12 Alarming Scams

INFO THAT SENIORS NEED TO KNOW

1. The grandparent scam

- How it works: The grandparent scam is a type of social engineering attack in which fraudsters claim the victim's grandchild is in trouble. Imposters pretending to be the police call and say that their grandchild has been in an accident or is involved in a crime.
- Scammers will then ask their targets to take out large sums of money or make a wire transfer to "save" their grandchild.
- The scammer will even use the real name of the victim's grandchild along with other identifying information that they find online to make the scam more believable. In other cases, the fraudster will even pretend to be the grandchild and claim to be in trouble.
- In a recent version of this scam, fraudsters send ride-sharing services like Uber to pick up the cash in an envelope.

Warning signs of grandparent scams:

- You receive an unsolicited call claiming that a grandchild or loved one is in danger.
- The caller asks for money as cash, gift cards, or wire transfers.
- The caller won't let you get off the phone or threatens you if you try to verify the information.
- The caller uses deception, intimidation, and coercion to force you to act quickly.
- **Related:** The 5 Best Identity Theft Protection Services For Seniors

2. Government imposter scams

- **How it works:** In this senior scam, fraudsters contact older people claiming to be representatives from a well-known government agency. This could include Medicare, the Internal Revenue Service (IRS), or the Social Security Administration (SSA).

- Fraudsters may use caller ID spoofing to make the call seem genuine. And once you're on the line, they may parrot your Social Security number (SSN) to further legitimize the call.
- Government imposter scams have different risks. Here are a few examples:
- **Medicare scams:** Scammers claiming to be Medicare representatives call their victims to "verify" their Medicare number. If you oblige, they'll use it to steal your health benefits (i.e., medical identity theft). Or, they might claim that the victim needs to pay a fee to receive a new card or special treatments and ask for their credit card numbers.
- **IRS scams:** During tax season, scammers will call elderly people claiming to be from the IRS and saying there's an issue with their return. They'll collect information to "secure" your tax file, but in reality, they'll use it to file phony tax refunds and commit identity theft.
- **Social Security scams:** In this scam, the imposter claims your SSN has been suspended due to an alleged crime. In order to reinstate it, they will demand payment usually in the form of gift cards.
- **FBI or law enforcement scams:** Scammers will even call claiming that there is a warrant out for the victim's arrest. If they don't pay a fee or relinquish their financial information, they could go to jail.
- **Covid scams:** Fraudsters take advantage of the fear and uncertainty of the pandemic to trick seniors into giving up sensitive data — such as bank accounts or health insurance information.
- Remember, these agencies will almost never reach out to you over the phone — especially if it's something as grave as a crime. If they do call, hang up and call the agency's official phone number.
- **Warning signs of government imposter scams:**
- You get an unsolicited call from someone claiming to be from a government agency.
- The caller uses threatening language and wants you to pay them using gift cards or wire transfers.
- The caller asks for your sensitive information, like your SSN, Medicare number, or credit card.
- **Related:** What Can a Scammer Do With Your Medicare Number?

3. Elder financial abuse

- **How it works:** Elder financial abuse happens when someone the victim knows and trusts — like a family member, close friend, or caregiver — tries to gain access to the senior's savings, credit, or assets. They could trick their victim into signing over access or power of attorney. Or, they might even threaten to withhold care if they don't receive access.
- **Warning signs of elder financial abuse:**
- Unfamiliar charges, new accounts and loans, or credit inquiries that you or your elderly loved one didn't make.
- Calls from companies or credit providers about debt you didn't take out.
- An elderly parent or grandparent has unexpected financial struggles.
- **Take action:** If you or a family member accidentally give scammers personal data (or its leaked in a data breach), they could take out loans in your name or empty your bank account. Try an identity theft protection service to monitor your finances and alert you to fraud.

