SENIORS: STEER CLEAR OF FRAUD SCHEMES

Fraud schemes have become increasingly sophisticated, and fraudsters have seniors in their sights. Protect yourself, your personal information and your money. If something is too good to be true, it likely is.

HOW DO I PROTECT MYSELF?

Avoid phone scams:

- If something does not sound right, hang up the phone.
- If you do NOT recognize the caller ID on your phone or a call is marked "spam risk," do NOT answer the phone.
- Remember:
  - » The IRS does NOT call to demand immediate payment.
  - » The IRS does NOT threaten you with arrest.
  - » The IRS does NOT call about taxes owed before sending a bill by mail.
  - » The IRS does NOT require you to pay your taxes with prepaid debit cards, wire transfers, money orders, gift cards, cryptocurrency or credit/debit cards.

Be suspect of unexpected emails or texts:

- Don't open attachments or click links. These files may have malicious code that could infect your computer or compromise your personal information.
- Don't give out your personal or financial information, even if you think an email is from your bank or financial institution. Fraudsters make emails and texts look legitimate.
- Do not use contact information included in emails or texts to verify an organization's information. Use a separate source to locate contact information for the organization for follow up.
- If you receive a suspicious email or text that claims to be from the IRS, do NOT reply. Forward the email or send a screenshot of the text to phishing@irs.gov. Then, delete it.

GENERAL TIPS:

- Protect your personal information. Never carry your Social Security card with you, and do NOT provide your number to others.
- Don't transfer funds to an unverified recipient.
- Don't visit suspicious websites. Secure websites have "https://" in the web address.

IRS:CI
OFFICE OF COMMUNICATION

IRS-CI wants to keep you safe.
Help us help you from becoming the next fraud victim.

“Who’s in Your Wallet” Resources

Main Elder Abuse Website
sdcda.org/helping/elder-abuse

Stop Scams Toolkit:
sdcda.org/content/helping/dont-get-hooked.pdf

Ways to Protect Yourself

- Do not isolate yourself - stay involved.
- Always tell solicitors: "I never buy from or give to anyone who calls or visits me unannounced. Send me something in writing."
- Always have a second line of defense at your front door, like a locked screen door or a security chain guard.
- Change your online password quarterly.
- Shred all receipts that contain your credit card number.
- Sign up for the "Do Not Call" list at 1-888-382-1222 and the "Opt Out Mailing" list at 1-888-567-8688.
- Use direct deposit for benefit checks.
- Obtain a credit check on yourself at least two or three times each year.
- Screen your caller ID for "private" or "unknown" callers.
- Never give your credit card, banking, Social Security, Medicare, or other personal information over the phone unless you initiated the call.
- Be skeptical of all unsolicited offers.
- Use a credit card instead of a debit card. Credit cards offer more protection in terms of compensation for fraudulent purchases.
- Change your passwords online if a computer has been infected with a virus.
- If you are having difficulty keeping track of your finances, hire a reputable fiduciary or professional to handle various aspects of your affairs. A public guardian may be appointed conservator by the Probate Court when no other alternatives are available.

Don't be afraid to talk about it and take action. Waiting could only make it worse.

Courtesy: sdcda.org/helping/elder-abuse