Avoiding Telephone and Internet Scams

Older adults are increasingly the targets of scam artists on the telephone who use lies, deception, and fear tactics to convince the older adult to send them money or provide personal account information. The Do-Not-Call registry may reduce calls from telemarketers representing legitimate businesses; however, it will not stop criminal telemarketers from calling.

Grandparent Scam

An example of a common telephone is the ‘grandparent scam.’ In this scenario, an imposter calls a grandparent pretending to be a grandchild in trouble. The scammer may even know the grandchild’s name. The scammer is usually crying making it hard to recognize the grandchild’s voice. The scammer pleads for the grandparent to immediately wire money and not tell any family members for fear of upsetting them. Many people will immediately jump to the assistance of the grandchild and won’t ask questions until later. Scammers also know that many older people may have experienced a hearing loss and won’t detect any differences from their grandchild’s voice. Or they may attribute the differences they do hear to the stress of the situation.
IRS Telephone Scam

According to the Internal Revenue Service (IRS), in this telephone scam, a scammer calls telling the consumer that he or she and must immediately pay taxes that are owed. In some cases, the scammers target immigrants, who are told that if they don’t pay the tax bill or otherwise follow instructions, they will face serious consequences, such as arrest and deportation, or the IRS could shut off their utilities, or revoke their driver’s licenses. Callers are frequently insulting or hostile to scare their potential victims.

These scammers frequently:

- Tell potential victims that they are entitled to big refunds, or that they owe money that must be paid immediately to the IRS. When unsuccessful, they often call back trying new strategies.
- May spoof the IRS toll-free number on caller ID to make it appear that it’s the IRS calling.
- Use common names and surnames to identify themselves and fake IRS badge numbers.
- May know the last four digits of a victim’s Social Security number.
- Send bogus IRS emails to victims to support their bogus calls.
- Create background noise to mimic a call site.
- Threaten jail time or driver’s license revocation.
- Hang up and call back pretending to be from the local police or DMV (with fake caller ID to trick you into believing that it is an official call) and threaten the consumer with arrest or revocation of their driver’s license.
For more information from the IRS on this type of scam, go to [irs.gov/newsroom/tax-scams-consumer-alerts](https://irs.gov/newsroom/tax-scams-consumer-alerts).

The IRS has warned that this crime continues year round. Remember, the IRS will always send taxpayers a written notification of any tax due via the U.S. mail. The IRS never asks for payment or credit card information over the telephone. And the IRS does not initiate contact with taxpayers by email, text message, or through social media to request personal or financial information such as PINs or passwords.
If you get a **phone call** from someone claiming to be from the IRS, here’s what you should do:

- If you know you owe taxes or you think you might owe taxes, call the IRS at **1-800-829-1040**. The IRS employees at that line can help you with a payment issue, if there really is such an issue.

- If you know you don’t owe taxes or have no reason to think that you owe any taxes (for example, you’ve never received a bill or the caller made some bogus threats as described above), or if you think the party who called you is not really with the IRS, then call and report the incident to the Treasury Inspector General for Tax Administration at **1-800-366-4484**.


- You can file a complaint using the FTC Complaint Assistant at [ftccomplaintassistant.gov](http://ftccomplaintassistant.gov); choose “Scams and Rip-offs” and then “Imposter Scams.”

If you get an **email** from someone claiming to be from the IRS, don’t open any attachments or click on any links contained in the message. Instead, forward the e-mail to [phishing@irs.gov](mailto:phishing@irs.gov). More information on how to report phishing scams involving the IRS is available on the IRS website, [IRS.gov](http://irs.gov).
Lottery and Sweepstakes Scams

Sweepstakes scammers call, email, or text consumers congratulations on winning a lottery, drawing, or sweepstakes, which the consumers usually have not even entered. The scammer asks the “winner” for an upfront payment to cover processing fees or taxes. In another variation, the scammers send a letter with an authentic looking, but phony, “Claim Certificate” or a “check” as an advance to pay the winnings. Bankers are generally aware of this scam and how to spot the phony checks. But if you deposit a phony check, the financial institution might hold you responsible for repayment of the entire amount of the fraudulent check even if you sent some of the money to the scammer.