4. False investment scams

- **How it works:** Seniors often spend a lifetime saving to achieve financial security. But that puts them at risk of false investments designed to steal their hard-earned money.
- In an investment scam, criminals pose as prudent financial advisors. They'll call unannounced with what appears to be a lucrative investment opportunity. However, this is an attempt to extract transaction fees or steal "investments" from their targets.
- There are several types of investment scams that specifically target seniors:
- **Ponzi schemes:** A Ponzi scheme uses the money from new investors to pay existing ones (rather than generating any actual returns). Ponzi schemes target seniors by promising high returns with little to no risk.
- **Illegitimate bonds and certificates of deposits (CDs):** In these scams, fraudsters use low-risk investments to trick wary seniors into investing. But these investments either don't give the return that they promise or don't exist at all.

- **Charitable gift annuities:** Here, a donor gives a large sum of money as a gift in return for a fixed income stream. But often, these charities don't exist and you're putting money right into the scammer's pocket.
- **Prime bank scams:** In this scam, con artists claim to have access to "secret overseas markets." But the whole narrative is a scam and any money you send is stolen.
- When it comes to avoiding senior investment scams, remember the golden rule of fraud: **If it seems too good to be true, it probably is.**
- **Warning signs of false investment scams:**
- They promise high returns with little or no risk involved. No investment is 100% safe or can guarantee returns.
- The "advisor" uses high-pressure sales tactics to get you to act quickly and without doing your due diligence.
- You're unable to withdraw your principal investment.

5. Tech support scams

- **How it works:** In this type of fraud, the scammer masquerades as a tech support representative from a company you trust like Apple or Microsoft. They'll claim that your computer or device is at risk of being infected by viruses and then trick you into granting them remote access or paying for software that you don't need.
- Sometimes, the goal is to trick the victim into downloading what they ***think*** is helpful software. But when they do, it's actually malware that opens up the potential for cyber attacks that target the victim's banking information.
- This scam often happens through phone calls, but it's also common to see pop-up ads on websites targeting seniors.
- According to FBI's most recent report, tech support scams have cost seniors over $200 million in losses.
- **Warning signs of tech support scams:**
- You receive unsolicited phone calls about tech support. • Companies like Apple will never proactively call you about these issues.
- A pop-up ad on a website claims that your device has viruses or promises to "speed up" your computer.
- The caller uses fear tactics to trick you into downloading software or clicking on links in emails.

- **Related:** The 7 Latest Geek Squad Scams (and How To Avoid Them)

6. Robocalls and phishing messages

- **How it works:** Seniors are more susceptible to telemarketing and phishing scams than other age groups. With robocalls and spam attacks, vast numbers of emails or calls are made to exploit inexperienced or vulnerable targets.
- **These messages all follow a similar pattern.** The call or message claims to be from a company or group you know and trust — like your bank, the IRS, or even companies like Netflix. But if you engage, they'll try to wrest personal information, passwords, or financial account information from you.
- **Spam emails are especially dangerous.** If you click on a link or download an attachment, you could unwittingly download malware that gives the hacker remote access to your device.
- **Warning signs of robocalls calls and phishing messages:**
- **You receive automated messages** that claim that you're in trouble or at risk. The IRS and other agencies will never use automated calls to get in touch with you.
- An email or caller asks you to "verify" sensitive information in order to secure an online account.
- An email or message includes a link or an attachment that you don't recognize or weren't expecting.
- **Related:** How To Identify a Medicare Scam Call: 7 Scams To Watch Out For

7. Sweepstakes and elder lottery scams

- **How it works:** Fraudsters reach out to an elderly victim and claim that they've won a contest, lottery, or sweepstakes that they never entered. But to receive winnings, they'll need to pay upfront fees and taxes and supply their banking information for the transfer.

- Scammers will often string along their victims for months or years, claiming that they need additional payment. But any money that's sent goes straight to the scammer.
- **Warning signs of sweepstakes and lottery fraud:**
- You or a loved one receives a notification that you have won a large sum of money from a contest you never entered.

