Dr. Ed Weir, PhD · 20 Years Inside Social Security
Sergeant, USMC · Over 2 million people turn to Dr. Ed every month

QUICK-REFERENCE CARD · 2026 EDITION

Scams Targeting Seniors: How to Spot Them

The 6 scams draining accounts in 2026 — what's real, what's fake, and exactly what to do.

THE GOLDEN RULES — TRUE FOR EVERY SCAM

- ✓ Real agencies **contact you first by mail**, not surprise calls or texts.
- ✓ **Urgency & threats** ("act now or lose your benefits") = scam.
- ✓ If **they** reached out, hang up and call the **real** number yourself.
- ✓ No real agency demands **gift cards, wire, crypto, or cash**.
- ✓ Never give an **SSN, bank, or one-time code** to someone who contacted you.
- ✓ When unsure, **slow down** and ask a family member. Scammers hate delay.

1 The SSA Impersonation Call

A caller claims to be from Social Security and says your **SSN was "suspended"** over criminal activity, that you owe money, or that your benefits will be cut off. They use threats and demand fast payment by gift card, wire, or cryptocurrency — sometimes with a **spoofed caller ID** showing a real SSA number.

THE TRUTH SSA will **never** threaten you, never suspend your SSN, and never demand payment by gift card, wire, or crypto. If someone threatens you on the phone, it is 100% a scam — hang up.

DR. ED'S TIP SSA does make legitimate calls — but never with threats or payment demands. When in doubt: hang up and call SSA yourself at **1-800-772-1213**.

2 Phishing Emails & Texts

An email or text looks like it's from SSA, Medicare, or "the government." It tells you to click a link to **"verify your identity," "update your account,"** or **"claim your COLA increase."** The link leads to a fake site built to steal your personal information.

THE TRUTH SSA will **never** email or text you a link to enter personal information. Don't click — delete it. Reach SSA only by typing **ssa.gov** into your browser yourself.

DR. ED'S TIP Report Social Security phishing at **oig.ssa.gov**, or call the SSA OIG Fraud Hotline at **1-800-269-0271**.

3 The "We Need to Verify Your Information" Scam

Someone calls, emails, or shows up at your door claiming they must **verify your SSN, bank account, or personal details** for a "benefit increase," "stimulus payment," or "COLA adjustment." They may claim to be from SSA, Medicare, or another agency.

THE TRUTH SSA already has your information and doesn't call to verify it. COLA increases are **automatic**. If anyone asks for your SSN, bank info, or card — by phone or at your door — it's a scam.

DR. ED'S TIP Never give your SSN to anyone who contacts **you**. If SSA truly needs to verify identity, they mail you a letter with specific instructions. In doubt? Call **1-800-772-1213**.

The Newer Digital Scams

These spread fast in 2025–2026. The FTC, FBI, and U.S. Postal Inspection Service have all issued public warnings.

4 The Empty Package + QR Code Scam ("Brushing 2.0")

A package you **never ordered** arrives — often a cheap item or just a note, with **no sender information**. The note says to **scan a QR code** to "find out who sent it," "register the gift," or "return it." Scanning takes you to a fake site that steals your card numbers and passwords — or downloads **malware** that hands hackers access to your phone.

THE TRUTH The FBI and FTC warn this is a twist on the "brushing" scam. **Never scan a QR code from an unexpected package.** The item is legally yours — keep it or toss it, but don't scan the code.

DR. ED'S TIP If you already scanned: change your passwords, watch your accounts, and pull free credit reports from Equifax, Experian & TransUnion. Report it at **ic3.gov**.

5 Facebook Scams — Cloned Friends, Hacked Accounts & Marketplace

Three common forms: **(a) Cloned profile** — a scammer copies a real friend's name and photo and sends you a **new** friend request, then asks for money or sends a bad link. **(b) Hacked account** — a friend's real account is taken over and messages you for cash or gift cards. **(c) Marketplace** — a fake buyer or seller asks you to **"send a verification code"** or pay a deposit. That code hands them control of your phone number or account.

THE TRUTH A real friend won't send a **second** friend request, and no legitimate buyer needs a code texted to **you**. Anyone asking for money, gift cards, or a one-time code is a scammer.

DR. ED'S TIP Verify by calling or texting the friend on a number you already have. **Never** share a verification code. Turn on two-factor login, and report the profile to Facebook and to **reportfraud.ftc.gov**.

6 The Fake Zoom (& Teams) Link Scam

You get a meeting invite by email or text — sometimes posing as **SSA, Medicare, or a doctor's office**. The link looks like Zoom but goes to a **lookalike site**. After a fake "meeting" with audio problems, an **"Update Available"** pop-up appears. Clicking it installs malware or remote-access software that can spy on you and drain accounts.

THE TRUTH Real Zoom **never** makes you download an update from a link in a message. Updates happen **inside** the Zoom app. A meeting link that asks you to install something is a trap.

DR. ED'S TIP Only get Zoom from **zoom.us** or your app store. Don't click links in surprise invites — confirm with the person first. If you ran a downloaded file, treat the device as compromised and have it checked.

How & Where to Report a Scam

SOCIAL SECURITY SCAMS
1-800-269-0271 · oig.ssa.gov

QR / PACKAGE / ONLINE FRAUD
FBI IC3 · ic3.gov

IF MONEY WAS SENT
Call your bank/card company right away — fast action can stop it.

FTC (ALL SCAMS & ID THEFT)
reportfraud.ftc.gov

ELDER FRAUD HOTLINE (60+)
1-833-372-8311

PROTECT YOUR CREDIT
Freeze it free at Equifax, Experian & TransUnion.

WHAT'S NEXT

1. **Share this guide** with a family member or neighbor who might be targeted — most victims never saw it coming.
2. **Don't feel embarrassed** if you've been hit. Scammers are professionals. Reporting fast protects you and others.
3. Run a free benefits check at **24help.org/screener** — free, safe, no scams.