

The logo consists of a blue rectangular border containing two white rectangular boxes. The left box contains the word "SCAM" in blue, bold, sans-serif capital letters. The right box contains the words "NOT ME" in white, bold, sans-serif capital letters.

Government Scam Prevention Guide

Protect Yourself from Government Impersonation Scams

Introduction

Government impersonation scams are among the most common frauds targeting Americans today. These scams work because they exploit our natural tendency to respond to authority figures and create fear about legal consequences. This guide will help you identify genuine government communications versus scam attempts.

IRS (Internal Revenue Service) Scams

The IRS Will NEVER:

- Call to demand immediate payment using specific payment methods (gift cards, wire transfers)
- Threaten to bring in law enforcement to have you arrested for not paying
- Demand payment without giving you the opportunity to question or appeal
- Ask for credit or debit card numbers over the phone
- Call you about an unexpected tax refund

The IRS Typically WILL:

- Send multiple notices by mail before calling
- Provide a legitimate notice number that can be verified
- Offer payment plans and options if you owe taxes
- Allow you to question or appeal the amount owed
- Direct you to make payments to the "United States Treasury"

To verify an IRS notice: Call the IRS directly at 1-800-829-1040

Social Security Administration (SSA) Scams

The SSA Will NEVER:

- Call to tell you your Social Security number has been suspended
- Threaten you with arrest or legal action if you don't immediately pay a fine or fee
- Require payment by retail gift card, cash, wire transfer, or cryptocurrency

- Demand secrecy about a problem with your Social Security number or benefits
- Send official letters containing personally identifiable information via email

The SSA Typically WILL:

- Send a letter via U.S. mail if there's an issue with your benefits
- Call only if you've requested a call or have ongoing business with them
- Provide clear information about any overpayments or issues
- Offer appeals processes for any decisions or determinations
- Direct payments to "U.S. Treasury" through their secure website or by mail

To verify SSA communication: Call the SSA directly at 1-800-772-1213

Medicare Scams

Medicare Will NEVER:

- Call you uninvited to sell you anything or ask for your Medicare number
- Call claiming to be conducting a "Medicare survey" asking for your Medicare number
- Call to tell you that you need to pay to get a new Medicare card
- Ask for payment to "upgrade" your coverage
- Call offering "free" medical supplies or services in exchange for your Medicare number

Medicare Typically WILL:

- Send information by mail using official letterhead
- Only call if you've called them first or left a message requesting a callback
- Provide written information about any changes to your benefits
- Direct you to [medicare.gov](https://www.medicare.gov) for official information
- Offer clear appeal processes for any coverage decisions

To verify Medicare communication: Call 1-800-MEDICARE (1-800-633-4227)

FBI/Law Enforcement Scams

The FBI or Law Enforcement Will NEVER:

- Call to inform you about arrest warrants
- Email or call threatening arrest unless you pay fines
- Request wire transfers, gift cards, or cryptocurrency payments
- Demand payment to resolve criminal charges
- Request remote access to your computer to "investigate" an issue

Law Enforcement Typically WILL:

- Visit in person with proper identification if you're under investigation
- Allow legal representation during any questioning

- Present official documentation for any legal actions
- Direct court-ordered fines to be paid to courts, not individuals
- Follow formal legal procedures for any charges or arrests

To verify FBI communication: Contact your local FBI field office directly (found at [fbi.gov](https://www.fbi.gov))

Immigration Services (USCIS) Scams

USCIS Will NEVER:

- Call to demand immediate payment to avoid deportation
- Request payment via gift cards, wire transfers, or cryptocurrency
- Threaten immigrants with deportation if they don't pay fees over the phone
- Ask for personal financial information over the phone
- Request payments to be sent to individuals rather than to "U.S. Department of Homeland Security"

USCIS Typically WILL:

- Send official correspondence through U.S. mail on official letterhead
- Provide written notifications about application status or issues
- Offer receipts for all payments
- Include case numbers on all correspondence
- Direct payments through official channels with proper documentation

To verify USCIS communication: Call USCIS at 1-800-375-5283

Red Flag Warning Signs of Government Scams

1. **Unsolicited Contact:** Government agencies rarely contact you without prior correspondence.
2. **Pressure Tactics:** Legitimate agencies don't use high-pressure tactics or demand immediate payment.
3. **Threats:** Government agencies don't threaten immediate arrest or other legal action if you don't pay immediately.
4. **Unusual Payment Methods:** Government agencies never request payment via gift cards, wire transfers, or cryptocurrency.
5. **Personal Information Requests:** Be skeptical of unsolicited requests for Social Security numbers, account numbers, or other sensitive information.
6. **Caller ID Spoofing:** Scammers can make their calls appear to come from government phone numbers. Don't trust caller ID.
7. **Official-Looking Emails with Suspicious Links:** Government agencies typically don't send unsolicited emails with links to click.

8. **Grammatical Errors:** Official government communications rarely contain spelling and grammar mistakes.
-

How to Protect Yourself

Always Verify

- Never call numbers provided in suspicious messages
- Look up the agency's phone number independently (on their official website or on your billing statement)
- Call the official number to verify if the agency is trying to reach you

Never Share Personal Information

- Don't give out personal information to unsolicited callers or emailers
- Government agencies already have your information on file

Take Your Time

- Legitimate government agencies don't demand immediate action
- Take time to research and verify before responding

Report Scams

- Report government impersonation scams to the FTC at [ReportFraud.ftc.gov](https://www.ftc.gov/ReportFraud)
 - Report to the specific agency being impersonated
 - File a report with local law enforcement if you've lost money
-

Stay Informed

Government scams evolve constantly. Stay informed about the latest scam tactics by checking:

- ftc.gov/scams
 - usa.gov/scams-and-frauds
 - aarp.org/money/scams-fraud
 - consumer.ftc.gov
-

Remember: Real government agencies will never threaten you, demand immediate payment, or require unusual payment methods like gift cards, wire transfers, or cryptocurrency.

If you've been victimized by a scam, it's not your fault. These scammers are professionals who use sophisticated tactics. Report the scam to help protect others.

