PARTICIPANT HANDBOOK

Savvy Saving Seniors®

Steps to Avoid Scams

BANK OF AMERICA

nco national council on aging®

CONTENTS

How Much Do You Know?

QUIZ: How Much Do You Know About Scams?

1. **If there's only a small amount of money involved, it's probably not a scam.**
   a. True
   b. False

2. **Credit-based scams only occur when someone contacts you.**
   a. True
   b. False

3. **One way to tell whether a website offers security to help protect your sensitive data is:**
   a. A small yellow lock appears in the left side of the web address bar.
   b. Your friends shop on the website all the time and never have a problem.
   c. You heard about the website through an online search engine.
   d. The security certificate for the site matches the name of the website.

4. **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.**
   a. True
   b. False

5. **If you think you've been tricked by an internet scam, you should:**
   a. 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 of the above.

6. **You realize your debit card has been lost or stolen. You should notify your bank:**

   a. Immediately as soon as you discover your card is missing.

   b. Within 10 business days.

   c. Before your next statement arrives, even if it is weeks later.

7. **Your credit report may suggest you've been a victim of identity theft if it shows:**

   a. You have a credit card, loan, or lease in your name that you know you don't have.

   b. A company you never tried to do business with has requested a copy of your credit report.

   c. A home address is listed that you don't recognize.

   d. All of the above.

8. **The usual suspects who might want to scam me include:**

   a. Strangers

   b. Family members

   c. Caregivers

   d. All of the above

Quiz Answers:

1. **False.** No matter how much money is involved, you should always be alert for a scam.

2. **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 website. 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 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.

4. **False.** The IRS, other government agencies, and banks will never contact you online to ask for personal information, such as an account number or your Social Security number.

5. **D.** After being tricked by an internet scam, monitor your accounts, alert the proper parties, and change all of your passwords, so 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 two business days. Notifying your bank within the three-day 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, 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 people in their life as potential financial abusers. This does not mean 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.

The Dirty Dozen: Top 12 Scams

Top 12 Scams Targeting Older Adults

1. **Social Security Impersonation Scams:** Things are not always what they seem, and any unsolicited contact from the Social Security Administration should be met with scrutiny. There are several variations to the Social Security impersonation scam. They usually involve requests for personal information, such as your Social Security number, date of birth, mother's maiden name, and/or bank account information. 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 for you to verify and call back. Also, Social Security will never send an email requesting personal information.

7 Social Security Scam Warning Signs

The Federal Trade Commission notes most Social Security impersonation scam calls share seven common warning signs:

1. Calls that are unexpected
2. Contact outside of business hours or on weekends
3. Claims of problems or criminal activity with your Social Security number
4. Aggressive threats if you don't comply
5. Demands for immediate payment or odd method of payment
6. Promises of additional benefits
7. Doctored credentials or phony documents

2. **Romance Scams:** There is no love lost for scammers who take advantage of older adults via online dating. 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 may be unknowingly participating in money laundering or shipping stolen merchandise. Scammers are also using social media to add credibility to their characters.

3. **Telemarketing/Robocall Scams:** The phone is still scammers' favorite weapon of choice when targeting older adults, and perhaps the most prevalent scam involves 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 may then be shared with similar scammers looking for easy targets, sometimes defrauding the same person repeatedly. In 2003, Congress created the National Do Not Call Registry to prevent telemarketers from calling all day. However, telemarketers have developed robocalls to get around the registry. Robocalls include prerecorded messages that are activated when an individual picks up the phone. The most common robocalls are IRS impersonation scams, where scammers will modify how their numbers appear on caller ID to make it look like the IRS is calling — a tactic called spoofing.

$380 Million Stolen

In the first half of 2022 alone, the Federal Trade Commission says phone scams stole an estimated $380 million from Americans.

4. **Investment Schemes:** From Ponzi schemes like the one made famous by Bernie Madoff (who defrauded thousands of people, including celebrities, out of billions of dollars) to emails from a fabled Nigerian prince looking for a partner to claim his inheritance money to complex financial products that many economists do not even understand, investment schemes have long been a successful method to take advantage of older adults. Remember: If it sounds too good to be true, it probably is!

