Seniors Against Scams

Steps to Avoiding Scams



PARTICIPANT'S GUIDE





CONTENTS

How Much Do You Know?	
Quiz: How Much Do You Know about Scams?	3
Quiz Answers	4
Top 10 Scams	
Top 10 Scams Targeting Older Adults	6
Avoiding Scams	
Tips for Avoiding Scams	9
Tips for Avoiding Telemarketing Fraud	0
Protecting Your Identity	
Tips for Protecting Your Identity	2
Protecting Yourself and Loved Ones from Scams	4
Protect Your Loved Ones: Signs to Look For	4
If You Are a Victim of a Scam or Financial Abuse	5
Helpful Resources	5
Appendix A	
Top Scams by State	6
Appendix B	
Attorneys General	0

HOW MUCH DO YOU KNOW?

QUIZ HOW MUCH DO YOU KNOW ABOUT SCAMS?



- If there's only a small amount of money involved, it's probably not a scam.
 - True
 - False
- Credit-based scams only occur when someone contacts you.
 - True
 - False
- One way to tell whether a website offers security to help protect your sensitive data is:
 - A small yellow lock appears in the left side of the address bar.
 - Your friends shop on the website all the time and never have a problem.
 - You heard about the website through an online search engine.
 - The security certificate for the site matches the name of the website.
- If you get an email from a federal government agency such as the IRS or the Social Security Administration requesting you to verify your information by clicking a link included in the email, it is safe to do so.
 - True
 - False
- If you think you've been tricked by an internet scam, you should:
 - Report it to the company whose email address or website was forged.
 - b. Change the passwords on all of your accounts.
 - c. Check your financial statements immediately.
 - d. All the above.

HOW MUCH DO YOU KNOW?

- You've just realized that your debit card has been lost or stolen. You should notify your bank:
 - a. Immediately or as soon as you discover your card is missing.
 - b. Within 10 business days.
 - Before your next statement arrives, even if it's weeks later.
- Your credit report may suggest that you've been a victim of identity theft if it shows:
 - You have a credit card, loan, or lease in your name that you know you don't have.
 - A company you never tried to do business with has requested a copy of your credit report.
 - A home address listed that you never lived in/owned.
 - d. All the above.
- The usual suspects who might want to scam me include:
 - a. Strangers
 - b. Family members
 - c. Caregivers
 - d. All the above

Quiz Answers:

- False. No matter how much money is involved, you should always be alert for a scam.
- False. Credit-based scams on the internet are on the rise. It can happen when you are seeking credit loans online as well. Be aware when entering applications online.
- 3. D. The security certificate for the site matches the name of the site. Seeing the yellow lock icon is a good sign because the closed icon lock signifies that the website uses encryption to help protect any sensitive or personal information that you enter. To ensure it is genuine, double click on it to view the security

HOW MUCH DO YOU KNOW?

certificate for the site. The name following "issued to" should match the name of the website. If the name is different, it may be a fake or "spoofed" website. If you are not sure if a certificate is real, do not enter any personal information.

- False. The IRS, other government agencies, and banks will never contact you online to ask for personal information such as account number and Social Security number.
- D. After being tricked by an internet scam, monitor your accounts, alert the proper parties, and change all of your passwords so that no one can access your accounts.
- 6. A. Notify your bank as soon as you discover your card is missing. Under the Electronic Fund Transfer Act, if your debit card is lost or stolen, your maximum liability is limited to \$50 if you notify your bank within 2 business days. Notifying your bank within the 2 to 60-day period will increase your liability for losses up to \$500. After the 60-day period, your bank is not required to reimburse you for unauthorized transfers. Once you report your card lost or stolen, your responsibility will be limited for unauthorized transactions from that point on.
- 7. D. Monitor your credit report frequently to look for warning signs of identity theft. A warning sign of identity theft in a credit report is a credit card, a loan, or lease in your name that you know nothing about. Having one of these signs show up on your report indicates that someone has learned enough information about you to steal your identity. Also pay close attention to the inquiries section of the report that shows who has requested a copy of your credit history report. Scammers can falsely claim to represent a company with a lawful right to obtain credit reports and then use the information to commit fraud.
- 8. D. Older adults need to be careful of all the individuals in their life as potential financial abusers. This does not mean that you need to isolate yourself from those who care about you, but it does mean you need to be alert to the motivations and actions of those around you. Monitor your accounts and limit family members with access to your accounts.

