

SCAM ALERT



Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

FOR IMMEDIATE RELEASE

February 19, 2026



SSA Office of the Inspector General Warns Public of Surge in Fraudulent “Social Security Statement” Emails



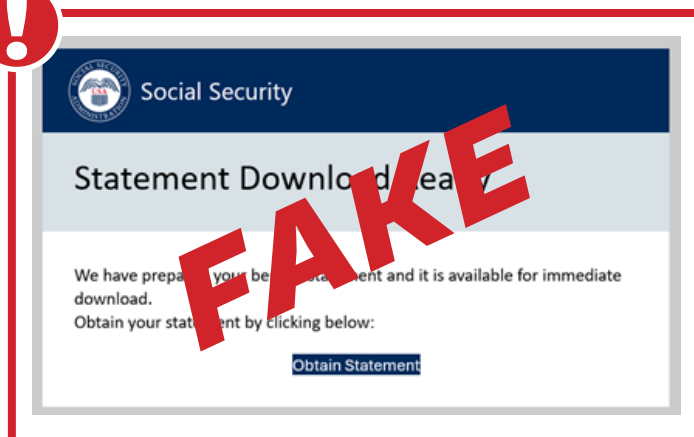
The Social Security Administration (SSA) Office of the Inspector General (OIG) is warning the public about a **significant increase in government imposter scam emails** that falsely claim to provide access to a recipient’s Social Security statement. Clicking links within the email may lead to identity theft, financial loss, or compromised data.

“We are seeing a sharp increase in fraudulent emails designed to look like official Social Security Administration communications,” said Michelle L. Anderson, Assistant Inspector General for Audit as First Assistant. “These messages are not from Social Security. Anyone who receives one should delete it immediately and report it.”

Official SSA communications originate from email addresses ending in “.gov.” These scam emails are designed to appear legitimate and often use official-looking language, logos, colors, and formatting to mislead recipients into clicking links or downloading attachments. Once clicked, the links may install malware or direct victims to fake websites intended to steal personal and financial information.

These emails are not from the Social Security Administration.

TYPE Don’t Tap! To access your *my Social Security* account, **type** in ssa.gov/myaccount.



Members of the press may make inquiries to Social Security OIG at oig.press@ssa.gov

Connect with us on social media:   

Common Warning Signs Include:

- Messages claiming your Social Security statement is ready to download
- Embedded links or attachments labeled as statements or documents
- Messages creating urgency or pressure to act immediately
- Sender addresses that do not end in “.gov”

What the Public Should Do:

- Do not click links or open attachments in unsolicited messages.
- Do not respond or provide personal information.
- To access or set up your Social Security account, go directly to ssa.gov/myaccount.
- Report suspicious emails immediately.

If You are a Victim:

Individuals who clicked a link, downloaded an attachment, or provided personal information should take immediate action:

- Stop all communication with the suspected scammer.
- Contact financial institutions to protect accounts.
- Report the incident to the SSA OIG at oig.ssa.gov/report.
- File a complaint with the FBI’s Internet Crime Complaint Center at ic3.gov.
- Report the scam to the Federal Trade Commission at ftc.gov.
- If financial loss occurs, contact local law enforcement.

Reminder:

The SSA and SSA OIG will **never**:

- Demand immediate payment.
- Send unsolicited attachments or direct download links.
- Threaten legal action, arrest, or benefit suspension because you don’t agree to pay immediately.
- Ask you to pay with gift cards, prepaid debit cards, wire transfers, cryptocurrency, cash, or gold bars.
- Offer to move your money to protect it.

SSA OIG urges the public to remain vigilant and share this information with friends, family, and community members, particularly older adults, who are frequently targeted by these scams.

For more information on Social Security–related scams or to report suspected fraud, visit ssa.gov/scam.



Members of the press may make inquiries to Social Security OIG at oig.press@ssa.gov

Connect with us on social media:   