5. **Tech Support/Internet Fraud:** Internet scams are a dime a dozen, but they could cost you dearly if you aren't careful. Pop-up windows that simulate virus-scanning software fool victims into either downloading a fake antivirus 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 antivirus

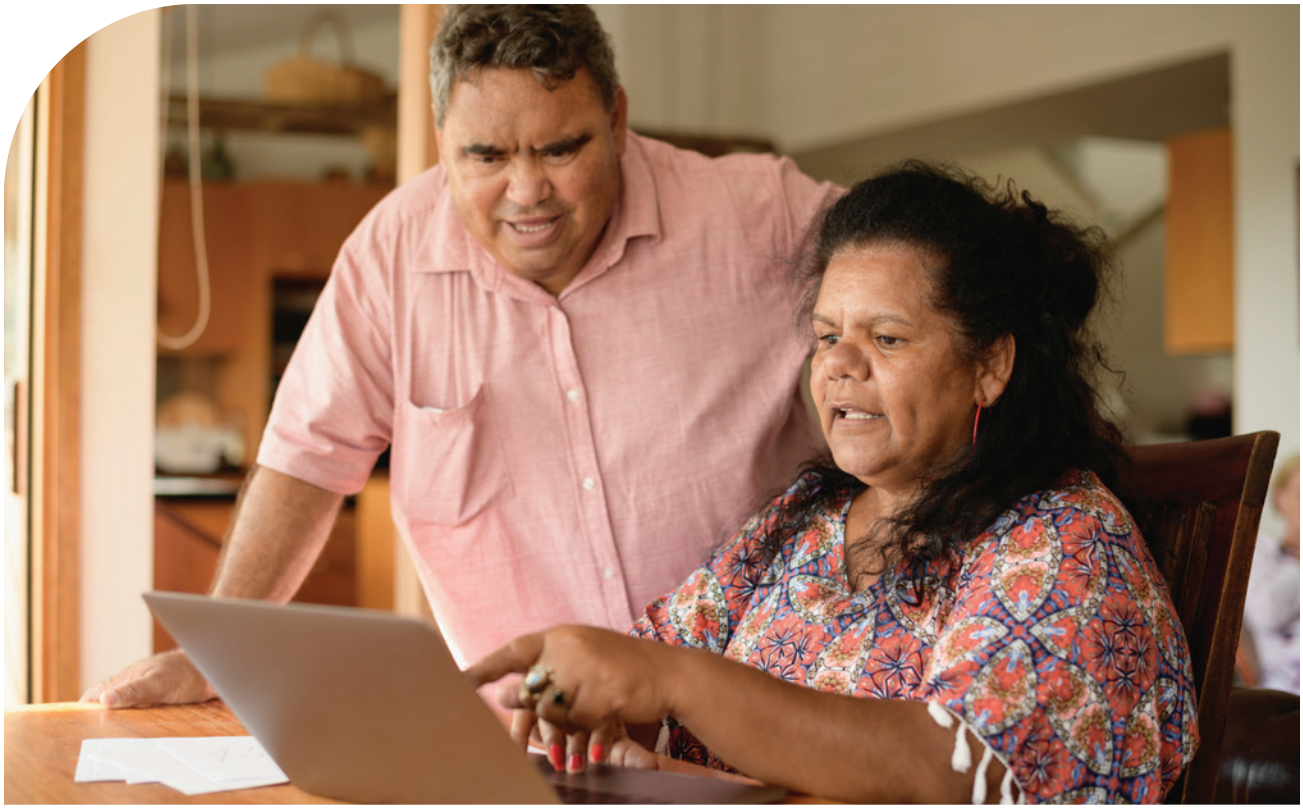
protection programs and ask for a credit card number. They may also ask for your computer password to gain access to your computer. Once in, they can install malware that provides long-term access to your personal and financial information on your computer.

6. **Spousal Death/Funeral Scams:** Unfortunately, scammers see tragedy as an opportunity to hurt rather than help. And there are two common types of scams they employ to exploit older adults dealing with the death of a spouse or loved one. In the first approach, scammers read obituaries and then call or attend the funeral to take advantage of the widow or widower. The scammer will claim the deceased had an outstanding debt that must be paid. 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 are necessary.

7. **Medicare/Medicaid Fraud:** Most older adults age 65+ qualify for Medicare and can enroll in a variety of Medicare plans, such as Medicare Advantage plans, Medicare prescription drug plans, or Medicare supplement plans. Scammers will prey on those who may need assistance with 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. Once obtained, scammers will then use that information to create accounts and apply for credit cards.

8. **Home Repair/Contractor Scams:** Knock, knock. Who's there? A scammer. Scammers will drive around neighborhoods seeking homes that may need repairs and are occupied by older adults. Once the victim has been targeted, the scammer will approach the home and provide an affordable quote for the proposed work. Once the victim agrees to the job, the scammer instructs them to pay for the work either in cash or a check written to the scammer. However, the scammer will either not complete the work or provide sloppy repairs. And it is often impossible to locate them afterward to right the wrong.