TOP 10 SCAMS



TOP 10 SCAMS TARGETING OLDER ADULTS

- 1. Social Security Impersonation Scam: The are several variations to the Social Security impersonation scam. They all involve a scammer calling and asking for personal information including Social Security number, date of birth, mother's maiden name, and/or bank account. Scammers are always looking for ways to obtain Social Security numbers. It is important to note that Social Security will rarely call you and, in those instances, the caller will provide their telephone number and extension. Also, Social Security will not send an email requesting personal information.
- 2. Romance Scams: Online dating has become another area for scamming for older adults. Scammers will create fictitious characters to trick older adults into developing a romantic relationship. Once a connection has been established, the scammer will create a story where they need money from the victim or need travel expenses covered to visit the victim. The scammer may also send a check to the victim to deposit or send a package on behalf of the scammer. However, the victim is unknowingly participating in a money laundering scam or shipping stolen merchandise. Scammers are also using social media to create a presence and credibility.
- 3. Telemarketing/Robocalls Scams: Perhaps the most common scam is when scammers use fake telemarketing calls. With no face-to-face interaction, and no paper trail, these scams are incredibly hard to trace. Once a successful deal has been made, the buyer's name is then shared with similar scammers looking for easy targets, sometimes defrauding the same person repeatedly.

TOP 10 SCAMS

In 2003, Congress created the Do-Not-Call registry to prevent telemarketers from calling all day. However, telemarketers have developed robocalls to get around the registry.

Robocalls include pre-recorded messages that are activated when an individual picks up the phone. The most common robocalls are the IRS impersonation scams where scammers will modify their numbers to make it look like the IRS is calling. Scammers are increasingly "spoofing" state and local numbers to trick people.

- 4. Investment Schemes: From pyramid schemes like Bernie Madoff (which included a number of older adult victims) to a fabled Nigerian prince looking for a partner, to claim inheritance money, to complex financial products that many economists do not even understand, investment schemes have long been a successful way to take advantage of older adults.
- 5. Tech Support/Internet Fraud: Internet scams are all over the web. Pop-up browser windows simulate virus-scanning software that fools victims into either downloading the fake anti-virus program or an actual virus that will allow the scammer to access the user's information on the computer. Scammers may also call you and claim to be from a well-known company or tech support. They will try to sell you anti-virus protection programs and ask for a credit card number. They may also ask for your computer password to gain access to your computer where they will install malware that provides long-term access to your personal and financial information on your computer.
- 6. Funeral/Cemetery Scams: There are two types of scams targeting older adults. In the first approach, scammers read obituaries and call or attend the funeral of a stranger to take advantage of the widow or widower. The scammer will claim that the deceased had an outstanding debt with them. In the other approach, funeral homes will add unnecessary charges to the bill for individuals or families who seem unaware of the costs associated with funeral services. The funeral home may also use hard pressure tactics on the family to pay for more expensive services than necessary.

TOP 10 SCAMS

- 7. Medicare/Medicaid Fraud: Most older adults, age 65 and older, qualify for Medicare, and can enroll in a variety of Medicare plans including Medicare Advantage plans, Medicare prescription drug plans or Medicare supplement plans. Scammers will prey on those who may be confused about Medicare and Medicaid coverage by posing as health insurance agents. In this role, scammers will ask older adults to provide their personal and financial information over the phone where the scammer will then create an account under that individual's name and apply for credit cards.
- 8. Home Repair/Contractor Scams: Scammers will drive around the neighborhood seeking homes occupied by older adults that may need repairs. Once the victim has been targeted, the scammer will approach the home and provide the victim with an affordable quote for the proposed work. Once the victim agrees to the job, the scammer instructs the victim to pay for the work either in cash or a check written to the scammer. However, the scammer will not complete the work or provide sloppy repairs.
- 9. Sweepstakes and Lottery Scams: Scammers inform an older adult that they have won the lottery or sweepstakes of some kind and need to make a payment to unlock the prize. Often, older adults will be sent a check that they can deposit in their bank account, knowing that while it shows up in their account immediately, it will take a few days before the (fake) check is rejected. During that time, the scammers will quickly collect money for supposed fees or taxes on the prize, while the victim has the "prize money" removed from his or her bank account as soon as the check bounces.
- 10.The Grandparent Scam: The Grandparent Scam is so simple and underhanded because it uses one of older adult's most reliable assets, their hearts. Scammers will place a call to an older adult and when the line is picked up, they will say something along the lines of: "Hi Grandma, do you know who this is?" When the unsuspecting grandparent guesses the name of the grandchild the scammer most sounds like, the scammer has established a fake identity. Once "in" the fake grandchild will usually ask for money to solve some unexpected financial problem, to be paid via Western Union or MoneyGram, which don't always require identification to collect.

