost funds, and protect themselves from further harm, such as contacting their bank or credit card companies and reporting the incident to law enforcement.
8. *D*
9. *False*. While online reviews and ratings can provide helpful insights, they can also be manipulated or faked. It's important to verify information from multiple sources. Be careful when making decisions based solely on reviews.
10. *False*. Banks and financial institutions typically do not request sensitive information like credit card numbers over the phone. This can be a warning sign of a scam.

*Copyright © 2025 American Custom Publishing Corporation,
Libertyville, IL. All rights reserved. The information in this
booklet is current as of April, 2025.*

Custom Full-Color Front and Back Covers Available with Orders of 1000+ Booklets

- Booklet promotes your program while helping protect older adults from scams and fraud.
- Senior-friendly format with larger type and “no-glare” paper stock for easier reading and writing.
- Extensive custom options.
- Available for immediate delivery.



For Prices and Custom Options:

SeniorWellnessGuides.com | info@acpinc.com

800-828-8225