
# CONSUMER ALERT: Spotting and Avoiding Imposter Scams

**BALTIMORE, MD (May 31, 2024)** – Attorney General Anthony G. Brown is warning consumers about the growing threat of imposter scams, with scammers using sophisticated technologies to deceive the people they target. These scammers impersonate trusted figures, such as government officials, official representatives from banks, law enforcement, tech support agents, or even family members or friends, to steal your money or personal information.

A note about artificial intelligence (AI): Voices generated by AI are often used in scams. These are fake voices created by computers to sound like real people. Scammers use this technology, mimicking voices and even speech patterns, to trick people into believing they are talking to someone they know or trust. This makes it very difficult to tell the difference between a legitimate call and a scam.

The bottom-line is no matter what kind of technology or trickery these fraudsters use, you can learn how to effectively spot and avoid all kinds of imposter scams. The Attorney General's Office is here to help you do this.

**Common Imposter Scam Types**

- Government Imposters: For example, the caller may claim to be from the IRS, Social Security Administration, or Medicare, and threaten you with fines or arrest.
- Family or Friend Imposters: A scammer may pretend to be a relative or friend in distress who needs money urgently.
- Tech Support Scams: Fake tech support agents will claim your computer has a virus and demand access or payment for unnecessary repairs.

**Recognize Imposter Scam Red Flags**

- Unsolicited Calls or Emails: Be cautious of unexpected contact from individuals claiming to be from reputable organizations. Scammers often pretend to be from the IRS, Medicare, or Social Security.
- Urgency and Fear Tactics: Scammers often create a sense of urgency, claiming that immediate action is required to avoid severe consequences, such as legal action, arrest, fines, or account suspensions. They may tell you that they are offering a limited-time deal to push you into making hasty decisions. Or they may claim there is a health emergency, and you must act immediately to protect a loved one.
- Requests for Personal Information: Be cautious if the caller asks for sensitive information, such as Social Security numbers, banking details, or remote access to your computer.
- Payment Requests: Requests for payment using gift cards, wire transfers, or cryptocurrency are major red flags.

**How to Verify Someone's Identity**

- Contact the Organization: If you receive a suspicious call, hang up, and then contact the organization or agency directly using official contact information found on their website or through trusted directories.
- Ask Questions: Always verify the caller's identity by asking questions only the real person would know. Scammers often struggle to answer detailed questions or provide verifiable information. Hang up and call back using a known, trusted number for the individual claiming to be on the phone.
- Use a Code Word: Establish a code word with friends and family members that only they would know and use in case of an emergency.

**Protect Yourself**

- Hang Up: If you suspect a scam, hang up immediately. You do not need to be polite to scammers.
- Never Share Personal Data: Never share personal information, such as Social Security numbers or bank details, over the phone or through email unless you are certain of the recipient's identity.
- Stay Calm and Don't Panic: Scammers rely on fear. Take your time to think and verify before acting on any request.
- Talk to Someone You Trust: Before taking any action based on an urgent call, consult with a trusted family member or friend to gain their perspective.

**Report Suspected Scams**

You can report suspected imposter scam calls or emails to:

- The Attorney General's Consumer Protected Division at www.marylandattorneygeneral.gov (file a general complaint)
- The Federal Trade Commission (FTC) at www.ftc.gov/complaint
- AARP Fraud Watch Network at www.aarp.org/fraudwatchnetwork

- The FBI at www.IC3.gov.

If a scammer does steal money from you, contact your local police department to report the theft. If the scam involved transferring funds, immediately contact the financial institution from which you transferred funds and ask that the transfer be reversed.

**Identity Theft**

If you suspect that an imposter scammer has obtained your personal information and could steal your identity, our Consumer Protection Division has tools available to help you address it. Visit www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx for helpful tips and steps you can take to protect yourself or recover from identity theft, or call our Identity Theft Program at 410-576-6491 or send an email to idtheft@oag.state.md.us.

This alert was issued to all consumers who have subscribed to receive consumer information from our office. Consumers can subscribe to this list here: https://public.govdelivery.com/accounts/MDAG/subscriber/new.

###

https://www.marylandattorneygeneral.gov/press/2024/053124CA.pdf