



FOR IMMEDIATE RELEASE October 20, 2022

## IG Warning: Offers to Increase Your Social Security Benefit Are from Criminals

Criminals Continue to Impersonate Government Agencies

DO NOT CLICK https://1gov-ssapp.com/system-ssa-logon

That unexpected offer from the Social Security Administration (SSA) to activate a benefit increase is from a criminal and not the real SSA. Do not share personal or financial information. Do not click on links or respond. Report suspected scams to oig.ssa.gov/report.

Criminals continue to impersonate SSA and other government agencies in an attempt to obtain personal information, money, or download malware onto phones.

Recent reports indicate that criminals are trying to trick people into sharing personal and financial information over the phone or through deceptive text and email messages that lure recipients to a fake Social Security website. Criminals falsely advise recipients to apply to receive Social Security benefits or extra money, such as a cost-of-living adjustment (COLA), or to set up an online account. The message may also provide fake contact information for SSA.

"Scammers are relentless in their attempts to lure you to their fake websites or to get you to respond in any manner to their fictitious offers. I urge members of the public to ignore unexpected messages and unsolicited offers. This simple step will help protect you from a scam," said Inspector General Gail S. Ennis. "Also, be alert for unusual business practices and contact Social Security directly with questions or concerns regarding SSA matters. Never click on the link."



"We are deeply concerned that fraudsters continue to find new ways to impersonate government agencies to deceive people into providing personal information or money," said Kilolo Kijakazi, Acting Commissioner of Social Security. "I strongly urge people to be vigilant,

and ignore suspicious emails, texts, or letters. If you receive a suspicious message, do not click on any links or attachments."

Ignore suspected scams and report them to <u>oig.ssa.gov</u>. Reporting these scams helps us identify emerging scam tactics and trends and protects others.

## **HOW A GOVERNMENT IMPOSTER SCAM WORKS**

Recognizing the signs of a scam can help you avoid falling victim to one. These scams primarily use telephone to contact you, but scammers may also use email, text message, social media, or U.S. mail. Scammers **pretend** to be from an agency or organization you know to gain your trust. Scammers say there is a **problem or a prize**. Scammers **pressure** you to act immediately. Scammers tell you to **pay** in a specific way.

## TIPS TO PROTECT YOURSELF

- 1. **Do not take immediate action.** If you receive a communication that causes a strong emotional response, take a deep breath. Hang up or ignore the message. Talk to someone you trust.
- 2. **Do not transfer your money! Do not buy that gift card!** Never pay someone who insists that you pay with a gift card, prepaid debit card, Internet currency or cryptocurrency, wire transfer, money transfer, or by mailing cash. Scammers use these forms of payment because they are hard to trace.
- 3. **Be skeptical.** Do not believe scammers who "transfer" your call to a government official or law enforcement officer, or who feed you a number as proof. Scammers can create fake numbers and identities. Do not trust your caller ID.
- 4. **Be cautious** of any contact claiming to be from a government agency or law enforcement, telling you about a problem you don't recognize or an unsolicited offer. Do not provide your personal information, even if the caller has some of your information.
- 5. Do not click on links or attachments. Block unwanted calls and text messages.

## FOR MORE INFORMATION ON SCAMS

Visit the ftc.gov/scam to read about common scams.

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.

###