Scams & Fraud Alerts

Cybercriminals often use **scams** to trick people into giving away money or personal information. These scams can come through phone calls, emails, text messages, or even snail mail. Older adults are frequently targeted with certain types of fraud. Here are some **common scams** to be aware of and **red flags** to help you spot them.

Common Scams Targeting Seniors:

- **Phishing Emails/Texts:** *Phishing* is when you receive an email or text that pretends to be from a legitimate source (like your bank, a government agency, or a company like Amazon) but is actually fraudulent. The message usually urges you to **click a link** or **provide information**. For example, an email might say "Your account is suspended! Click here to verify your identity." If you click the link, it may take you to a fake login page that steals your username and password, or it might install malware. **How to spot phishing:** Look for generic greetings and grammatical errors (e.g. "Dear Customer" instead of your name) and check the sender's email address carefully – often it's off by a letter or comes from a weird domain. Phishing messages also create a sense of urgency or fear ("Act now or your account will be closed!") – that's a big red flag. **Never** click suspicious links. If you think the issue might be real, open your web browser yourself and go to the company's official website (or call them at their official number) instead of clicking the link in the message.

- **Tech Support Scams:** This scam is rampant. You receive a phone call (or a popup on your computer) from someone claiming to be Microsoft, Apple, or another tech support, saying they "detected a virus" or "your computer is sending errors." They'll sound very professional and urgent. They might ask you to **grant them remote access** to your computer or to pay for a "security subscription." In reality, **there is nothing wrong with your computer** – the scammer just wants access to your PC and your credit card info. Remember: **Microsoft or Apple will never cold-call you about a virus** on your computer. If you get an unexpected tech support call, hang up. If a scary "your computer is infected, call us" message pops up, ignore it. *What if you did click or call?* – If you gave a stranger remote access, immediately *disconnect your computer from the internet* and have a trusted tech person or legitimate service check it out. If you gave out credit card info, call your card company and report a fraud. But ideally, don't let it get that far – be extremely skeptical of any unsolicited tech help. Legitimate tech companies don't initiate calls; you have to reach out to them first.

- **Lottery/Prize Scams:** "Congratulations, you've won a $5,000 Walmart gift card in our sweepstakes! Just pay a $100 processing fee to claim it." Any message or call that says you won a huge prize **out of nowhere** is almost certainly a scam, especially if they ask you to pay **any money upfront**. Real lotteries **never** make you pay to get your winnings. Scammers will often ask for that fee via untraceable methods like gift cards or wire transfers. If you send $100, they'll likely come back and say, "Now you also need to pay taxes, send another $500," and so on. **Rule of thumb:** If you're told you won a contest you don't remember entering, be very suspicious. Don't pay or give banking info to anyone claiming you won something. It's best to hang up or delete the message. You can always independently verify by contacting the supposed organization directly, but never use the phone number or email they gave you in the message – look up the official contact info.

- **"Grandchild in Trouble" / Family Imposter Scam:** This is a cruel one. You get a call: "Grandma, it's me! I need help – I'm in jail in Mexico and I need money for bail. Please don't tell Mom and Dad, they'll be so mad." The caller *sounds* distressed, you assume it's your grandson or someone similar. They urgently ask you to **wire money** or buy **gift cards** and give them the codes to get them out of trouble. In reality, it's a scammer impersonating your loved one. They often scrape personal info from social media to make the story convincing ("Remember my friend John? I went to visit him and this happened…"). They will beg you to keep it secret. **If you get a call like this, pause and verify.** Ask the caller something only your real grandchild would know ("What's the name of your dog?"), or set up a family 'safe word' that only they would know. Or hang up and call your grandchild (or their parent) on their known number to check. 99% of the time, you'll find your real grandson is safe at home and had no idea about this. This scam works because of emotion and urgency. Train yourself that in any **urgent money request**, you must double-check the story, no matter who they claim to be. It's better to offend someone by verifying than to lose money to a criminal.

These are just a few examples. Other scams include **IRS/government impersonation** (threatening you with arrest for taxes unless you pay immediately – note: the IRS always contacts by mail first and never demands payment by phone like that), **romance scams** (someone you meet online professes love then asks for money), **Medicare/health scams**, employment scams and more. The specific story may vary, but they all seek to either scare you or woo you into sending money or info.