AVOIDING SCAMS



TIPS FOR AVOIDING SCAMS

- Be aware that you are at risk from strangers and from persons closest to you.
- Do not isolate yourself stay involved with family, friends, and community activities.
- 3. Always tell salespeople that come to your door or call you on the phone: "I never buy from (or give to) anyone who calls or visits me unannounced. Please send me your information in writing."
- Shred all receipts with your credit card number.
- Sign up for the "Do Not Call" list (www.donotcall.gov) to prevent telemarketers from calling and take yourself off multiple mailing lists.
- Use direct deposit for benefits checks to prevent checks from being stolen in the mail.
- Never give your credit card, banking, Social Security, Medicare, or personal information over the phone unless you initiated the call.
- 8. Be skeptical of all unrequested offers and thoroughly do your research if you are seeking any type of services. Also, be sure to get references when possible.

AVOIDING SCAMS

Tips for Avoiding Telemarketing Fraud

It is very difficult to get your money back if you have been cheated over the telephone. Before you buy anything by telephone, remember:

- Don't buy from an unfamiliar company. Reasonable businesses understand that you want more information about their company and are happy to comply.
- Always ask for and wait until you receive written material about any offer or charity. If you receive brochures about costly investments, ask a trusted source to review them. Unfortunately, beware, not everything written down is true.
- Always check out unfamiliar companies. Check them with your local consumer protection agency, Better Business Bureau, state attorney general, or other watchdog groups. Unfortunately, not all bad businesses can be identified through these organizations.
- Obtain a salesperson's detailed information. Ask for their name, business identity, telephone number, street address, mailing address, and a business license number before you begin business. Scammers will provide false names telephone numbers, addresses, and business license numbers. Verify the accuracy of these items.
- Find out where the money will go. Before you give money to a charity or make an investment, find out what portion of the money is paid in commissions and what portion goes to the charity or investment.



AVOIDING SCAMS

- Look for a guarantee. Before you send money, ask yourself a simple question "What guarantee do I really have that this salesperson will use my money in the manner we agreed upon?"
- Do not pay in advance for services. Pay for services only after they are delivered.
- Be cautious of companies that want to send a messenger to your home. Some fraudulent companies want to send someone to pick up money, claiming it is part of their service to you. In reality, they are taking your money without leaving any trace of who they are or where they can be reached.
- Always take your time making a decision. Reasonable companies
 will not pressure you to make a snap decision. Be sure to discuss
 big investments offered over the telephone with a trusted source. It
 is never rude to think about an offer.
- Do not pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.
- If you do not understand, do not respond. Never respond to an offer you do not understand thoroughly.
- Know who you are dealing with. Never send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or Social Security numbers to unfamiliar companies or unknown individuals.
- Realize that your information is being shared. Your personal information is often brokered to telemarketers through third parties.
- Be cautious of help with losses. If you have been victimized once, be wary of individuals who call offering to help you recover your losses for a fee paid in advanced.
- Always report fraud. If you have information about fraud, report it immediately to state, local, or federal law enforcement agencies.

Remember: If it sounds too good to be true, it probably is!

