# Scam-Proof Your Retirement

How to spot, stop and report the scams aimed at adults 55+

A large-print guide for adults 55+

SeniorAffair.com

# Start Here

Scammers have never had better tools. A convincing website, a friendly voice on the phone or a message that looks like it came from your bank can all be created in an afternoon. That means the old clues, like a clean design or a confident tone, tell you very little today.

This guide gives you something better: a calm, repeatable way to check any offer, call or message before you act. You do not need to be a technology expert. You only need to slow down.

> **The one rule that beats almost every scam**
>
> - Slow down. Scams depend on speed, secrecy and fear. If someone says you must act right now, that is your signal to stop.
> - Nobody legitimate will be upset if you say, “Let me call you back.”

## Don’t treat everything as a scam

Being careful is different from being afraid of everything. A scam is when someone takes your money or information through lies. They promise something they can’t or won’t deliver, or they hide who they are so you can’t find them later.

A product that disappointed you, a salesperson who was pushy, or a plan that cost more than you hoped is not automatically a scam. Learning the difference keeps you safe without making you distrust honest businesses, family and friends.

# The Tactics Scammers Use

Different scams look different, but most use the same few levers. Learn these and you can spot a new scam you have never heard of.

1. **Urgency.** “Your account will be closed today.” “This offer ends in one hour.” Pressure is designed to stop you from thinking.
2. **Fear.** A caller says there is a warrant, a problem with your Medicare, or a hacked bank account. Fear makes people act first and check later.
3. **Secrecy.** “Don’t tell your family, they won’t understand.” Honest businesses never need you to hide a transaction.
4. **Authority.** They claim to be a government agency, a bank, a tech company or a grandchild in trouble.
5. **Odd payment.** Gift cards, wire transfers, cryptocurrency, cash in the mail or payment apps to a stranger. These are hard or impossible to reverse.
6. **Too good to be true.** A prize you didn’t enter, a guaranteed return, a “free” gift that needs a fee.

## Scams you are most likely to meet

| Scam | How it usually starts | What to do |
|---|---|---|
| Medicare or insurance call | A call, text or email about your Medicare card, a “refund” or a new plan. They ask for your Medicare number or bank details. | Hang up. Look up the official number yourself and call 1-800-MEDICARE (1-800-633-4227). |
| Grandchild in trouble | A voice says, “Grandma, it’s me,” and needs bail or repair money, and begs you not to tell anyone. | Hang up and call your grandchild or a parent on the number you already have. Consider a family code word. |

| Scam | How it usually starts | What to do |
|---|---|---|
| Bank or fraud alert | A text or call says there is suspicious activity and asks you to move your money to a “safe account.” | Never move money on an incoming call. Call the number printed on your card. |
| Tech support pop-up | A screen warning says your computer is infected and shows a phone number. | Close it or turn the device off. Real warnings never ask you to call a number or pay with gift cards. |
| Romance or friendship | Someone online is loving and attentive, but can never meet and soon needs money. | Never send money to someone you have not met in person. |
| Prize or sweepstakes | You “won” something you never entered, and must pay a fee first. | Real prizes don’t charge fees. Stop all contact. |

# How Getting Scammed Hurts

The first hit is the money. The second hit is slower: embarrassment, doubt and the temptation to keep it secret. Scammers count on that shame. Please remember that smart, careful people are fooled every day by professionals whose full-time job is fooling people.

If this ever happens to you, the best thing you can do is tell someone quickly. The faster you act, the more you may be able to recover or stop.

# Read Any Offer Before You Buy

Use this checklist for any offer that reaches you, whether it is a product, a service, a plan or an investment.

- [ ] Can I find a real company name, a street address and a phone number I can call?
- [ ] Can I reach a real person, and do they answer plain questions plainly?
- [ ] Is the price, and everything it includes, clear before I give a card number?
- [ ] Are they pushing me to pay today or keep it secret?
- [ ] Do the reviews sound like real people, or all the same?
- [ ] Would I still want this if nobody pressured me?

### Red flags that deserve a stop

- No company name, address or way to reach a person
- All upside and no risk, with thin proof
- Payment only by gift card, wire, crypto or payment app
- You didn’t ask for the contact
- You are asked to keep it secret

## Research the person behind the offer

- Search the company name with the words “scam,” “complaints” or “reviews.”
- Check the business with your state attorney general or your local Better Business Bureau.

- For a financial professional, ask for their name and check them with the regulator that applies to them before you share anything.
- Ask a trusted person: a family member, a friend, your bank or a librarian.

# Protect Your Money and Information

- Never share your Medicare number, Social Security number, bank details or passwords with someone who contacted you first.
- Use a credit card online when you can. Card issuers generally give you stronger dispute options than a debit card or a transfer.
- Let unknown numbers go to voicemail. You can call back on a number you look up yourself.
- Turn on alerts for your bank accounts so you see activity quickly.
- Consider a free credit freeze with Equifax, Experian and TransUnion.
- Use a different password for each important account, or a password manager.
- Don’t click links in unexpected texts or emails. Type the website address yourself.

## Medicare and insurance caution

Medicare scams are common because everyone on Medicare has a number worth stealing. Treat any unexpected call, text or email about Medicare, a new card, a refund or a plan with suspicion. Medicare cards are free. If you are unsure, hang up and call 1-800-MEDICARE yourself. During open enrollment, compare plans through official tools or a licensed advisor you chose, not a stranger who called you.

# If You Already Got Scammed

Act today. Do these in order. You are not alone, and it is worth reporting even if it feels small.

1. **Stop all contact** with the scammer. Don’t send more money to “fix” it.
2. **Call your bank or card company** right away, using the number on your card. Ask about stopping or reversing payments.
3. **If you paid by gift card,** call the card company at once and report it.
4. **Change passwords** for any account that might be affected, and turn on two-step sign-in.
5. **Place a credit freeze or fraud alert** if you shared personal details.
6. **Report it.** The Federal Trade Commission takes reports at ReportFraud.ftc.gov. For identity theft, use IdentityTheft.gov.
7. **For Medicare fraud,** call 1-800-MEDICARE or your Senior Medicare Patrol (SMP) at 1-877-808-2468.
8. **Talk to someone.** The AARP Fraud Watch Network helpline is 1-877-908-3360.

# Your Scam-Proof Plan

Fill this in now, while you are calm. It will help you later when you are not.

**The three people I will call before I send money or share information:**

**My family “code word” for emergencies:**

**Accounts where I will turn on alerts or a credit freeze:**

### Pocket card

- If I didn’t start it, I don’t trust it.
- I never pay with gift cards, wires or crypto for a stranger.
- I hang up, look up the real number and call back.
- I tell someone before I act.

This guide is for general information and personal reflection only. It is not legal, financial, medical or professional advice. For decisions about your health, money, safety or legal affairs, talk with a qualified professional. Websites, phone numbers and programs change, so confirm contact details on official sites.