- The person you speak with asks for upfront payment through non-traceable methods (gift cards, wire transfers, etc.)
- They ask for your banking information to complete the deposit.
- **Related:** How To Spot (and Avoid) Publishers Clearing House Scams

8. Romance scams

- **How it works:** In this type of elder fraud, scammers create fake personas on dating apps or social media to lure their targets. Con artists will research you online and use details that you've shared publicly to entangle you.
- Once they establish a rapport, scammers begin to request money, often in the form of gift cards, travel expenses, or healthcare costs.
- Seniors lost the most amount of money to tech support, identity theft, and romance scams. Source: FBI Elder Fraud Report
- Many victims of romance scams are pressured into fraudulent investments, especially involving cryptocurrencies. Even worse, those aged 50–69 made up the majority of victims, losing a total of $179.65 million in the first three quarters of 2022 alone. Always keep yourself safe and be aware of the dangers of online dating.
- **Warning signs of elderly romance scams:**
- The "relationship" moves at a frantic pace, with the other person claiming to be irrevocably invested.
- They promise to meet up in person or on video chat but always come up with an excuse at the last minute.
- They ask for money or financial help for family or healthcare issues.

9. Funeral scams

- **How it works:** In one of the most vile forms of elder fraud, con artists target deceased people with funeral scams. Scammers raid obituaries and then attend funerals claiming that the deceased has an outstanding debt.

- **Warning signs of funeral scams:**
- Someone you don't know demands payment at a funeral.
- You're approached by an individual who claims to know the deceased but has no tangible evidence of their relationship.

10. Reverse mortgage scams

- **How it works:** Many seniors would have built equity in their homes that they want to turn into a reliable and steady income. Reverse mortgages are available to homeowners over the age of 62 as a way to access their home equity.
- But scammers target the elderly with billboards, ads, and fliers for reverse mortgage scams. They'll claim to be helping you get access to your equity. But in reality, they either steal the money or even commit deed fraud and "steal" your home.
- **Here are a few other variations of a reverse mortgage scam:**
- **Mortgage relief:** Seniors in need of financial aid might want to use a reverse mortgage to avoid foreclosure. Scammers target them with claims of fast approval on loans in exchange for an upfront fee.
- **Fraudulent contractors:** Sometimes scammers will come to your home and offer free consultations. They'll convince elderly homeowners to take out a reverse mortgage and pay for pricey and unnecessary repairs or home "updates."
- **Warning signs of reverse mortgage scams:**
- High-pressure sales tactics that try to get you to consent to a reverse mortgage without doing your due diligence.
- Someone claims that they need power of attorney in order to finalize a reverse mortgage.
- Contractors or vendors suggest that you take out a reverse mortgage to pay for costly repairs.
- **Related:** How To Stop Car Extended Warranty Scam Calls For Good

11. Online shopping scams

(Fraudulent products, non-delivery, etc.)

- **How it works:** Online scams are rampant. But senior citizens are especially vulnerable to online shopping scams. The FBI received over 13,000 complaints of fraudulent products and non-delivery in 2021 — making it the second most reported fraud among the elderly.
- Online shopping scams come in many different forms. You could buy fraudulent pharmaceutical drugs or health and beauty products. Or, you could use your credit card details on a phishing site that is set up by hackers.
- **Warning signs of online shopping scams:**
- Poor design or spelling errors on the website.
- The website you're shopping from is unsecure. This means it uses HTTP and not HTTPS.
- Example of a secure website URL from a government website Secure websites use https not http and should include a lock by the URL.

12. Charity scams

- **How it works:** Charity scams prey your desire to help others. Fraudsters pretend to be a legitimate charity and steal donations and personal information. Fraudsters will also often call elderly victims in the wake of a natural disaster.
- They'll claim to be helping victims and solicit donations. But if you send money or give them your financial information, they'll disappear with them.
- **Warning signs of charity scams:**
- The charity doesn't appear on official sites like Charity Navigator or the BBB Wise Giving Alliance.
- You find evidence of fraud when you Google the charity's "name + fraud/scam/complaint".
- The charity's name is very similar to a larger organization you're familiar with.