What Are Social Security-Related Scams?

Criminals continue to impersonate SSA and other government agencies to obtain personal information or money. Our October webinars on cybersecurity (sponsored by Pension Fund and NBA Older Adult Ministries) were not recorded for security reasons, and some very helpful information was shared, such as these instructions:*

A scammer might call, email, text, write letters, or send messages on social media claiming to be from SSA or Office of the Inspector General (OIG). A scammer might use the name of a person who really works there and might send a picture or attachment as proof. Recognizing the signs of a scam gives you the power to ignore criminals and report the scam.

Four Signs of a Scam:

Scams come in many varieties, but they all work the same way:

1. Scammers **pretend** to be from an agency or organization you know to gain your trust.
2. Scammers say there is a **problem** or a prize.
3. Scammers **pressure** you to act immediately.
4. Scammers tell you to **pay** in a specific way.

Scammers are experts of manipulation and deception. Scammers will:

- **Pressure** you to make quick decisions.
- Ask you to **pay** with gift cards, precious metals (gold or silver), prepaid debit cards, wire transfers, cryptocurrency, or by mailing cash.
- Spoof official government phone numbers, or even numbers for local police departments.
- Say they are **transferring** your call to a law enforcement agent or government official who can help protect your money or help you avoid arrest.
- Use the **real names** of government employees.
- Threaten **arrest or legal action** unless you immediately pay.
- Threaten to **suspend** your Social Security number or account.
- Claim to need **personal information or payment** to activate a cost-of-living adjustment (COLA) or other benefit increase.
- **Threaten** to seize your bank account.
- Tell you to **move your money** to a protected bank account to keep it safe.
- Meet you in-person to **pick up cash, gold bars,** or other assets.
- **Demand** secrecy.
- **Email attachments** or **text** pictures of badges, credentials, or official-looking documents.
- **Direct message** you on social media, asking for personal information or money.
- Build a **relationship** (friendship or love) over time before eventually offering to help trade or invest money.

(Continued)

Fake Social Media Accounts:

Scammers create fake social media accounts using SSA images, colors, and jargon. This helps them appear as if they are associated with or endorsed by Social Security. The imposter accounts could look like an official SSA or OIG account or claim to be a government official. Social Security will never ask for sensitive or personal information through social media, email, or text message.

Here are some ways to spot a government imposter on social media:

- Number of followers is low.
- Incorrect punctuation or spelling.
- Links to websites that do not end in ".gov".
- Requiring payment for government forms or documents that are typically free. For example, charging a fee for a replacement Social Security number card.
- Incorrect social media handle.

Advice to Avoid Scams:

Protect yourself, friends, and family — If you receive a suspicious call, text, email, social media message, or letter from someone claiming to be from Social Security:

1. **Pause.** If you receive a communication that causes a strong emotional response or if you feel rushed, pause. Take a deep breath and talk to someone you trust.
2. **Hang up or ignore the message.** Do not click on links or attachments.
3. **Protect your money.** Scammers will insist that you pay with a gift card, gold bars or other precious metals, prepaid debit card, cryptocurrency, wire transfer, money transfer, or cash. Scammers use these forms of payment because they are hard to trace.
4. **Protect your personal information.** Be cautious of any contact claiming to be from a government agency or law enforcement telling you about a problem you don't recognize, even if the caller has some of your personal information.
5. **Spread the word** to protect your community from scammers.
6. **Report the scam** to the Office of the Inspector General at oig.ssa.gov/report.

*Read the entire article here:
https://www.ssa.gov/scam/?utm_source=sfmc&utm_medium=email&utm_campaign=Oct.+Cyber+Webinars+Attendee+Thank+You&utm_term=Social+Security%3a+Protect+Yourself+from+Scams&utm_id=5381793&sfmc_id=658954228

Links to More Resources

- FBI Elder Fraud Tools
- Internet Crime Complaint Center (IC3)
- Reporting Medicare Fraud & Abuse
- Social Security: Protect Yourself from Scams