9. **Sweepstakes and Lottery Scams:** Everyone dreams of winning it big, but you may find yourself in the very real nightmare of losing big if it turns out to be a scam. Typically, scammers will inform an older adult that they have won the lottery or a sweepstakes of some kind but need to make a payment to unlock the prize. Often, older adults will receive 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 adults' most reliable assets: their hearts. Scammers will place a call to an older adult posing as a grandchild. They may say, "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 and will usually ask for money to solve some unexpected financial problem. They typically ask to be paid via Western Union or MoneyGram, through a friend, or by some other odd payment method.

11. **Employment Scams:** Whether looking to keep their minds or bodies active during retirement or to bolster their finances on limited incomes, many older adults are in the market for a job. And scammers try to take advantage of older adults seeking work in several ways. They may promote easy work-from-home jobs and tell you that all you need to do is pay for training or a starter kit. It's only after you pay that you find out there is no real job. In 2020, the Federal Trade Commission identified a similar scam on LinkedIn in which fake companies would send offers for a high-paying job. The catch? You would first have to send a large deposit to secure the interview. Some scammers are also posting jobs in an effort to gain your personal information after they pretend to hire you. This is one of the ways scammers use their oldest trick in the book—"phishing" for information.

Because their emails, text messages, voicemail messages, and even voice calls are not authenticated and can't be traced, they feel freedom to mimic trusted brands, including potential employers, in their communications. Sophisticated scammers are very skilled at creating spoof email templates and websites, like companies you may visit for a job, that are almost indistinguishable from the real thing, right down to how the website address appears. You may think you're receiving a credible message from an employer, and if you're not paying close attention, you might not notice the trickery until it's too late. That's why knowing how to spot phishing communications is the first step in keeping sensitive personal information safe from thieves. Some telltale signs of a phishing email or text message include:

- Offers that seem too good to be true
- High-pressure sales pitches that stress urgency
- Alerts that there's a problem with your account (e.g., suspicious activity or outdated payment information)
- Shortened or misspelled links
- Emails that don't address you by name
- Messages with poor grammar and spelling
- Direct requests or demands for payment
- Requests to confirm personal information

12. **COVID-19 Scams:** Last but certainly not least, scammers saw the COVID-19 pandemic and all its repercussions as an opportunity to pounce. By June 2021, the Federal Trade Commission had already logged more than 500,000 consumer complaints related to COVID-19 and stimulus payments. And 73% of those complaints involved fraud and identity theft. Examples of COVID-19 scams include companies fraudulently selling so-called miracle cures, but these products are not backed by medical evidence, are not FDA approved, and could cause more harm. Likewise, scammers may call older people to offer vaccination in exchange for money or personal information, so keep in mind you can get vaccinated against COVID-19 at no cost, without providing your banking information, and from a variety of reputable sources. There have also been reports of older adults being offered free COVID-19 tests or supplies from people claiming to be from Medicare or the Department of Health and Human Services. These scammers then use the victim's Medicare information to submit false health care claims.

Avoiding Scams

Tips to Avoid Scams

- Be aware that you are at risk from both strangers and the people closest to you.
- Do not isolate yourself. Stay involved with family, friends, and community activities.
- Always tell salespeople who 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 documents with your credit card number.
- Sign up for the National Do Not Call Registry at *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 to a verified number.
- 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.

Power in a Pause

There is power in a pause. Most scammers push a sense of urgency to get you to share your personal or financial information quickly before you realize their request is illegitimate. If you can practice pushing pause every time your personal or financial information is requested, you can protect yourself from a variety of scams. Any legitimate organization will be OK with you contacting them directly via a verified line of communication.

Tips to Avoid 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 will want more information about their companies 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. Beware, not everything written down is true.
- **Always check out unfamiliar companies.** Check them with your local consumer protection agency, the Better Business Bureau, your state attorney general, or another watchdog group. 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, so 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.
- **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 and completed correctly.
- **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, they are 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 already been victimized once, be wary of individuals who call offering to help you recover your losses for a fee paid in advanced.

