Attorney General
**Josh Stein**

Published October 2023

# SENIOR SCAM GUIDE

# A letter from Attorney General Josh Stein

**At the North Carolina Department of Justice, our mission is to protect the people of North Carolina. That includes protecting people from scammers and fraudsters. And unfortunately, these bad actors too often try to scare or confuse people who are more vulnerable, including older people.**

Scammers are getting more sophisticated by the day – their technology is better, and so are their schemes. We all have to be more careful about what we say, where we send money, and what personal information we share.

I hope that this guide gives you an idea of the most common tactics scammers use to part older people from their money. Please share it with your loved ones and discuss these tips. My office's Consumer Protection Division will work to try to get your money back if it falls into a scammer's hands, but the most effective defense is always preventing these scams from happening in the first place.

If you are or think you might have been the victim of a scam, or if you are simply unsure whether something is legitimate, then please call my office at 1-877-5-NO-SCAM or file a complaint at www.ncdoj.gov/complaint. You can also contact us for help in Spanish by calling 919-716-0058.

We have consumer protection specialists who can help you determine whether or not something is the real deal, and our attorneys will fight to hold bad actors accountable when possible.

These are the best tips to know to protect yourself and your hard-earned money. You can also sign up online to get email alerts from us on fraud and other public safety issues at www.ncdoj.gov/subscribe or follow us on Facebook at www.facebook.com/NCDOJ or on X, formerly known as Twitter, at www.twitter.com/ncago.

***—ATTORNEY GENERAL JOSH STEIN***

# Table of Contents

# COMMON TARGETS

Our office's Consumer Protection Division investigates complaints about frauds against senior citizens. We know that scammers will regularly target certain groups of people. To be clear, scammers can try to take advantage of anyone. But, if you fall into any of these groups, you should be extra vigilant about scams:

- People who are in their late seventies or older.
- People who live alone, or whose spouse has recently died or become disabled, and they've taken on financial responsibilities.
- People who are worried about the adequacy of their savings or their ability to remain in their own homes.
- People who are bright, accomplished, and capable of conducting their day-to-day affairs without assistance.

Here is additional helpful information to remember about people who may have been victimized by a scammer. Keep these points in mind when you're concerned someone you know might have been scammed, and please offer help and assistance.

- Scam victims worry about their adult children's reactions to scam transactions. Often, they may think that warnings from you or their loved ones are motivated by greed or control.
- Scam victims rarely report fraud to law enforcement. Instead, reports typically come from other people who observed the fraud.
- Scam victims are often quite secretive about their financial transactions and are reluctant to acknowledge these transactions even during conversations with family, law enforcement, or their financial institutions.
- Victims frequently deny they are engaged in irregular transactions even when confronted with evidence of same.

Additionally, people who fall victim to a scam once are far more likely to fall victim to a scam again, or to another form of elder fraud. They may even fall victim to frauds designed to get their money back from the initial scam.

If you have questions about whether you've been the victim of a scam, or you want to find information to verify whether something is a scam, visit www.ncdoj.gov/protecting-consumers or call our office at 1-877-5-NO-SCAM. You can also contact us for help in Spanish by filling out this consumer complaint form or calling 919-716-0058.

# TELEMARKETING SCAMS

Unwanted phone calls can be a nuisance. While some telemarketers call to sell you something, other robocallers want to steal your money or your personal information. Robocallers cost people as much as $40 billion a year. Attorney General Stein is leading nationwide efforts to cut down on robocalls by preventing them from getting on the telephone network and working with law enforcement to hold illegal robocallers accountable.

You can avoid telemarketing scams by **following these tips:**

- **Hang up.** Do not press a number to avoid further calls. This alerts robocallers that they have reached an active number and could lead to more unwanted calls.
- **Sign up for the Do Not Call Registry** at 1-888-382-1222 or www.donotcall.gov. If your phone number is on the Do Not Call Registry, legitimate telemarketers are not allowed to call you. Once you've signed up, you'll know that telemarketers who call are probably out to scam you.
- **Remember that you do not know who is on the other end of the call.** They may claim to be the government or a family member, but it is safest to stay skeptical. Especially if they ask for money!
- **Unless you are familiar with the company, do not respond** to mailings and email messages about sweepstakes or lottery prizes. Doing so can get you on a list of potential targets that fraudulent telemarketers around the world purchase.
- **If it sounds too good to be true, it probably is.** These deals are great only for the person selling them.
- **Don't let the pressure push you.** People use high-pressure tactics – like fear and excitement – to get you to make a quick decision. If you feel like you have to give away your money or data, it's probably a scam.
- **Never give your bank account, credit card or Social Security number** to someone you don't know.

