Elder Fraud Prevention Guide

Common scams, red flags, and safeguards to protect against financial exploitation

Older adults are targeted by scams more than any other age group, often because fraudsters assume they have savings, live alone, or are less likely to report it. This guide covers the most common scams, the warning signs, and the safeguards that make the biggest difference.

1. Common Scams to Know

- Grandparent/family emergency scam — a caller claims to be a grandchild in trouble and needs money wired immediately
- Government imposter scam — a caller poses as the IRS, Social Security, or Medicare, threatening arrest or loss of benefits
- Tech support scam — a pop-up or call claims the computer is infected and asks for remote access or payment
- Sweepstakes/lottery scam — a notice claims a prize was won, but a fee or taxes must be paid first
- Romance scam — an online relationship develops, followed by requests for money
- Home repair or contractor scam — an unsolicited offer for repairs, often demanding payment upfront for incomplete or unnecessary work
- Medicare/health insurance scam — a caller requests a Medicare number to send a free device or supplies
- Grandparent-of-the-bank scam — a caller posing as a bank or credit card fraud department asks for account numbers or a PIN to 'verify' a purchase

2. Red Flags of a Scam

- Pressure to act immediately or keep the request secret from family
- A request for payment by gift card, wire transfer, or cryptocurrency
- An unexpected call, text, or email asking to confirm personal or financial information
- A caller who already seems to know some personal details, used to build trust
- Any request for a Social Security number, Medicare number, or bank PIN over the phone
- An unfamiliar number claiming to be a known agency, bank, or family member

> *Legitimate government agencies and banks will never ask for payment by gift card or demand immediate payment over the phone. That request alone is a reliable sign of fraud.*

3. Everyday Protective Habits

- Do not answer calls from unknown numbers; let them go to voicemail

Elder Fraud Prevention Guide

Common scams, red flags, and safeguards to protect against financial exploitation

- Hang up and call the organization directly using a number from an official statement or website
- Never give personal, banking, or Medicare information to an unsolicited caller
- Talk to a trusted family member before sending money or gift cards to anyone unfamiliar
- Set up a family code word to verify emergencies before sending money
- Register home and cell numbers with the National Do Not Call Registry
- Shred documents containing personal or financial information before discarding

4. Protecting Finances & Accounts

- Set up account alerts for withdrawals, transfers, or new charges
- Review bank and credit card statements monthly for unfamiliar activity
- Consider a trusted contact designation on bank and investment accounts
- Freeze credit reports with the three major bureaus if not actively applying for credit
- Use strong, unique passwords and enable two-factor authentication where available
- Be cautious about sharing financial details even with new friends or online contacts

5. Online & Phone Safety

- Never click links or download attachments from unexpected emails or texts
- Verify a website address before entering any personal information
- Be skeptical of urgent pop-ups claiming a computer is infected
- Avoid giving remote access to a computer to anyone who calls unsolicited
- Be cautious with new online relationships that quickly ask about finances

6. If You Suspect Fraud

- Stop all contact and payment immediately
- Do not be embarrassed to tell a family member — scammers count on silence
- Report to local police and file a report with the FTC at reportfraud.ftc.gov
- Report to the NC Department of Justice / Attorney General's Consumer Protection Division
- Contact the bank or credit card company immediately if money or account numbers were shared
- Place a fraud alert or credit freeze with the credit bureaus if personal information was exposed

> *The Adult Protective Services line and local police non-emergency number are worth keeping posted alongside other emergency contacts, so reporting fraud is a quick call, not a search under stress.*

7. How Family & Caregivers Can Help

- Check in regularly and ask openly about any unusual calls, texts, or emails received
- Help set up account alerts and review statements together periodically
- Keep communication judgment-free, so concerns are shared early rather than hidden
- Share this guide with other family members and caregivers involved in day-to-day support

---

Home Helpers® Home Care caregivers get to know clients well and are an extra set of eyes for unusual activity, unfamiliar visitors, or signs of financial exploitation. The Cared-4℠ program's regular Wellness Calls also give clients another consistent, trusted voice to talk things through with before acting on any unexpected request.