Slam The Scam: Social Security Related Scams

The Social Security Administration named March 9th, 2023 “National Slam the Scam Day”. On National Slam the Scam Day, the SSA provides tips to recognize Social Security-related scams and stop scammers from stealing your money and personal information.

What Are Social Security-Related Scams?

Criminals continue to impersonate SSA and other government agencies in an attempt to obtain personal information or money. Scammers might call, email, text, write, or message you on social media claiming to be from the Social Security Administration or the Office of the Inspector General. They might use the name of a person who really works there and might send a picture or attachment as “proof.”

Four Basic Signs of a Scam

Recognizing the signs of a scam gives you the power to ignore criminals and report the 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.

Known Tactics Scammers Use

Scammers frequently change their approach with new tactics and messages to trick people. We encourage you to stay up to date on the latest news and advisories by following SSA OIG on LinkedIn, Twitter, and Facebook or subscribing to receive email alerts.

These are red flags; you can trust that Social Security will **never**

- **Threaten** you with arrest or legal action because you don’t agree to pay money immediately.
- **Suspend** your Social Security number.
- Claim to need **personal information or payment** to activate a cost-of-living adjustment (COLA) or other benefit increase.
- **Pressure** you to take immediate action, including sharing personal information.
- Ask you to **pay with** gift cards, prepaid debit cards, wire transfers, cryptocurrency, or by mailing cash.
- **Threaten** to seize your bank account.
- Offer to **move your money** to a “protected” bank account.

- **Demand** secrecy.
- **Direct message** you on social media.

Be skeptical and look for red flags. If you receive a suspicious call, text message, email, letter, or message on social media, the caller or sender may not be who they say they are. Scammers have also been known to:

- Use legitimate names of Office of Inspector General or Social Security Administration employees.
- “Spoof” official government phone numbers, or even numbers for local police departments.
- Send official-looking documents by U.S. mail or attachments through email, text, or social media message.

It is illegal to reproduce federal employee credentials and federal law enforcement badges. Federal law enforcement will never send photographs of credentials or badges to demand any kind of payment, and neither will federal government employees.

Report the scam.

How to Avoid a Scam

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. **Remain calm.** If you receive a communication that causes a strong emotional response, take a deep breath. 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, prepaid debit card, cryptocurrency, wire transfer, money transfer, or by mailing 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.

How to Report

When you report a scam, you are providing us with powerful data that we use to inform others, identify trends, refine strategies, and take legal action against the criminals behind these scam activities.

Report a scam

What to Do if You Were Scammed

Recovering from a scam can be a long and difficult process. Here are some reminders:

- Do not blame yourself. Criminal behavior is not your fault.
- Stop contact with the scammer. Do not talk to them or respond to their messages.
- Notify the three major credit bureaus: Equifax, Experian, and TransUnion to add a fraud alert to your credit report.

The Federal Trade Commission’s “What To Do if You Were Scammed” article has information about what to do if you paid someone you think is a scammer or gave a scammer your personal information or access to your computer or phone.

The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.