## Scam Story

A caller offers you a Medicare drug discount card with many benefits. You are asked to give your bank account numbers so your account can be debited to pay for the discount card. But the card you receive is not honored by your pharmacy, or you receive nothing at all. Meanwhile, the scammer withdraws funds from your checking account for items or services you didn't order.

**Remember:** Whenever anyone contacts you and you're unsure of their authenticity, hang up and call our office. Never give out your bank information to someone you don't know.

# SWEETHEART/FRIENDSHIP SCAMS

One of the most common frauds our office sees is the sweetheart or friendship scam, where scammers lure the victim into a bogus romance or friendship and manipulate the victim's feelings to rob them of their money. Often, these scammers target seniors who have just been through a major life event that might make them more vulnerable, such as losing a spouse. The scammer befriends a potential victim by using mutual interests or supposed mutual friends to create a connection and exploit their trust. Typically, the scammer makes contact online through LinkedIn, Facebook, dating sites, or messaging apps.

You can avoid sweetheart and friendship scams by **following these tips:**

- **Share your information carefully.** Never give out your personal information, especially your address or account numbers, to anyone online. Make sure your social media profiles are set to private. Often, scammers use information learned on social media profiles to manipulate victims.
- **Be skeptical of anyone you've never met in person.** Avoid anyone who says they can only communicate with you online, asks you to email or communicate outside of the dating site, or claims they are wealthy, foreign citizens. Never send money to someone you've never met in person, even if their story sounds convincing. If an online love interest or new friend ever asks you for money, it's probably a scam.
- **Ask someone you trust for help.** When in doubt, reach out to your friends and family to verify. If you think you might have been the victim of a scam, call our office.

## Scam Story

You are contacted by someone overseas who has seen the personal information you posted on a social networking or dating website. The "sweetheart" uses email, messaging apps, and phone or text conversations to strike up a friendship, which eventually blooms into a romance. Once they gain your trust, your new love interest calls to tell you they're in the hospital overseas and asks you to wire them money to help with medical bills.

**Remember:** Sweetheart and friendship scammers often claim to be living or working overseas, and they pretend to have a mutual connection with you based on information they've learned about you through your social media profiles. The scammer may wait months to gain your trust before they ask you for money. If an online love interest ever asks you to send them money, it is usually a scam.

# SWEEPSTAKES SCAMS

Many scammers attempt to use your excitement to get you to make a bad decision. You may get a telephone call, email, or letter telling you that you've won the lottery or urging you to apply for a sweepstakes because you're already a finalist. Often, the scammer will ask you to pay a down payment or fee to collect your prize money. The most common ploy is for the scammer to tell you that you need to prepay your taxes on the winnings.

You can avoid sweepstakes scams by **following these tips:**

- **Never send money to anyone who says you've won a prize.** This includes people you've exchanged emails or letters with, as well as telemarketers. It's illegal to have to pay anything upfront to win a prize. Any prize that requires you to send money to cover taxes or other costs first is a scam. Don't be fooled if they include a check to cover taxes and fees. The check is fake.
- **Protect your personal information.** Never give out your Social Security number, bank account, or credit card number in order to win a prize.
- **Be skeptical.** If anyone tells you that you've won a prize or contest you don't remember entering, it's probably a scam.
- **It is illegal to offer lottery tickets over the phone or through the mail.** Anyone who contacts you to offer lottery tickets is trying to cheat you.

## Scam Story

A person calls you from a number you don't recognize and tells you that you won a $3,000,000 prize in a lottery. The caller insists that you must pay taxes on the winnings before you can collect the money and instructs you to go to your bank to wire funds to an out-of-state account. From there, the money usually ends up overseas. The scammer may even steal money from your account because you gave him account information.