Sweepstakes Recovery Scam

Once it is apparent that no winnings are forthcoming, the victim may receive another call from a person claiming to be an attorney representing sweepstakes winners. In exchange for an upfront fee, the so-called “attorney” offers to collect the winnings on behalf of the victim. Needless to say, the “attorney” is actually an associate of the original scammer and there is no chance of recovering the original loss or the fraudulent fee that the fake “attorney” charges.
Tips for Avoiding Telephone Scams

Scammers can be very convincing. If something seems unusual, check it out.

- You cannot win a sweepstakes or a lottery that you did not enter.
- Never “pay to play.” A legitimate sweepstakes will not ask for money upfront.
- Be suspicious of any pressure to send funds via wire transfer or a pre-paid reloadable card.
- Pay attention to warnings from your financial institution telling you that a request sounds like a scam. Your banker may have encountered similar situations in the past.
- Scammers often claim an emergency, hoping you will respond quickly without checking out the situation first. Before offering your help to someone who claims to be a grandchild (or any other relative/friend), be sure to telephone your grandchild or his/her parents at a number you know to be valid to find out if the request is legitimate.
- If a caller claims to be from an established organization such as a hospital, a charity, or a law enforcement agency, look up the number of the organization independently before taking action.
- Consider it a red flag if the caller insists on secrecy. Never allow anyone to discourage you from seeking information, verification, support and counsel from family members, friends or trusted advisers prior to making any financial transaction.
Activity 1: Telephone Scams

Read each scenario and then, based on what you have learned, answer the questions in the spaces provided:

Instructor: Refer participants to Activity 1 on page 30 in their Resource Guides. Work together as a class or have participants work in small groups, or individually, to answer the questions. Reveal the answers so they can check their thinking.

Scenario 1

Jane is home watching TV when the telephone rings. She answers the call and the man on the line says “Congratulations! You’ve won $2.7 million dollars in the lottery!” Jane is surprised. Although she buys lottery tickets, she hasn’t given her name to anyone. The caller tells her that there are a couple of things she needs to do before she can receive her check. He directs Jane to go to her bank and withdraw $2,700 to cover processing fees. He tells her to forward the funds through a local wire service or to buy and send a special prepaid card that will expedite the process. Jane heads to her bank to withdraw the money. The next day the person calls to say they received the funds and an additional $5,000 is needed to pay the taxes.
**Question:** What were the red flags that should have warned Jane that she was about to become a victim of a scam?

**Answers:**
- You cannot win a lottery or sweepstakes you did not enter.
- A legitimate sweepstakes or lottery will not ask winners for money upfront.
- Jane was asked to send funds via a wire service or a prepaid card to expedite the process.

**Scenario 2**
A few weeks after Jane used a pre-paid card to transfer money to the scammer, she received a call from a person claiming to be an attorney representing sweepstakes winners. The attorney offered to recover the winnings for Jane but she would have to pay him a $7,000 fee up front.

**Question:** What should Jane do?

**Answers:**
- Jane should not send any more money.
- Jane should report the scam to the FTC.
- Jane should call the police.

**Scenario 3**
Jack lives alone in his home of 40 years. He has become increasingly hard of hearing, which has made it difficult for him to communicate on the telephone. One afternoon he receives a call from a distressed-sounding person who says “Hi Grandpa, this is your favorite
grandson.” When Jack asks “is this Johnny?” the caller says “yes grandpa, it’s Johnny.” Johnny says he’s in Canada and has been arrested. Johnny explains that he needs Jack to wire $2,500 to bail him out. Johnny also says “please don’t tell Mom – I don’t want her to get upset.” Jack hurries to his bank and insists on wiring the money despite warnings from the teller and the bank manager that this sounds like a scam.

