

KEEPING TENNESSEE SENIORS SAFE

***WHAT YOU NEED TO
KNOW ABOUT PHONE
AND INTERNET SCAMS***



State of Tennessee
Office of the Attorney General & Reporter



Department of
**Commerce &
Insurance**

Consumer Affairs

Contact (800) 342-8385
www.tn.gov/commerce/section/consumer-affairs



Scammers use the internet or telephone to trick millions of people every year into sending money or giving out personal information. Scammers can be polite and charming. They may say they work for a company that you recognize. They may know your name or certain things about you and make you feel special. They promise things like lottery winnings, prizes, friendship, or romance. But they don't keep these promises.

Are you an older adult? Do you have savings? Do you live alone? Then be on the lookout for scammers. The Tennessee Attorney General's Office wants seniors, their families, and caretakers to know about common phone and internet scams, how to stop them, and how to get help and report them.



HOW DOES A PHONE OR INTERNET SCAM WORK?

Scammers may offer prizes, products, or services. They want you to say "yes" quickly. They say you must act right away. They may even try to scare you by saying you could be taken to court or to jail. Look out for statements like these:

- You've been specially selected for our offer.
- This is a free trial offer.
- You'll get a prize if you buy our product.
- You've won money in the lottery.
- Don't tell anyone that you've won.
- You have to pay us now to receive our special offer.
- You trust me, right?
- We need you to confirm your personal/billing information.
- If you don't pay us now, we will sue you (or you will be arrested).

PHONE AND INTERNET SCAMS

- **Imposter Scams:** An "imposter" is someone who pretends to be someone else. Scammers may email or message you and say they are a family member or someone who wants to be your friend. They may even say they love you. They try to win your trust and ask you to send them money.
 - ❖ Grandparent/Grandchild Scam: *"Grandma, I need money for bail. Please don't tell mom!"*
 - ❖ Romance scam: *"I wish I could visit you, but I don't have enough money for a plane ticket."*
 - ❖ Government Grant scam: *"You've been awarded a grant and just have to pay taxes and fees to get it."*
- **Tech Support Scams:** You get an email or a pop-up alert on your computer. It says your computer has a virus or other security issue. You are told you must call a tech support company. This company asks for remote access to your computer so they can

fix the problem. Once they have access, they say your computer has many different viruses that they can take care of—if you pay them a large amount of money. Or they may install malware—a program that steals your personal data, like usernames and passwords, or even whole computer files.

- **Lottery Scam:** Scammers say they are lottery officials or with a sweepstakes company. They tell you you’ve won money. Then they ask you to pay them upfront to cover fees or taxes. But they take your money and never give you the winnings they promised.

- **Phishing Scam:** Scammers pretend to be from credit card companies or banks. They trick you into giving them your personal information. They may send you an email or text like this:

- ❖ Warning: We have detected an unauthorized transaction on your account. To ensure your account is not compromised, please click the link below and confirm your identity.

- ❖ Our records indicate that your account was overcharged. You must contact us immediately to receive your refund.

- **IRS Imposter Scam:** Scammers say they are with the Internal Revenue Service (IRS). They say you owe back taxes. They may threaten that you’ll be arrested, deported, or have your driver’s license taken away if you don’t pay them. Or they might say you must give them your bank account number to receive a tax refund. If you receive this call, contact the IRS right away at (800) 366-4484, or visit their website: www.irs.gov/uac/report-phishing. Remember, the IRS will contact you initially by mail (NOT email or

phone), and will always give you a chance to question or appeal any amount they say you owe. They will never say you will go to jail for not paying.

- **Utility Bill Scam:** Scammers say they're from your local utility company. They say you're behind on your bill and that your service will be cut off if you don't pay right now. They ask for your credit card information over the phone. Remember, utility companies usually send notices of overdue service fees by mail. Always call your utility company using the number on your bill to find out if you really owe them money.

HOW TO AVOID PHONE AND INTERNET SCAMS

- Sign up your phone number with the National Do Not Call Registry by visiting www.donotcall.gov or calling 888-382-1222. If you get a telemarketing sales call after you are on the registry it might be a scam. You can also sign up with the Tennessee Regulatory Authority's Do Not Call Program, www.tn.gov/tra/topic/tennessee-do-not-call-program or call 877-872-7030.
- If a caller says you must act right now to receive a special offer, don't do it. Ask them to give you contact information and send you information in writing so you have time to research the organization and review the offer.



- If the caller says they're with a company you recognize, but you're still not sure they're telling you the truth, hang up. Call the company using a number from their official website or the phone book.
- Look out for websites with misspelled words or logos and pictures that are hard to see or read. They may be fake sites run by scammers. Check the URL (site address) to see if the web address matches the one for the real company.
- Only enter banking or other sensitive personal information on secure websites that you trust. The web address should start with `https://` and the web browser should display a closed padlock, which means the connection to the server is encrypted. This will protect your information so no one else can see it or use it.
- Only share your financial and personal information with callers that you know and trust.
- Pay with a credit card. Don't send cash, use a debit card, or send a wire transfer. When you use your credit card, you may have protections against fraud through your credit card company.

WHAT TO DO IF YOU BECOME A VICTIM

Here are some things you can do:

1) Document It: Write down everything you remember about what happened. Include the names of the companies and people you spoke with. Also write down the dates you spoke with them.

2) Take Action and Report:

- Contact your bank or credit card company right away. Stop the payment if you can.
- Report what happened to federal and/or state agencies. Here are some places you can call for free:
 - ❖ Eldercare Locator helpline, (Department of Health and Human Services): (800) 677-1116.
 - ❖ Anti-Fraud Hotline (U.S. Senate Aging Committee): (855) 303-9470 between 9 a.m. to 5 p.m. EST, or visit www.aging.senate.gov/fraud-hotline.
 - ❖ Victim Connect hotline (VictimConnect Resource Center, National Center for Victims of Crime): (855) 484-2846.
 - ❖ Federal Communications Commission's Consumer Call Center: (888) 225-5322.
- File a complaint with the following state and federal regulators:



- ❖ Call the Tennessee Division of Consumer Affairs at (800) 342-8385 or (615) 741-4737, or visit www.tn.gov/commerce/section/consumer-affairs to file a complaint.
- ❖ File a complaint with the Federal Communications Commission at www.consumercomplaints.fcc.gov.
- ❖ File a complaint with the Federal Trade Commission at www.ftc.gov/complaint.
- ❖ File a complaint with the Federal Bureau of Investigation (FBI) Internet Crime Complaint .Center (IC3) at www.ic3.gov.

3) Tell your family, caregivers, and friends: Tell others what happened so that they can help you and protect themselves.



RESOURCES

The following websites provide more information on phone and internet scams:

- **U.S. Department of Justice, Elder Justice Website:** www.justice.gov/elderjustice
- **Federal Communications Commission:** www.fcc.gov
- **Federal Trade Commission:** www.ftc.gov/complaint
- **Federal Bureau of Investigation:** www.fbi.gov/scams-and-safety
- **Federal Financial Fraud Enforcement Task Force:** www.stopfraud.gov



State of Tennessee

Office of the Attorney General & Reporter



Department of
**Commerce &
Insurance**

Consumer Affairs