



10 common scams and how to avoid them

TECHNOLOGY & INNOVATION

Familiarize yourself with these common swindles, often targeting retirees.

As we age, we may become more susceptible to fraudsters who make a living preying on retirees. This can be especially true for widows and widowers who are making decisions alone and may be particularly trusting of friendly strangers. In order to protect ourselves and those we love, it's important to be aware of the most common scams older Americans fall for.

1. Lottery scam

You get an unsolicited phone call or email saying you've won a large prize. All you need to do is send money to pay for shipping, taxes or some ancillary fee. You send the money, but the fictional prize never arrives.

2. Grandchild scam

Your grandchild calls to confess her troubles. Or so you think. It's not uncommon for someone posing as your grandchild to call and, preying on your compassion, claim to be in a crisis situation and need money urgently. They may also beg you not to call their parents (which would give the scam away).

3. Charity scam

You donate to one charity and end up being on every charity list. That's because they sell your name, phone number and email to other nonprofit and commercial organizations. These could include companies with similar names to charities you support – but they exist solely to scam donations.

4. Computer scam

Someone calls pretending to be from a major company, such as Microsoft, and says he can see that your computer has a virus. He offers to help you get rid of it by asking you to log into a website that lets him control your computer – and then steals your ID information.

5. Timeshare scam

If you own a timeshare, you may get a call from someone claiming they're authorized to sell it for you, for a fee. After paying, however, you never hear from them again.

6. Homeowner scam

A man comes to your door and offers to clean your gutters or trim your trees, which sounds like a good idea. Until he asks for prepayment and never completes the job.

7. Medical scam

You get an unsolicited call about a discounted price for some kind of medical equipment (i.e., heart monitor, wheelchair or bathtub bench). You're asked for a deposit and your personal information or Medicaid number to send the equipment, which never arrives.

8. Foreclosure scam

You're approached by a "professional" who claims your home is under threat of foreclosure and offers to pay off your mortgage or taxes if you sign over the deed to the property. With your deed, the fraudster can then refinance the mortgage for the full value of your home and take the money. Keep in mind, even if you sign over a deed to someone, you are still liable for your mortgage obligations.

9. Caregiver and sweetheart scam

These predators claim to care deeply for you or your well-being, but after winning your trust, they gain access to your accounts to steal money or identity information.

10. Title company scam

Before purchasing or closing on a new property, a scammer intercepts an email from your real estate agent or title company. You're then sent fraudulent payment instructions to complete the transaction. Red flags include last-minute changes to instructions, a change in tone or word choice from prior emails, a new sender address and multiple payment requests.

These scams are common and widespread. But speaking with trusted loved ones or your financial professional before making decisions can help you avoid these traps. Additionally, keep in mind these tips for staying safe:

- Don't pay for things you don't remember ordering.
- Don't give your personal information to unknown third parties.
- Work with financial institutions that use fraud protection to safeguard your credit card and banking information.
- Don't click links in the body of suspicious emails, especially if they claim to come from your bank, credit card company, real estate agent or title company. Instead, log in to the company's official website or call them directly to verify.
- Don't let strangers into your house. Instead, ask for a business card and say your spouse, kids or lawyer will be in touch.
- Be wary of caregivers and suitors, especially if you notice signs of substance abuse or other red flags.

- Limit the purchases and donations you make by check, which may list your home address or other key data.

If you suspect you've fallen victim to a scam or that your identity has been compromised, it's time to act. Report the incident to your advisor right away to help protect your accounts, and consult [identitytheft.gov](https://www.identitytheft.gov) to see the Federal Trade Commission's recommendations for critical next steps. Additionally, reporting cybercrime incidents to the [FBI](https://www.fbi.gov) can help federal agencies respond quicker and more effectively to threats.