**Question:** What are the red flags in this story?

**Answers:**
- The caller claims an emergency situation.
- Jack is pressured to send money via wire transfer or pre-paid reloadable card.
- To avoid detection, the caller insists that Jack keep the call and the wire transfer of funds secret from those who could verify the report of an emergency.
- His trusted representatives at the bank or credit union warn him that he may have been targeted by a scam.
Phantom Debt Collection Scam

Scam debt collectors try to trick their victims into paying a debt that doesn’t exist. These phony debt collectors often contact older adults by phone and refuse to answer questions about themselves and the underlying debt. Phony debt collectors may have some information about the older person that they’ll use to appear to be legitimate. Scam debt collectors may use scare tactics and may threaten to do things that they can’t do, such as arresting the older person or physically hurting him or her unless the debt is paid immediately.

Other characteristics of this scam may include:

- You do not recognize the debt, and the debt collector refuses to give you information about the debt.
- The debt collector refuses to give you a mailing address or phone number.
- The debt collector claims that it can press criminal charges against you, if you refuse to pay the debt collector immediately.
- The debt collector asks you for sensitive personal financial information.
- The debt collector asks you to use an anonymous way to pay, such as buying and sending a prepaid debit card, providing the card number over the phone, or using a wire transfer or an electronic transfer from your bank account.
How to respond to a possible debt collection scam

If you receive a call from someone claiming to be a debt collector, ask for more information. Don’t ignore your suspicions if you don’t recognize the debt, and don’t give in to threats.

- Ask the caller for his or her name, company, street address, and telephone number.
- Sample letters you can use to respond to debt collectors can be found at consumerfinance.gov/consumer-tools/debt-collection.
- If you dispute the debt or ask for the name of the original creditor in writing within 30 days of the caller’s first communication, the debt collector usually has to stop all debt collection activities until it verifies the debt or provides you that information.
- If you can’t verify the information the collector provides, do not give money or your financial information (such as a bank account number or credit card number) to the caller or company.
- Do not give the caller your financial or personal information such as your social security number or date of birth.
- Keep the letters or documents a debt collector sends you, and keep copies of anything you send to a debt collector. You can also write down dates and times of conversations along with notes about what you discussed. These records can help you remember, or show others what actually happened.
You can also submit a complaint to the CFPB (1-855-411-2372) or consumerfinance.gov and you can contact your state Attorney General’s office through the National Association of Attorneys General at naag.org/naag/attorneys-general/whos-my-ag.php.

Activity 2: Phantom/Scam Debt Collection

Read the scenario and then, based on what you have learned, answer the questions in the spaces provided:

Scenario
Pamela is sitting down to eat when she receives the sixth call today from a phone number that she does not recognize. Pamela usually does not answer the phone unless she recognizes the number because she is wary of scams.

Pamela does not pick up the phone. The caller leaves a voice message stating that Pamela owes $349 to Federal Collections, Inc. The message says that if Pamela does not pay $349 by 11:00 a.m. tomorrow, a warrant will be issued for her arrest. Pamela would be humiliated if she were arrested in front of her neighbors. She picks up the phone.
The caller tells Pamela that she can avoid being arrested by wiring $349 through a money transfer.

**Question:** What are the red flags that should warn Pamela that this is a scam?

**Answers:**
- The caller does not inform Pamela of her right to dispute the debt.
- The caller calls from a company whose name suggests that is affiliated with the government.
- The caller demands immediate payment.
- The caller threatens to arrest Pamela.
- Scammers often use wire transfers to transfer money anonymously.

**Question:** If you were Pamela, what would you do?

**Answers:**
- Hang up, and leave the phone off the hook for a while to give myself time to think about the situation.
- Call a trusted friend or a family member.
- Record the time and content of future calls.
- If the caller calls back, ask the teller to send me in writing the amount of the original debt, an explanation of any additional charges, the name of the creditor, a phone number where they can be reached, and an address where I can send a dispute letter.