TIPS FOR PROTECTING YOUR IDENTITY

Many people do not realize how many ways identity thieves can obtain personal information, nor how easy it is for them to do it. Here is how to protect yourself:

- Monitor your bank and credit card statements. Check your accounts regularly to catch any purchases made on your credit card by unknown individuals. The same goes for cash withdrawals.
- Do not fall for internet scams. Identify internet scams and do not respond to any attempts. Do not click on links in emails from unknown senders.
- Beware of telephone scams. Never give out personal information over the phone to someone who claims to represent your bank, credit card company, or other organizations.
- Be careful with your mail. Identity thieves may steal your mail
 right out of the mailbox in order to obtain your personal identifying
 information. To reduce this threat, do not let mail accumulate in your
 mailbox for a long time. If you are planning an extended leave of
 absence, have the post office hold your mail for you. When sending
 out sensitive mail, consider dropping it off at a secure collection box
 at the post office.
- Be careful when using account information in public. Be sure to cover the keypad when entering your PIN or filling out forms with personal information on it in private. Do not give out credit card information over the phone in a public place. Place these types of calls in a private setting.
- If you think you have been a victim of identity theft:
 - Contact your bank(s) and credit card companies immediately.
 - File a report with the police. The policy may not be able to do much, but the police report is valuable when working with companies to clear up the issue.

- > Put out a fraud alert to the credit-reporting agencies:
- Experian:
 1-888-EXPERIAN (1-888-397-3742)
 https://www.experian.com/ncaconline/fraudalert
- Equifax:
 1-888-766-0008
 https://www.equifax.com/personal/credit-report-services/
- Transunion:
 1-800-680-7289
 https://www.transunion.com/fraud-alerts



Protecting Yourself and Loved Ones from Scams

Financial exploitation and scams are serious concerns. They deprive older adults of their hard-earned assets and retirement savings. Making matters worse, older adults with fixed incomes and limited earning potential, are rarely able to recover financially.

Everyone is subject to scams; however older adults are identified as easy marks and are frequently targeted by scammers. The scammers may be strangers preying on older adults who may be lonely, isolated, confused, or desperate for cash or attention. There are also instances of financial abuse by family members where the victim is pressured into giving money or assets to a family member.

It is important to be on the lookout, not only to protect your assets, but also to help you identify possible scams against yourself, family members, and friends.

Protect Your Loved Ones: Signs to Look For

- A large amount of money missing from their bank account(s).
- Numerous withdrawals of smaller amounts, such as \$100 at a time.
- A large check written to someone you do not know.
- A change in their power of attorney or the beneficiaries on their insurance or investment accounts.
- Bouncing checks or unpaid bills where they should be enough money in their bank account to cover their needs.
- Unusual or unnecessary purchases, such as buying new golf clubs or a diamond bracelet.
- Unnecessary home repairs.
- Becoming close with a younger or inappropriate individual(s).
- A caregiver who becomes overly interested in the older adult's finances or who will block access to the older adult.
- Older adult suddenly appears confused, unkempt, or fearful.
- Piled up sweepstakes mailings, magazine subscriptions, or "free gifts."

If You Are a Victim of a Scam or Financial Abuse

Do not be afraid or embarrassed to talk about it with someone you trust. You are not alone, and there are people who can help. Doing nothing could only make the situation worse. Keep handy the phone numbers and resources you can refer to, including the local police, your bank (if money has been taken from your accounts), and Adult Protective Services.

To obtain the contact information for Adult Protective Services in your area, call the Eldercare Locator, a government-sponsored national resource line, at 1-800-677-1116 or visit their website at https://eldercare.acl.gov/Public/Index.aspx.

Helpful Resources

- Administration on Aging Legal Assistance Programs Legal Services for the Elderly Program https://acl.gov/programs/legal-help/legal-services-elderly-program
- Better Business Bureau Senior Fraud Programs 804-780-2222 https://www.bbb.org/richmond/programs-services/bbb-educationoutreach/senior-fraud-program/
- Consumer Financial Protection Bureau Office of Financial Protection for Older Americans https://www.consumerfinance.gov/practitioner-resources/ resources-for-older-adults/
- National Center on Elder Abuse https://eldermistreatment.usc.edu/national-center-on-elder-abusencea-usc/
- National Center on Law and Elder Rights https://ncler.acl.gov/
- Senior Medicare Patrol https://acl.gov/programs/protecting-rights-and-preventing-abuse/ senior-medicare-patrol-smp
- 7. Social Security Fraud Hotline
- Supporting Adult Protective Services (APS)
 https://acl.gov/programs/elder-justice/supp orting-adult-protective-services

TOP SCAMS BY STATE

These scams are based on calls into the Aging Committee's Fraud Hotline in 2018.

