How to Help Protect Older Adults from Telephone and Internet Scams

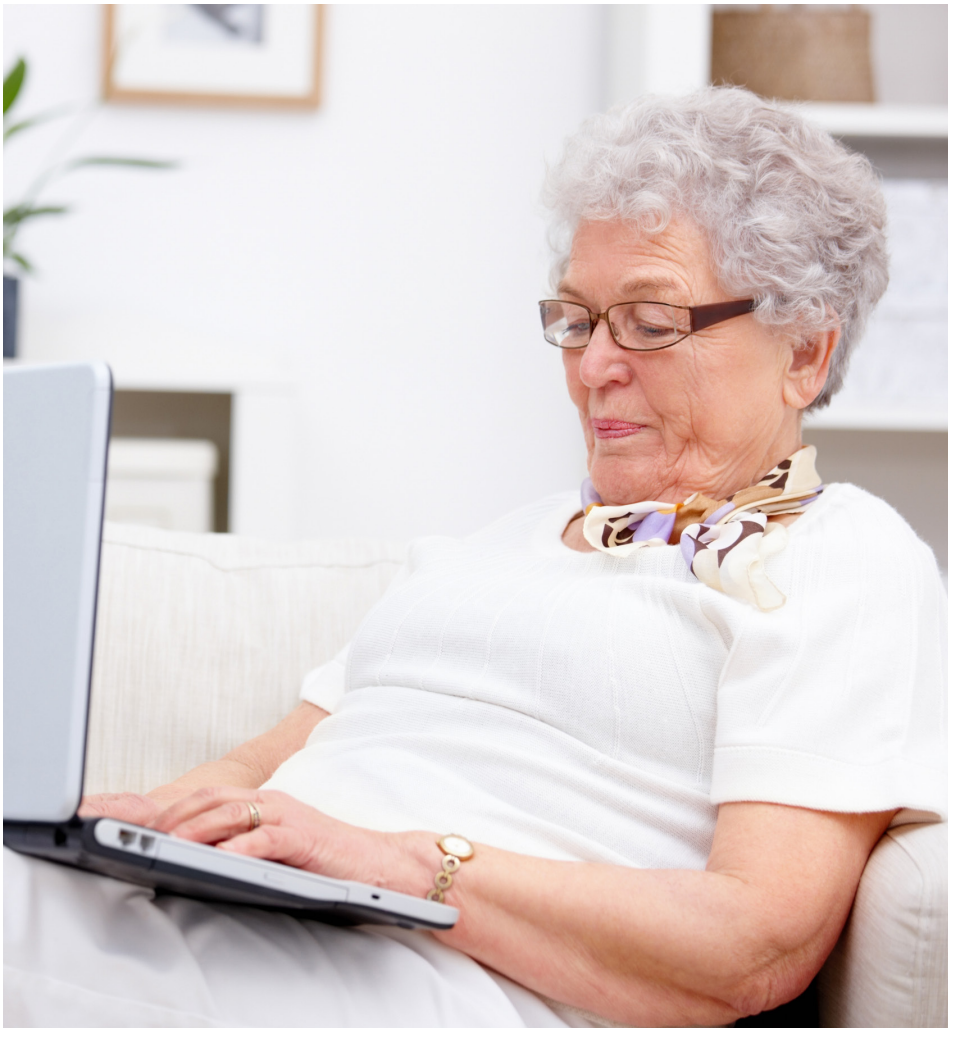
Overview

This guidance will help providers answer the following questions regarding telephone and internet scams targeting older adults:

What are the most popular scams targeting older adults?

Are there some practical tips to help older adults avoid scams?

Who can I call to report scams?



Background

Financial fraud targeting older Americans is a growing epidemic that costs seniors an estimated $2.9 billion annually according to the Government Accountability Office (GAO). This estimate is likely low as often seniors do not report fraud because they are too ashamed to admit they have been scammed, may not even know that they are victims, or do not know how to report it.

In the ongoing efforts to protect seniors from internet and telephone scams, the US Senate Special Committee on Aging (Aging Committee) has taken a keen interest in helping protect seniors from internet and telephone scams. The Aging Committee set up a fraud hotline and releases an annual report detailing the number and types of fraud complaints the hotline receives.

LeadingAge®

June 2018

The 2018 Fraud Book noted that the Aging Committee's Fraud Hotline alone received more than 1,400 complaints of fraud targeting seniors around the country. The top 10 scams reported in 2017 were: IRS impersonation scams, robocalls and unsolicited phone calls, sweepstakes scams/Jamaican lottery scam, "Can you hear me?" scams, grandparent scams, computer tech support scam, romance scams, elder financial abuse, identity theft, and government grant scams. However, these are not the only scams attempted against older adults.

The Aging Committee is just one of many federal and state government entities that is fighting fraud against older adults. In fact, all the state attorneys general offices have a number to report fraudulent activities. In addition to the government agencies, there are private and nonprofit entities that also provide guidance on how to help older adults avoid scams.

