10-Minute Scam Check

Senior Fraud Guide | seniorfraudguide.com

Print this page and keep it beside the phone or on the refrigerator. Work through the four parts whenever a call, text or offer makes you feel rushed.

1. Pause: six red flags that mean stop

1. Urgency plus secrecy. Real banks, police and government agencies never ask you to keep a payment secret or stay on the line while you go to the bank.
2. An unusual payment method. Gift cards, wire transfers, cryptocurrency or cash by courier are hard to trace and hard to reverse.
3. A request for remote access. No tech company or bank cold-calls you to install AnyDesk, TeamViewer or similar software.
4. An offer too good to be true. Guaranteed returns, a prize you never entered, or a job that pays very well for very little work.
5. A new number and a new photo. Call your family member back on the number you already have saved, not the one in the message.
6. Small errors that add up: odd wording, a mismatched email domain, or a greeting that does not sound right.

2. Check: eight steps that protect you

- [ ] Agree a callback rule: money requests are confirmed on a number you already have.
- [ ] Choose a family code word that is not posted anywhere online.
- [ ] Turn on two-factor authentication for email, banking and social media.
- [ ] Use a password manager with a long, unique password for every account.
- [ ] Ask your bank for alerts on unusual or large transactions.
- [ ] Set social profiles to friends-only; remove public phone numbers and birthdays.
- [ ] Review bank and card statements weekly, and your credit reports each year.
- [ ] Never share a one-time security code, PIN or password with anyone who contacts you.

My family code word: _____

My bank's phone number (from the back of my card): _____

The person I call before I pay anything: _____

3. Report: who to contact

Where to report	What it covers
Fraud and identity theft	ReportFraud.ftc.gov | IdentityTheft.gov – free FTC reporting and a personal recovery plan.
Online crime, including cloned voices	ic3.gov – the FBI's Internet Crime Complaint Center.
Unwanted calls and texts	DoNotCall.gov. Forward spam texts to 7726.
Investment offers	Check the seller at Investor.gov before sending money.
Your bank or card issuer	Call the number on the back of your card immediately; fast reporting can sometimes stop a transfer.
Local police	File a report, especially if someone came to your door or you were threatened.

4. Remember one sentence No bank, government agency, tech company or family emergency has ever required you to buy gift cards, send cryptocurrency, or keep a payment secret. If someone says it does, hang up and call back on a number you looked up yourself.

General educational information, not legal, financial or medical advice. Reporting routes change over time – confirm current details on the official website. A Spanish edition is available at seniorfraudguide.com/assets/scam-check-checklist-es.pdf. (c) 2026 Senior Fraud Guide. You may print and share this page for personal, non-commercial use.