**Remember:** Legitimate lotteries do not require you to prepay fees or taxes. Never give out your personal information over the phone. Scammers try to play on your emotions to get you to give them your information. Be skeptical and call our office if you're unsure of a caller's authenticity.

# INVESTMENT SCAMS

You want financial security and the ability to leave a nest egg for your children and grandchildren. Scammers often target seniors with fake annuity or investment opportunities. Unfortunately, with many money-making offers, the only person who makes money is the person who is selling them. If someone offers you a deal to make money that sounds too good to be true, it could be a scam.

You can avoid money-making scams by **following these tips:**

- **Make sure you understand an agreement before you sign.** Read all forms completely and consult with a knowledgeable friend or professional before you agree to anything. Never invest in or buy something that you don't understand.
- **Make sure the offer is legitimate.** The North Carolina Secretary of State's office regulates securities and the people who sell them. Before you buy, call their Investor Hotline at (800) 688-4507 to learn more about a seller. You can also contact our office to determine if a seller is legitimate.
- **Beware of high-pressure sales pitches.** Avoid offers that are only good "now or never." Remember, if it sounds too good to be true, it probably is. You should never make a decision or share financial information under pressure.

## Scam Story

A mortgage lender offers you a loan to consolidate your debts, help your grandchildren go to college, or pay for home improvements. The caller tells you that this offer is for a limited time only and you must act in the next 10 minutes. It sounds like a great offer, but the loan is a bad deal for you because it includes a high interest rate and expensive hidden fees. The end result is that you quickly lose equity in your home and continue to face high payments for a modest loan.

**Remember:** Money-making scams often target seniors because their home mortgages have already been paid off and they want to help pay for their grandchildren's expenses. Never act quickly without verifying an investment or product. If anyone offers you a loan, hang up and call our office or a trusted lawyer or financial advisor.

# TECH SUPPORT SCAMS

Tech support scams are increasingly common. Scammers contact their victims by phone, email, or through pop-up messages on a home computer. The scammer claims to have found a problem with the computer that they can fix if the victim allows remote access to the computer. Once the scammer gains access to the computer, they can access any information stored on it or on any network connected to it. Even password-protected information is vulnerable, as the scammer can install malware that uncovers usernames and passwords.

You can avoid tech support scams by **following these tips:**

- **If someone claiming to be from a tech company contacts you by phone, email, or text message, do not respond.** Legitimate tech companies won't contact you in any of these ways.
- **If you receive a pop-up message on your computer telling you to call or click on a link because something is amiss with your computer, don't click and don't call.** Real tech companies will never ask you to call or click on a link, and clicking the link can allow the scammer to install malware.
- **If you think there's something wrong with your computer, update your security software and run a scan.**
- **If you're looking for tech support, find a company you know and trust.** Many software companies offer support online or by phone, and stores that sell computer equipment also offer technical support in person.
- **If you gave a scammer remote access to your computer, update your computer's security software.** Then, run a scan and delete anything that it identifies as a problem.
- **If you gave your username and password to a tech support scammer, change that password right away.** If you use the same password for other accounts or sites, change it there, too.

## Scam Story

A pop-up message from a well-known tech company appears on your home computer, stating that your computer is at risk due to suspicious activity. The message gives you a link to click or a number to call. You call the number and speak with a "technician" who instructs you to give them remote access to the computer, at which point they gain entry to your bank account and steal your money. The scammer also asks for credit card information as they sell you a worthless computer maintenance service.

**Remember:** If a tech company contacts you out of the blue and offers to fix your computer, that contact is likely the beginning of a scam. Do not allow remote access to your computer and do not give out any personal information.

# HEALTH CARE SCAMS

We all want to keep ourselves and our loved ones safe. Scammers often attempt to exploit fears of getting sick to steal people's money and personal information. If someone contacts you offering miracle cures, free prescription medication, or relief for medical bills, it could be a scam.

You can avoid health care scams by **following these tips:**

- **Avoid products that are too good to be true. Be skeptical of products that claim to be miracle cures or say they have a secret ingredient.** Remember that scammers often try to make you excited to cloud your judgement.
- **Never buy a product or share your information unless you're sure of the seller's authenticity.** If someone contacts you and you haven't heard of them, hang up and call your doctor or our office.
- **Get medical advice from your doctor.** Scammers may call offering treatment for chronic pain or other ailments, but only take advice from your trusted doctor.

