THRIVING SENIOR

Helping seniors live better, one tip at a time

Senior Fraud Defense Checklist

The 15 steps that actually stop scammers - 2026 edition

☐ Guard your Medicare number like a credit card

Your Medicare number is as sensitive as your Social Security number. Never give it to anyone who calls you unsolicited, knocks on your door, or contacts you by email or text. Legitimate Medicare representatives do not call you out of the blue to ask for it. If you need to verify a Medicare question, call 1-800-MEDICARE directly.

☐ Create a family emergency code word today

Choose a simple, memorable word or short phrase and share it privately with your closest family members. If anyone ever calls claiming to be a family member in crisis, ask for the code word before doing anything else. Scammers using cloned voices cannot know a private word your family just created. Write it down and store it somewhere only you can access.

☐ Set a verbal passphrase with your bank

Call your bank using the number on the back of your debit or credit card and ask to add a verbal security passphrase to your account. This is a word or phrase that must be spoken before any transaction can be processed. It adds a layer of verification that phone scammers cannot easily bypass, even if they know your account number.

☐ Review your Medicare Summary Notice every month

Medicare mails or electronically sends a Medicare Summary Notice listing every service billed to your account. Read it carefully each month and look for appointments, procedures, or equipment you do not recognize. If something looks wrong, call 1-800-MEDICARE immediately. Catching fraudulent billing early limits the damage and creates a paper trail.

☐ Freeze your credit at all three bureaus

Contact Equifax, Experian, and TransUnion individually and request a free security freeze on your credit file. You can do this online at each bureau's website or by phone. A freeze prevents new credit accounts from being opened in your name. It does not affect your existing accounts or credit score and can be lifted temporarily whenever you need to apply for credit.

☐ Sign up for FTC scam alerts by email

Go to ftc.gov and subscribe to consumer alert emails. The FTC sends plain-language notices when new scams emerge so you know what to watch for before a scammer calls. Staying current on active scam tactics is one of the simplest and most effective prevention habits you can build, and it takes less than two minutes to set up.

☐ Memorize the gift card rule and repeat it often

No government agency, bank, utility company, IRS official, or law enforcement officer will ever ask you to pay a debt, penalty, or fee using gift cards. If anyone makes this request by phone, text, or email, it is a scam without exception. Hang up immediately. Share this rule with friends and family members so everyone around you knows it too.

☐ Never allow remote access to your computer

If a pop-up message, email, or phone caller claims your computer is infected and asks you to call a number or download software so a technician can fix it remotely, do not comply. Legitimate tech companies like Microsoft and Apple do not contact customers this way. Shut down the browser, restart your computer, and call a trusted local technician if you have concerns.

☐ Register all your phone numbers at donotcall.gov

Visit donotcall.gov or call 877-382-4357 to register your home and cell phone numbers on the National Do Not Call Registry. Legitimate telemarketers are required to honor this list. The registry will not stop all unwanted calls, especially from scammers who ignore the law, but it reduces solicitation calls and makes unwanted calls easier to identify as suspicious.

☐ Place fraud alerts on your financial accounts

Contact each bank, brokerage, and credit card company you use and ask about fraud alert options. Many institutions will text or email you any time a transaction exceeds a threshold you set, a new payee is added, or your account is accessed from an unfamiliar device. Set these alerts as sensitive as the institution allows so you catch unauthorized activity within minutes.

☐ Verify every charity before you donate

Before giving to any charity, especially one that contacts you by phone or email, check it at ftc.gov/charity or use the IRS Tax Exempt Organization Search at apps.irs.gov. Disaster and health-related scam charities spike after major news events. A legitimate charity will not pressure you for immediate payment, and will always allow you time to verify their credentials.

☐ Order your free credit reports annually

Go to annualcreditreport.com, the only federally authorized source for free credit reports, and request your reports from all three bureaus. Review each one for accounts you did not open, addresses you do not recognize, or inquiries from lenders you never contacted. Dispute any errors directly with the bureau that issued the report.

☐ Establish a trusted contact with your broker or advisor

Federal regulations allow financial institutions to accept a trusted contact designation on your account. This is a person the institution can reach out to if they have concerns about your account activity without giving that person any authority over your money. Call your brokerage or financial advisor and ask to add a trusted family member or close friend.

☐ Pause 24 hours before any large financial decision

Commit to a personal rule that you will never move, wire, withdraw, or give money in response to an unexpected request without waiting at least 24 hours and speaking to a trusted person first. Scammers depend on urgency and panic. Introducing a mandatory pause gives you time to verify the situation and almost always reveals the fraud before damage is done.

☐ Know where to report fraud immediately

Keep these numbers and websites written down in a place you can find them: FTC at reportfraud.ftc.gov or 877-382-4357, FBI Internet Crime Complaint Center at ic3.gov, Social Security Administration at ssa.gov or 1-800-772-1213, Medicare at medicare.gov or 1-800-MEDICARE, and your local Adult Protective Services through eldercare.acl.gov. Report even if you are unsure. Reports save others.

What to Do Next

If you have already been targeted or victimized by a scam, report it immediately at reportfraud.ftc.gov and contact your bank or financial institution right away, because the sooner you act the greater the chance of stopping or reversing a transaction. Do not let embarrassment prevent you from reporting: these are professional criminals who target sharp, experienced people, and your report directly helps law enforcement protect others. You can also call the Eldercare Locator at 1-800-677-1116 to connect with a local elder fraud specialist who can guide your next steps.

Print this page. Work through one box at a time. Every box you check is one more layer of protection.