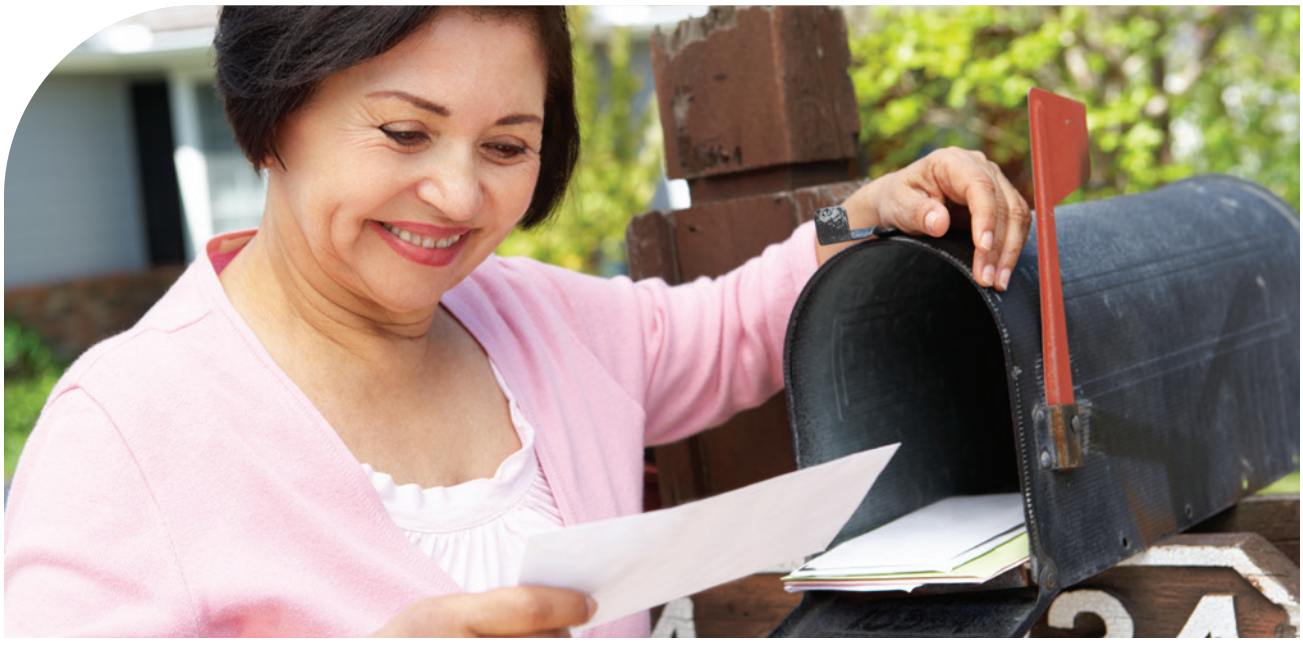
Remember: If it sounds too good to be true, it probably is!

Protecting Your Identity

Tips to Protect 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.



- **Mind 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 cover your paper when filling out forms with personal information on it in public. 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 all of your banks and credit card companies immediately.
  - File a report with the police. The police 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:
      888-EXPERIAN (888-397-3742)
      Experian.com/fraud/center.html
    - Equifax:
      888-766-0008
      Equifax.com/Personal/Credit-Report-Services/
    - TransUnion:
      800-680-7289
      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 in need of 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.

Financial scams often go unreported or can be tough to prosecute, so they're viewed as a low-risk crime. However, they're devastating to many older adults and can leave them with limited ability to recover their losses. 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: Know the Signs

- A large amount of money is missing from their bank account(s).
- There are numerous withdrawals of smaller amounts, such as $100 at a time or a large check was written to someone you do not know.
- There has been a change in their power of attorney or the beneficiaries on their insurance or investment accounts.
- There are bouncing checks or unpaid bills when there 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, can be a red flag.
- Unnecessary home repairs could mean they have been scammed.
- Becoming close with a younger or inappropriate individual(s) may be cause for alarm.
- A caregiver who becomes overly interested in the older adult's finances or who will block access to the older adult may be up to no good.
- Older adults who suddenly appear confused, unkempt, or fearful may be a victim of a scam.
- Piled up sweepstakes mailings, magazine subscriptions, or "free gifts" could be signs of scams.

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 800-677-1116 or visit its website at *Eldercare.acl.gov*.

Helpful Resources

- Administration for Community Living's Legal Services for Older Americans Program
  acl.gov/Programs/Legal-Help/Legal-Services-Elderly-Program
- Better Business Bureau Resources for Older Adults
  804-780-2222
  bbb.org/all/older-adult-resources
- Consumer Financial Protection Bureau
  ConsumerFinance.gov/Consumer-Tools/Educator-Tools/Resources-for-Older-Adults/
- National Center on Elder Abuse
  ncea.acl.gov
- National Center on Law and Elder Rights
  ncler.acl.gov
- Senior Medicare Patrol
  smpResource.org
- Social Security Fraud Reporting
  800-269-0271
  oig.ssa.gov
- Adult Protective Services Locator by State
  ncea.acl.gov/Resources/State.aspx

Appendix A

Top Scams Reported by State

Knowledge is power, and knowing which scams are happening most often in your area may help you recognize them more readily. Below are the top reported scams targeting older adults in each state based on calls to the U.S. Senate Special Committee on Aging's fraud reporting hotline in 2021.