If you or someone you know are the victim of a scam or fraud attempt, please call the Aging Committee's Fraud Hotline at 1-855-303-9470.

General Tips on How to Avoid Scams

Here are some friendly reminders on how to avoid scams. The following tips from the Aging Committee are reminders that help older adults identify general scams:

- Con artists force you to make decisions fast and may threaten you.
- Con artists disguise their real number, using fake caller IDs.
- Con artists sometimes pretend to be the government (e.g. IRS).
- Con artists try to get you to provide them personal information like your Social Security number or account numbers.
- Before giving out your card number or money, please ask a friend or family member about it.
- Beware of free travel offers.

Source: Tips from United States Senate Special Committee on Aging for Avoiding Scams, 2018 Fraud Book.

Internal Revenue Service (IRS) Impersonation Scam

The most common scam targeting older adults in 2017, according to the Aging Committee, is the IRS impersonation scam. In this scam, a caller claims to be from the IRS and claims that the person owes taxes and/or penalties to the government that are payable immediately. The caller then attempts to secure payment from the victim to clear the alleged outstanding debt.

The IRS, in response to the impersonation scams that have targeted Americans for the last several years, drafted the following advice to help people identify suspicious calls that may be associated with the IRS imposter scam:

- The IRS will never call a taxpayer to demand immediate payment, nor will the agency call about taxes owed without first having mailed a bill to the taxpayer.
- The IRS will never demand that a taxpayer pay taxes without giving him or her the opportunity to question or appeal the amount claimed to be owed.
- The IRS will never ask for a credit or debit card number over the phone.
- The IRS will never threaten to send local police or other law enforcement to have a taxpayer arrested.
- The IRS will never require a taxpayer to use a specific payment method to pay taxes, such as a prepaid debit card.

Source: https://www.irs.gov/newsroom/five-easy-ways-to-spot-a-scam-phone-call

Additional IRS resources on avoiding scams: https://www.irs.gov/newsroom/tax-scamsconsumer-alerts

Unsolicited Phone Calls, Robocalls, and Telephone Scams

A. General Tips

Although the Do-Not-Call Registry passed in 2003, Americans are still being victimized by unsolicited phone calls. In fact, according to the Federal Communications Commission, there are over 2.4 billion robocalls each month.

Some of the different telephone or robocall scams include lottery scams, "can you hear me scams," grandparents scam, and computer technical support scams.

The FCC has drafted a few handy tips to help older adults avoid falling prey to telephone scams, especially if the caller is using a fake caller ID:

- Never give out personal information such as account numbers, Social Security numbers, mother's maiden names, passwords or other identifying information in response to unexpected calls or if you are at all suspicious.
- If you get an inquiry from someone who says they represent a company or a government agency seeking personal information, hang up and call the phone number on your account statement, in the phone book or on the company's or government agency's website to verify the authenticity of the request.
- Use caution if you are being pressured for information immediately.
- If you have a voicemail account with your phone service, be sure to set a password for it. Some voicemail services are preset to allow access if you call in from your own phone number. A hacker could spoof your home phone number and gain access to your voice mail if you do not set a password.

Source: https://www.fcc.gov/consumers/guides/spoofing-and-caller-id

B. Can You Hear Me? Scam

In early 2017, a new scam came to the attention of the Senate aging committee – the "can you hear me" scam. In this scam, the caller (or robocaller) asks the person answering the phone "can you hear me?" or "are you there?" The goal is to get the person to respond "yes." The scammer records the "yes" answer and then attempts to use it as a voice signature to authorize unwanted charges or billings.

The Federal Trade Commission (FTC) published the following tips for consumers who get a call from somebody they don't recognize asking, "Can you hear me?":

- Don't respond, just hang up. If you get a call, don't press 1 to speak to a live operator or any other number to be removed from the list. If you respond in any way it will probably just lead to more robocalls – and they're likely to be scams.
- Contact your phone provider. Ask your phone provider what services it provides to block unwanted calls.
- Put your phone number on the Do Not Call registry. Access the registry online or by calling 1-888-382-1222. Callers who don't respect the Do Not Call rules are more likely to be crooks.
- File a complaint with the FTC. Report the experience online or call 1-877-382-4357.

Source: https://www.consumer.ftc.gov/blog/2017/03/calls-asking-can-you-hear-me-now

C. Grandparent Scam

A common scam that specifically targets older Americans is the "grandparent scam." Imposters either pretend to be the victim's grandchild, claim to be holding the victims' grandchild hostage, or trying to help the grandchild out of a desperate situation. The perpetrator typically claims the grandchild is in trouble and needs money to help with an emergency, such as getting out of jail, paying a bill (hospital bill is a common one), or to come home from a foreign country. The caller targets the grandparent specifically because they claim the grandchild does not want to involve their child's parent(s) to avoid getting in trouble. They urge the grandparent to keep it a secret to make the ruse more believable.