## Scam Story

You received a letter offering a product that claims to provide relief for your illness or chronic medical condition. It comes with a money-back guarantee, which helps convince you to try it. But the guarantee requires you try the product for at least four months, and by then the company that sold it to you has disappeared. You ask your doctor about the product after you bought it, and they tell you it won't treat your condition anyway.

**Remember:** Scammers target seniors with products that treat common ailments, like chronic pain. Criminals often push snake oil products that don't work. Before you buy a product, always check with your doctor to make sure it is legitimate.

# HOME REPAIR SCAMS

Homes need regular maintenance and repair, but don't let scammers trick you into paying for improvements you don't need. Many scammers knock on your door and offer to do a simple job, such as cleaning your gutters. Then, the scammer claims they found other problems that need immediate repair. If someone you don't know comes to your door and offers to fix a problem with your home you weren't aware of, be wary.

You can avoid home repair scams by **following these tips:**

- **Stick to reputable contractors and companies.** Stick to companies you trust or get a referral from a friend. Check credentials – especially whether the contractor is licensed by the North Carolina Licensing Board for General Contractors – and contact our office or the Better Business Bureau to learn if a company has been the subject of lots of complaints. Under North Carolina law, a contractor must be licensed to solicit or do work costing $30,000 or more.
- **Don't fall for the gambit of a contractor or handyman offering to do one job but then claiming to find other problems needing repair.** These scammers often move from neighborhood to neighborhood or even from state to state. Out-of-state phone numbers or license plates are telltale signs that the person at your door is a scammer.
- **Never pay upfront.** Be very wary of any request to pay deposits or other fees for tree removal or cleanup in advance. Only pay when the work is done and you are satisfied. Avoid paying with cash. Use a check or a credit card instead – that way your bank can stop the payment if the work isn't done.
- **Don't let anyone rush you.** Take your time to make a good decision. Get a second opinion and compare prices before you agree to a deal. If an offer is only good "now or never," find someone else to do the job.

## Scam Story

A contractor you don't know knocks on your door. He says his crew just paved another driveway in the neighborhood. They have some leftover paving material and can repave your driveway for an excellent price if you agree to do it now. They coat the driveway with a thin layer of asphalt but tell you they did more work than anticipated, and they therefore insist you pay a lot more than the agreed-upon price. A $3,000 job becomes $8,000, and a few weeks later the new surface crumbles, but the contractor is long gone.

**Remember:** Be skeptical of anyone who knocks on your door unexpectedly. Scammers may try to build credibility by saying they did work at a neighbor's house. Only do business with contractors you trust or have verified with our office, the Better Business Bureau, or the NC Licensing Board for General Contractors, and always get a second opinion on any work that needs to be done.

# CHARITY SCAMS

Making a donation to a charity or nonprofit is a great way to give back to your community. North Carolinians contribute billions of dollars to charity each year, and criminals often try to take advantage of people's good intentions to steal their money. Make sure that when you donate money, it goes to helping others, not lining the pockets of scammers.

You can avoid charity scams by **following these tips:**

- **Make sure the charity is legitimate.** Research charities before giving by calling our office and checking their license with the Secretary of State. You can also use resources including the Better Business Bureau's Wise Giving Alliance, Charity Navigator, Charity Watch, or GuideStar to research charity organizations.
- **Give to charities you know.** Be cautious of crowdfunding websites and unsolicited emails, text messages, and social media posts asking you to donate. Instead of responding to solicitations, give to organizations you've heard of or seen do good work in your community.
- **Pay by credit card or check.** Cash gifts can be lost or stolen. For security and tax record purposes, it is best to pay by credit card. If you do write a check, make sure you make it out to the charity directly, not a third-party fundraiser. If anyone asks you to pay with prepaid gift cards or debit cards, it is probably a scam.

## Scam Story

You receive a phone call from an unknown number after a recent hurricane. They say they are from a charity you haven't heard of and they are raising money to help hurricane cleanup costs. The caller tells you they need the money within 24 hours so it can be put to use. When you ask how to donate, they ask you to mail them a prepaid debit card with your donation.