Alabama

- Elder Financial Abuse
- IRS Impersonation Scam
- Social Security Impersonation Scam
- 4. Romance Scam
- Jamaican Lottery Scam

Alaska

- Unsolicited Phone Calls
- Government Grant Scam

Arizona

- Computer Tech Support Scam
- 2. IRS Impersonation Scam
- Unsolicited Phone Calls
- Elder Financial Abuse
- Social Security Impersonation Scam

Arkansas

- IRS Impersonation Scam
- Sweepstakes Scam
- Inheritance Scam
- Health-Related Scam

California

- Elder Financial Abuse
- Romance Scam
- 3. IRS Impersonation Scam
- Computer Tech Support
 Scam
- Sweepstakes Scam

Colorado

- Elder Financial Abuse
- 2. IRS Impersonation Scam
- Grandparent Scam
- Romance Scam
- Social Security Impersonation Scam

Connecticut

- Romance Scam
- IRS Impersonation Scam
- Identity Theft
- 4. Impending Law Suits Scam
- Social Security Impersonation Scam

Delaware

- Charity Scam
- Computer Tech Support Scam
- Grandparent Scam
- 4. Identity Theft

Florida

- Unsolicited Phone Calls
- Grandparent Scam
- Computer Tech Support
 Scam
- IRS Impersonation Scam
- Elder Financial Abuse

Georgia

- 1. Charity Scam
- 2. Elder Financial Abuse
- 3. Jamaican Lottery Scam
- Timeshare Scam
- Romance Scam

Hawaii

- Grandparent Scam
- IRS Impersonation Scam
- Romance Scam
- Sweepstakes Scam

Idaho

- Social Security
 Impersonation Scam
- Unclaimed Property Scam
- 3. IRS Impersonation Scam
- Jamaican Lottery Scam
- Unsolicited Phone Calls

Illinois

- Elder Financial Abuse
- Sweepstakes Scam
- Grandparent Scam
- 4. IRS Impersonation Scam
- Unsolicited Phone Calls

Indiana

- Romance Scam
- IRS Impersonation Scam
- 3. Identity Theft
- Sweepstakes Scam
- Mortgage Fraud

lowa

- 1. Jamaican Lottery Scam
- Grandparent Scam
- Impending Law Suit Scam
- Romance Scam

Kansas

- Sweepstakes Scam
- Elder Financial Abuse
- Jamaican Lottery Scam
- 4. Unsolicited Phone Calls

Kentucky

- Grandparent Scam
- Elder Financial Abuse
- Romance Scam

Louisiana

- Consumer Complaints
- IRS Impersonation Scam
- Romance Scam

Maine

- 1. IRS Impersonation Scam
- 2. Unsolicited Phone Calls
- Computer Tech Support Scam
- Social Security Impersonation Scam
- Grandparent Scam

Maryland

- IRS Impersonation Scam
- Grandparent Scam
- Computer Tech Support Scam
- 4. Debt Collection Scam
- Romance Scam

Massachusetts

- 1. Unsolicited Phone Calls
- Computer Tech Support Scam
- 3. Grandparent Scam
- IRS Impersonation Scam
- Impending Law Suit Scam

Minnesota

- IRS Impersonation Scam
- Identity Theft
- Impending Law Suit Scam
- Sweepstakes Scam
- Investment Fraud

Mississippi

- Sweepstakes Scam
- 2. Romance Scam

Missouri

- Computer Tech Support
 Scam
- Elder Financial Abuse
- Jamaican Lottery Scam
- Identity Theft
- Romance Scam

Montana

- 1. Elder Financial Abuse
- Unsolicited Phone Calls

Michigan

- Computer Tech Support
 Scam
- 2. Romance Scam
- IRS Impersonation Scam
- Investment Fraud
- Unsolicited Phone Calls

Rhode Island

- Elder Financial Abuse
- IRS Impersonation Scam
- Sweepstakes Scam
- Unsolicited Phone Calls