Older adults should follow the tips outlined above and hang up. Reaching out the grandchild or a parent should help alleviate any anxiety over their grandchild's safety.

LeadingAge®

Internet Scams

There has been an increase in computer-based scams as well over the last few years. This is not surprising given that technology is changing rapidly and more consumers are using the internet to communicate and shop for products. Two types of internet or computer-based scams that have been popular lately are the tech support and romance scams.

A. Tech Support Scams

One type of computer-based or computer-related scam involves the request to fix technical issues on your computer. Imposters either target older adults through telephone calls alerting the target of the scam to computer issues that need to be resolved immediately or they make contact through pop-up alerts while users are browsing the internet making similar claims.

According to Microsoft, there were over 180,000 complaints from consumers related to computer-based fraud between May 2014 and October 2015. Microsoft estimates that 3.3 million Americans are victims of technical support scams annually, with a losses around $1.5 billion.

Although these fraud losses are over all ages, older adults are often the most vulnerable to these types of scam.

The FTC has some useful tips to help consumers avoid falling victim to computer-based scams:

- Do not give control of your computer to a third party that calls you out of the blue.
- Do not rely on caller ID to authenticate a caller. Criminals spoof caller ID numbers. They may appear to be calling from a legitimate company or local number when they are not even in the same country as you.
- If you want to contact tech support, look for a company's contact information on its software package or on your receipt.
- Never provide your credit card or financial information to someone who calls and claims to be from tech support.
- If a caller pressures you to buy a computer security product or says there is a subscription fee associated with a call, hang up. If you're concerned about your computer, call your security software company directly and ask for help.
- Make sure you have updated all of your computer's anti-virus software, firewalls, and pop-up blockers.

Source: http://www.consumer.ftc.gov/articles/0346-tech-support-scams

B. Romance Scams

As more and more people turn to the internet for dating websites, the number of related romance fraud claims have risen as well. The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3), received 14,546 calls in 2016 about romance and confidence scams. In 2014, IC3 reported that nearly 50% of the victims were 50 and older. The volume of complaints and the amount of money lost in this scam have both steadily increased in recent years.

The FBI's IC3 has the following tips to help older adults to avoid romance scams:

- Be cautious of individuals who claim the romance was destiny or fate, or that you were meant to be together.
- Be cautious if an individual tells you he or she is in love with you and cannot live without you but needs you to send money to fund a visit.
- Fraudsters typically claim to be originally from the United States (or your local region), but are currently overseas, or going overseas, for business or family matters.

Sources: 2018 Fraud Book and FBI Resources https://www.collins.senate.gov/sites/default/files/2018%20Fraud%20Book.pdf

LeadingAge®

Identity Theft

One type of fraud that continues to affect older adults is identity theft. Perpetrators use the stolen identity to run up credit card bills, drain bank accounts and damage credit scores. In addition to financial fraud there has been an increase of using stolen identities to procure medical care and services and prescriptions. The disruption in the lives of victims of identity theft is severe, time-consuming, and can take years to recover from such incidents. Nearly half of the identity theft victims in 2015 were over 50 years old according to the FTC.

If you are a victim of identity theft, here are some helpful tips:

What to do Right Away:

1. Call the companies where you know the fraud occurred.
2. Place a fraud alert with a credit reporting agency and get your credit report from one of the three national credit bureaus.
3. Report identity theft to the FTC.
4. File a report with your local police department

What to do Next:

1. Close new accounts opened in your name.
2 Remove bogus charges from your accounts.
3. Correct your credit report.
4. Consider adding an extended fraud freeze.

Tips to Help Secure Your Identity:

- Neither Medicare nor Social Security will call to ask for your bank information or SSN.
- There will never be a fee charged to obtain a Social Security or Medicare card.
- Never give out personal information over the phone to someone you do not know.
- Sensitive personal and financial documents should be kept secure at all times.
- Review all medical bills to spot any services that you didn't receive.

Source: https://www.identitytheft.gov

Conclusion

The prevalence of scams attacking consumers continues to threaten the financial well-being and peace of mind of older adults. Numerous federal agencies and the US Senate Special Committee on Aging continue to address these scams and try to provide guidance to help older adults combat these attempts.

While the Aging Committee continues to hold hearings on the scams affecting older adults, we all must remain vigilant to help protects seniors. We urge LeadingAge members to help distribute information to their residents (and families) to let them know there are resources and a number to call if they are victims of a scam.

If you or someone you know is the victim of a scam or fraud attempt, please call the Aging Committee's Fraud Hotline at 1-855-303-9470. The Aging Committee's Fraud Book is a great resource and includes additional numbers for consumers to call to report fraud to their state jurisdictions as well as other federal agencies.

Resources:

US Senate Special Committee on Aging 2018 Fraud Book

IRS resources

FTC resources

FCC resources

FBI resources

LeadingAge®