The Most Common Telephone Scams Targeting Seniors

1. The Grandparent Scam (AI Voice Cloning)

How it works: Scammers harvest a 3–5 second audio clip of a grandchild from social media (TikTok, Instagram, voicemail), feed it into a voice-cloning tool, and call the grandparent. The cloned voice is crying or panicked, claiming the grandchild has been arrested, been in a car accident, or is in a hospital. A second voice — a fake "lawyer," "bail bondsman," or "officer" — then takes over and gives payment instructions.

Key details:

- FBI IC3 reported **$5M+ in losses** from family-emergency scams targeting those 60+ in 2025; AI-linked fraud grew **400%** year-over-year.
- Typical ransom demanded: **$2,500–$15,000**.
- ~70% of people in independent tests **cannot distinguish** an AI-cloned voice from a real one (McAfee Labs).
- The tools are cheap: a Telegram bot starts at ~$30/week; a cracked voice-cloning account sells for ~$150.

Red flags:

- "Please don't tell Mom and Dad" — **secrecy is the #1 red flag** in virtually every documented case.
- Extreme urgency: "I need this in the next hour."
- Payment via gift cards, crypto, wire, or a courier picking up cash at your door.
- The caller opens with "It's me" or "It's your grandson" and waits for you to supply the name.

Best defense: Agree on a **family code word** (e.g., "Purple Cactus") that only your immediate family knows. An AI clone cannot answer for it. Also: **hang up and call the person directly** at their known number — never use a number the caller provides.

---

2. Government Impersonation Scams (IRS, SSA, Medicare)

How it works: The caller claims to be from the IRS, Social Security Administration, or Medicare and says your benefits will be suspended, your SSN is compromised, or you owe back taxes. They threaten arrest, deportation, or bank seizure unless you pay immediately.

In 2026, scammers have escalated by using **real SSA employee names**, fake badge photos, and forged letters on Supreme Court or SSA OIG letterhead.

Key details:

- FTC received **330,000+ complaints** for government impersonation in 2025, a **25% increase** over the prior year.
- The SSA OIG has issued multiple 2025–2026 alerts about fake letters claiming "SUSPENSION OF SOCIAL SECURITY NUMBER DUE TO CRIMINAL ACTIVITIES."
- Scammers spoof caller ID to display real government phone numbers.

Red flags:

- Threats of arrest or legal action unless you pay **right now**.
- Claim your SSN has been "suspended" — **SSNs cannot be suspended**.
- Payment demanded via gift cards, gold bars, cryptocurrency, wire transfer, or cash pickup.
- A "transfer" to a second caller posing as a law enforcement agent.
- Sending you a photo of a "badge" to verify identity.

Best defense: The real IRS communicates by **U.S. Mail first** and never takes gift cards or threatens arrest. The real SSA will never demand payment or threaten to suspend your number. If in doubt, hang up and call the agency directly at **1-800-772-1213** (SSA) or the number on the back of your Social Security card.

---

3. Tech Support Scams

How it works: A pop-up appears on the victim's computer claiming it's infected with a virus and displays a phone number to call "Microsoft support" or "Apple support." The "technician" asks for **remote access** (AnyDesk, TeamViewer, UltraViewer), "finds" non-existent problems, and charges fees to fix them. Advanced versions escalate: the scammer claims your **banking accounts have been hacked**, transfers you to a fake "bank security officer," and instructs you to withdraw cash, buy gold, or wire money to a "safe" account.

Key details:

- FBI: Tech support scams cost seniors **over $1 billion in 2025**.

- Average per-complaint loss: **~$34,000**; nearly 6,000 older adults lost **more than $100,000 each**.
- Adults 60+ are **5× more likely** than younger people to be victimized.
- One documented case: a 77-year-old Maryland woman authorized **five wire transfers totaling $661,000** over 28 days after a fake Microsoft pop-up.
- A "refund scheme" follow-up: after the initial theft, scammers call back offering a "refund" but claim they overpaid and ask the victim to send gift cards to cover the "overage."

Red flags:

- **Microsoft, Apple, or Google do not make unsolicited support calls. Ever.**
- A pop-up gave you a phone number — legitimate security warnings never include one.
- They ask you to install remote-access software during an unexpected call.
- Payment via gift cards, wire, or cryptocurrency.
- They tell you to keep your computer on (so they can maintain access).

Best defense: Turn the computer off. If you called the number, you're already in the scam. Never grant remote access to an unsolicited caller.

---

4. Prize, Sweepstakes & Lottery Scams

How it works: The victim receives a call, text, or email saying they've won a cash prize, lottery, or government grant. To "claim" the winnings, they must first pay a processing fee, tax, or registration charge. The prize never exists. Variants include:

- **Fake government grants** (e.g., "You've been selected for a $10,000 federal stimulus payment" — pay $500 to activate it).
- **Sweepstakes** where the "winner" must pay customs or shipping fees.
- **Fake investment opportunities** promising guaranteed returns on a "prize fund."

Red flags:

- You never entered a contest but "won."
- You must pay money to receive money.

- The prize is delivered in gift cards, crypto, or prepaid cards.
- Extreme pressure to respond within hours.

Best defense: If you didn't enter, you didn't win. No legitimate prize requires an upfront payment.

---

5. Fake Bank & Medicare Renewal Scams

How it works: These arrive as texts, calls, or emails claiming:

- **Bank:** "We detected unauthorized activity on your account. Call this number immediately to secure your funds." The "bank representative" then asks for account numbers, passwords, one-time codes, or instructs you to move money to a "secure account."
- **Medicare:** "Your Medicare card needs to be renewed. Call this number to avoid a $500 penalty." The caller harvests your SSN, Medicare number, and banking details.

Key details:

- The "Phantom Hacker" variant (warned about by NY AG in 2025) combines a fake hacking alert with **two follow-up calls** impersonating the victim's bank and a government agency, creating a multi-layered trust chain. Since 2024, these coordinated attacks have stolen **over $1 billion**.
- Scammers use **SIM-swapping** or intercept one-time passcodes to bypass 2FA.

Red flags:

- Your bank or Medicare will **never** call you to report unauthorized activity — they'll mail you.
- You're asked for your password, PIN, or one-time code.
- Payment or "transfer" is requested to a "protected" or "safe" account.
- The message contains a link to click.
- The sender's email isn't from the bank's or Medicare's official domain.

Best defense: Hang up and call the number on the **back of your card** or **1-800-633-4227** (Medicare). Never share one-time codes with a caller. If you clicked a link, change your password immediately and contact your bank.

Universal Rules for All Five Scams

Rule	Why
Hang up and call back on a known number	Defeats caller-ID spoofing and voice cloning
Never pay with gift cards, crypto, or wire	No legitimate institution uses these methods
Treat urgency + secrecy as automatic red flags	Real emergencies survive a 5-minute callback
Use a family code word	An AI clone or stranger can't answer for it
Report it — FTC (reportfraud.ftc.gov) or FBI IC3 (ic3.gov)	