

## No Gift Giving to Scammers This Holiday Season

### Chapter 1 How to Spot a Government Imposter Scam

Scammers are pretending to be government employees. They may threaten you and may demand immediate payment to avoid arrest or other legal action. These criminals continue to evolve and find new ways to steal your money and personal information. Do not fall for it! We want you to know how you and your loved ones can avoid becoming victims!

#### Watch our public service announcement here

## Chapter 2 Be Alert

If you owe money to Social Security, we'll mail you a letter with payment options and appeal rights. We only accept payments electronically through Pay.gov, Online Bill Pay, or physically by check or money order through our offices. We will never:

- Threaten you with arrest or legal action because you don't agree to pay us money immediately.
- Suspend your Social Security number.
- Promise a benefit increase in exchange for money.
- Ask you to send us gift cards, prepaid debit cards, wire transfers, Internet currency, cryptocurrency, or cash through the U.S. mail.

We only send emails or text messages if you have opted in to receive them and only in limited situations, including the following:

- When you have subscribed with Social Security to receive updates and notifications by text or email.
- As part of Social Security's enhanced security when accessing your personal my Social Security account.

We may email or text you about programs and services but will never ask for a return call to an unknown

#### Chapter 3 Know What to Look for

- The caller or sender says there is a **problem** your Social Security number or account.
- Any call, text, or email asking you to pay a fine or debt with retail gift cards, wire transfers, pre-paid debit cards, internet currency, or by mailing cash.
- Scammers **pretend** they are from Social Security or another government agency. Caller ID, texts, or documents sent by email may look official, but **they are not**.
- Callers threaten you with arrest or other legal action.
- Internet scammers may use "phishing" schemes to trick a recipient into revealing personal information by clicking on malicious links or attachments.

### **Chapter 4** Be Proactive

Protect yourself, friends, and family!

- If you receive a questionable call, hang up and report it at <u>oig.ssa.gov</u>.
- Do not return unknown calls, emails, or texts.
- Ask someone you trust for advice before making any large purchase or financial decision.
- Do not be embarrassed to report if you shared personal information or suffered a financial loss.
- Learn more at <u>oig.ssa.gov/scam</u>.
- Share this information with others.



# No Gift Giving to Scammers This Holiday Season

### **Chapter 5** If you receive a suspicious call, text, or email:

- 1. Hang up.
- 2. Do not return unknown calls, texts, or emails.
- 3. Do not give money or personal information.
- 4. Report the scam to the Office of the Inspector General (OIG) using the instructions below.

If you receive a call, text, or email that you believe to be suspicious, about a problem with your Social Security number or account, do not respond or engage with the caller or sender. Report Social Security phone, email, and text scams through our dedicated <u>online form.</u>

#### **Chapter 6** How to report a suspicious call, text, or email:

When reporting these suspicious communications, please be sure to capture as much information as you can. This includes:

- 1. Taking a screenshot or photo of the website, social media post, email, or text message(s).
- 2. For emails and text messages, please try to capture the entire message and any included message links. Also, let us know how you received or came across the suspicious message.
- 3. For U.S. postal mailings, if you can, scan or take cell phone pictures of the complete mailing, including the front and back of the outside envelope. Please hold onto the actual mailing for at least 30-days after reporting. We may decide to retrieve the hard copy of the mailed item.

This information will help ensure that we can locate the suspicious communication.

#### **REPORT A SCAM**