**Remember:** Scammers often try to pressure victims into making donations quickly to cloud their judgement. They also may reference recent disasters to add urgency to their solicitations. Never trust someone you don't know from an organization you haven't heard of. Instead, hang up and call our office to see if the charity is legitimate. Never make a donation with a prepaid card. Use credit cards or checks to keep a record of your donation.

# IMPOSTER SCAMS

Scammers will often pretend to be people with authority, like a government agency, law enforcement, or even your bank. Sometimes they scam you by offering a bogus government grant, which they claim you will receive after you prepay various fees. They might use the threat of legal consequences, arrests, or fines to get your money before you're able to think clearly. But government and law enforcement representatives don't call you to threaten arrest, and they won't ask you to pay your way out of it.

You can avoid imposter scams by **following these tips:**

- **Don't rely on caller ID to decide if a call is trustworthy.** The caller ID might show the government agency or company's name to make it look real. Scammers use spoofing technology to make their calls look legitimate.
- **Hang up and call the company or government agency directly.** Using a number listed on their website, call the company to ask if the call is legitimate.
- **If they're threatening arrest, it's a scam.** Don't send them money or personal information.
- **Always remember that the IRS will never call you about alleged unpaid taxes.** If you truly owe money to the IRS, the IRS will contact you by mail.
- **Never give your money to someone who demands payments from gift cards, wire transfers, or cryptocurrency.** Scammers use these methods because they are difficult to track. It is nearly impossible for law enforcement to recover money once it has been sent. Demands to use a payment method like these are a clear sign of a scam.

## Scam Story

You get a call saying that the sheriff's office has put out a warrant for your arrest because you failed to appear for jury duty. You can pay a fine or you'll have to serve jail time. If you agree, the caller says they'll transfer you over to the county clerk's office to make your payment. The money you pay goes directly in the scammer's pocket.

**Remember:** Law enforcement and government agencies don't call and demand payment over the phone in exchange for not getting arrested. Look up the number for the sheriff's office independently and call them.

# GRANDPARENT SCAMS

Criminals will sometimes pretend to be your family member in trouble and in need of money. They find out who your loved ones or grandchildren are by scouring the internet and social media. Then, when they call you, they have enough information to make the call sound real. They pretend to be your family member and ask for money to get out of a crisis. They may even use artificial intelligence (AI) to create a voice recording that sounds exactly like your grandchild. They ask you to wire money or load funds onto gift cards. We all want to help our loved ones when they are in difficult situations, but we can't let our concern rush us into falling for a scam.

You can avoid grandparent scams by **following these tips:**

- **Verify with someone you trust.** Call another relative or call the relative who claims to be in trouble. Verify even if the caller asks you not to.
- **If someone claims to be a loved one, ask the person questions that only your real family member would be able to answer.**
- **Share carefully on social media.** Make sure your privacy settings prevent strangers from accessing information about you or your family.
- **Never wire or send money in response to a phone call, email, or online message.** Once the money has been received by a fraudster, it's almost impossible to get it back.

## Scam Story

You receive a call from your grandson, who is terrified and asking for your help. He says he's been traveling with friends and was in a car accident and has to pay damages to the person he injured. He pleads with you not to tell his parents and claims he has no money. He asks you to go to your bank and wire funds to him so that he can pay the person he injured.

**Remember:** Never send money to someone unless you've verified who you're speaking to by talking to others or by looking up numbers online.

# CRYPTOCURRENCY SCAMS

Cryptocurrency is a relatively new digital currency, which can be used to either pay for purchases or to make investments. Scammers love to capitalize on cryptocurrency transactions because they are difficult to understand, irreversible, and hard to track back to the scammer. Cryptocurrency also has fewer legal protections, so there's often no legal recourse if you're scammed. If you're going to invest in cryptocurrency, do your research, ask for expertise, and don't fall for promises to get rich.