Alabama

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Alaska

- Identity Theft
- Business Impersonation and Shopping Scams
- Health Care Scams
- Sweepstake and Lottery Scams

Arizona

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams

- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Arkansas

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud

California

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Colorado

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Connecticut

- Government Imposter Scams
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Delaware

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Health Care Scams
- Sweepstake and Lottery Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Florida

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Georgia

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Romance Scams
- Financial Services Impersonation and Fraud

Hawaii

- Government Imposter Scams
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud

Idaho

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Health Care Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud

Illinois

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams\

Indiana

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams

- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Iowa

- Government Imposter Scams
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud

Kansas

- Government Imposter Scams
- Business Impersonation and Shopping Scams
- Health Care Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Kentucky

- Government Imposter Scams
- Business Impersonation and Shopping Scams
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud

Louisiana

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Health Care Scams
- Sweepstake and Lottery Scams
- Romance Scams
- Financial Services Impersonation and Fraud

Maine

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Maryland

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams

- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Massachusetts

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Michigan

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Minnesota

- Government Imposter Scams
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Mississippi

- Government Imposter Scams
- Health Care Scams
- Romance Scams
- Financial Services Impersonation and Fraud

Missouri

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud

Montana

- Government Imposter Scams
- Business Impersonation and Shopping Scams

Nebraska

- Government Imposter Scams
- Business Impersonation and Shopping Scams
- Health Care Scams
- Sweepstake and Lottery Scams
- Romance Scams
- Financial Services Impersonation and Fraud

Nevada

- Government Imposter Scams
- Health Care Scams
- Sweepstake and Lottery Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

New Hampshire

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Person-in-Need and Grandparent Scams

New Jersey

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

New Mexico

- Government Imposter Scams
- Identity Theft
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

New York

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams

- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

North Carolina

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud

North Dakota

- Business Impersonation and Shopping Scams
- Health Care Scams

Ohio

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Oklahoma

- Government Imposter Scams
- Business Impersonation and Shopping Scams
- Health Care Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Oregon

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Pennsylvania

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams

- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Rhode Island

- Government Imposter Scams
- Business Impersonation and Shopping Scams
- Health Care Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

South Carolina

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud

South Dakota

- Government Imposter Scams
- Business Impersonation and Shopping Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud

Tennessee

- Government Imposter Scams
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Texas

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Utah

- Government Imposter Scams
- Business Impersonation and Shopping Scams
- Health Care Scams
- Romance Scams
- Financial Services Impersonation and Fraud

Vermont

- Government Imposter Scams
- Sweepstake and Lottery Scams

Virginia

- Government Imposter Scams
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Washington

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

West Virginia

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Health Care Scams
- Sweepstake and Lottery Scams
- Romance Scams

Wisconsin

- Government Imposter Scams
- Identity Theft
- Business Impersonation and Shopping Scams
- Robocalls and Unsolicited Calls
- Health Care Scams
- Sweepstake and Lottery Scams
- Tech Support and Computer Scams
- Romance Scams
- Financial Services Impersonation and Fraud
- Person-in-Need and Grandparent Scams

Wyoming

- Government Imposter Scams
- Health Care Scams
- Tech Support and Computer Scams
- Romance Scams

Source: U.S. Senate Special Committee on Aging (2021). Fighting Fraud: Top Scams in 2021. Retrieved from: https://www.aging.senate.gov/imo/media/doc/aging_committee_fraud_book_20221.pdf.

Appendix B

Attorneys General – States

Alabama
334-242-7300

Alaska
907-269-5100

Arizona
602-542-5025

Arkansas
800-482-8982

California
916-445-9555

Colorado
720-508-6000

Connecticut
860-808-5400

Delaware
302-577-8600

Florida
850-414-3300

Georgia
404-651-8600

Hawaii
808-586-1500

Idaho
208-334-2400

Illinois
312-814-3000

Indiana
317-232-6330

Iowa
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
517-335-7622

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
505-490-4060

New York
518-776-2000

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

Attorneys General – Territories

American Samoa
684-633-4163

District of Columbia
202-442-9828

Guam
671-475-2720

Northern Mariana Islands
670-237-7600

Puerto Rico
787-721-2900

U.S. Virgin Islands
340-774-5666

Source: U.S. Senate Special Committee on Aging (2021). Fighting Fraud: Top Scams in 2021. Retrieved from: https://www.aging.senate.gov/imo/media/doc/aging_committee_fraud_book_20221.pdf.

national council on aging®

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