South Carolina

- Consumer Complaints
- Computer Tech Support Scam
- IRS Impersonation Scam
- Impending Law Suit Scam
- Romance Scam

South Dakota

- Computer Tech Support
 Scam
- 2. Impending Law Suit Scam
- Identity Theft
- IRS Impersonation Scam

Tennessee

- Romance Scam
- Computer Tech Support Scam
- Grandparent Scam
- Sweepstakes Scam
- 5. Unsolicited Phone Calls

Texas

- 1. IRS Impersonation Scam
- 2. Sweepstakes Scam
- 3. Romance Scam
- Elder Financial Abuse
- Identity Theft

SECTION TITLE1

Utah

- IRS Impersonation Scam
- 2. Bank Fraud
- 3. Elder Financial Abuse
- Romance Scam
- Unsolicited Phone Calls

Vermont

1. IRS Impersonation Scam

*Since the Fraud Hotline did not receive any calls from consumers in Vermont between 2017 and 2018, this list is based on call data from 2015 and 2016.

Virginia

- Sweepstakes Scam
- Computer Tech Support Scam
- Grandparent Scam
- Identity Theft
- IRS Impersonation Scam

Washington

- IRS Impersonation Scam
- Grandparent Scam
- Identity Theft
- 4. Inheritance Scam
- Romance Scam

West Virginia

- Elder Financial Abuse
- 2. IRS Impersonation Scam

Wisconsin

- 1. Can You Hear Me? Scam
- 2. Computer Tech Support Scam
- Sweepstakes Scam
- Health-Related Scam
- Grandparent Scam

Wyoming

1. Romance Scam

Source: United States Senate Special Committee on Aging (2019). Fighting Fraud: Senate Aging Committee Identified Top 10 Scams Targeting Our Nation's Seniors. Retrieved from: https://www.aging.senate.gov/fraudbook/index.html.

APPENDIX B

ATTORNEYS GENERAL

Alabama

(334) 242-7300

Alaska

(907) 269-5100

Arizona

(602) 542-5025

Arkansas

(800) 482-8982

California

(916) 445-9555

Colorado

(720) 508-6022

Connecticut (860) 808-5400

Delaware

(302) 577-8600

District of Columbia

(202) 442-9828

Florida

(850) 414-3300

Georgia

(404) 656-3300

Hawaii

(808) 586-1500

Idaho

(208) 334-2400

Illinois

(312) 814-3000

Indiana

(317) 232-6330

lowa

(515) 281-5044

Kansas

(785) 296-3751

Kentucky

(502) 696-5300

Louisiana

(225) 326-6465

Maine

(207) 626-8800

Maryland

(410) 576-6300

Massachusetts

(617) 727-2200

Michigan

(517) 373-1110

Minnesota

(651) 296-3353

Mississippi

(601) 359-3680

Missouri

(573) 751-3321

Montana

(406) 444-2026

Nebraska

(402) 471-2682

Nevada

(702) 486-3132

New Hampshire

(603) 271-3658

New Jersey

(609) 292-8740

, ,

New Mexico

(SOS) 490-4060

New York

(518) 776-2000

APPENDIX B

North Carolina

(919) 716-6400

North Dakota

(701) 328-2210

Ohio

(614) 466-4986

Oklahoma

(405) 521-3921

Oregon

(503) 378-4400

Pennsylvania (717) 787-3391

Rhode Island

(401) 274-4400

South Carolina

(803) 734-3970

South Dakota (605) 773-3215

Tennessee

(615) 741-3491

Texas

(512) 463-2100

Utah

(800) 244-4636

Vermont

(802) 828-3173

Virginia

(804) 786-2071

Washington

(360) 753-6200

West Virginia (304) 558-2021

Wisconsin

(608) 266-1221

Wyoming

(307) 777-7841

Puerto Rico

(787) 721-2900

US Virgin Islands

(340) 774-5666

Source: United States Senate Special Committee on Aging (2019). Fighting Fraud: Senate Aging Committee Identified Top 10 Scams Targeting Our Nation's Seniors. Retrieved from: https://www.aging.senate.gov/fraudbook/index.html.







251 18th Street South, Suite 500 Arlington, VA 22202 571-527-3900 ncoa.org