You can avoid cryptocurrency scams by **following these tips:**

- **Watch out for unsolicited messages that seek payment specifically in cryptocurrency.** Anyone who requests payment through wire transfer, gift cards, or cryptocurrency could be a scammer.
- **Be extremely skeptical of get-rich-quick guarantees.** If someone promises you fast profits in return for you sending cryptocurrency, it's probably a scam.
- **Make sure you know exactly who you're doing business or investing with.** Search their name, or the name of the company, with the words "scam" or "review" to validate their credibility. If you are unsure if a company is legitimate, call our office before doing business with them.
- **Be wary of impersonators.** Just because someone tells you who they are or who they represent, it does not mean it is the truth.
- **Do not fall for scare tactics.** Any message that threatens consequences if you do not send cryptocurrency is a scam.

## Scam Story

Elon Musk, the founder of Tesla, emails you and tells you he's investing in a cryptocurrency project that's going to triple his money. He says he's confident about the value of the project and wants you to join him in making an investment that will triple your profits as well.

**Remember:** Don't fall for impersonators or get-rich-quick schemes. Do your homework before you make any financial investments.

# PHISHING SCAMS

Most of us store our most valuable personal and financial information on our phones, computers, and online accounts. That means our data is more vulnerable to hacking attempts, including phishing scams. Scammers will pretend to be a friend, your bank, or another organization you trust and ask for money or claim you need to make a payment immediately. Most “emergencies” are really just scams.

Don’t let phishing scammers hack you by **following these tips:**

- **If you get an email or a text, look at it closely.** Hover over the sender’s email to see whether the address is legitimate. Look out for spelling and grammar errors, messages at unusual times of day, or any other red flags that strike you as odd – if anything seems off, don’t click on or open the message.
- **Don’t open emails,** click links, or download attachments from people you don’t know.
- **Use strong passwords,** change them regularly, and don’t share them with others.
- **Never send personal information,** like your Social Security number or bank account information, over email or text.
- **Remember, if you’re asked to pay via gift card or Bitcoin, it’s a scam.**

## Scam Story

You get an email from your bank at 3 a.m. that says your account has been overdrawn and is about to be frozen. You’ll need to wire $3,000 immediately to maintain access to your bank account. The email includes a link to log into your bank account and make the payment.

**Remember:** If you receive an email asking for money or highlighting an issue you need to address, call the organization directly at a number you know to be true so you can verify.

# AFFINITY SCAMS

Scammers often prey upon your relationships and connections. The easiest way for a scammer to get you to trust them is to use the relationships you already have – your school, your colleagues at work, your friends at church, or your softball league. Scammers might reach out to you pretending to be another member of an organization you're a part of, or they might use your hobbies, interests, or cultural or professional background to forge a connection with you and gain your trust. Once they gain your trust, you're less likely to question them or their motives if they ask for money or if they try to sell you something.

You can avoid affinity scams by **following these tips:**

- Even if someone claims to have a connection with you, **verify that they are who they say they are.** Reach out to others in your group or someone you know and trust.
- **Do your own research.** Regardless of what someone might claim, either in trying to sell you a product or asking you for money, take the time to verify it on your own.
- **Don't let the pressure get to you.** If an opportunity is time-limited or will go away shortly, it's probably a scam. Scammers often create a nonexistent deadline to put more pressure on you.
- **Don't respond to emails you weren't expecting.** If someone you don't normally email with, or an organization you don't normally hear from, reaches out via email or text, be on your guard and call or otherwise verify whether it's real.

## Scam Story

You get an email from someone who claims to work for churches, including yours, to help churchgoers make the best investments for their future. He says he's helped others at your church increase their profits and put aside enough money for retirement. He says he's a pastor's son who believes deeply in using his talent and connections to help his fellow churchgoers. He offers to invest $500 for you as an initial investment, so you can see how much money you might earn.

**Remember:** When it comes to your money, be sure to research thoroughly before you give it to someone else. Make sure they're a legitimate person for you to do business with.

# REQUEST A PRESENTATION

The North Carolina Attorney General's Office provides presentations about scams and identity theft to groups of consumers across the state.

For more information or to schedule a presentation for your group, please visit www.ncdoj.gov/outreach or contact:

Public Protection Section
North Carolina Department of Justice
Attorney General's Office
9001 Mail Service Center
Raleigh, North Carolina 27699-9001
Telephone: (919) 716-6780
Email: outreach@ncdoj.gov