State of Connecticut
Attorney General George Jepsen

Quick Tips

The IRS Imposter Scam

How the scam works:

The phone rings, and your caller ID says the call is from the Internal Revenue Service. A prerecorded voice tells you that you that you owe tax money and will be arrested, prosecuted or face other legal action if you do not immediately send funds, usually using a pre-paid debit card or wire transfer. The call is threatening and convincing — but it's very likely part of a pervasive, nationwide scam.

Each year, thousands of taxpayers receive suspicious phone calls, emails, faxes or notices claiming to be from the IRS. Often, these scams will fraudulently use the IRS name or logo when communicating in order to appear more authentic to victims. The overall objective of the scammers is to trick consumers into revealing personal and financial information, such as Social Security numbers, bank account or credit card numbers, which is then used to commit identity theft or steal a consumer's money, or to get a consumer to send money directly to the scammer.

Identify the scam:

- The truth is the IRS usually first contacts people by mail – not by phone – about unpaid taxes. And the IRS won't ask for payment using a pre-paid debit card or wire transfer. The IRS also won't ask for a credit card number over the phone.
- The IRS will never ask for detailed personal and financial information like PIN numbers, passwords or similar secret access information for credit card, bank or other financial accounts. The IRS does not initiate taxpayer communications through e-mail and will not send a message about a consumer's tax accounts.
- The address of the official IRS Web site is www.irs.gov. Do not be confused or misled by sites claiming to be the IRS that end in .com, .net, .org or other designations instead of .gov.
- Scammers use fake names and IRS badge numbers. Scammers also generally use common names and surnames, like "Steven Martin," to identify themselves and may be able to recite the last four digits of a victim's Social Security number.
- Scammers spoof the IRS toll-free number on caller ID to make it appear that it's the IRS calling and can send bogus IRS emails to some victims to support their bogus calls.
- After threatening victims with jail time or driver's license revocation, scammers hang up and others soon call back pretending to be from the local police or DMV and the caller ID supports their claim.

How to avoid the scam and what to do if you have been scammed:

- If you receive an e-mail from someone claiming to be the IRS or directing them to an IRS site, you should never reply to the message, open any attachments or click any links. Attachments and links may contain a malicious code or a virus that will infect your computer. If someone calls you on the phone claiming to be from the IRS, hang up. If you owe Federal taxes, or think you might owe taxes, call the IRS at 1-800-829-1040. IRS workers can help you with your payment questions.
- If you have fallen victim to an IRS scam, file a complaint with the Internet Crime Complaint Center (IC3), which is a partnership between the Federal Bureau of Investigation, the National White Collar Crime Center, and the Bureau of Justice Assistance. Information on filing a complaint with the IC3 can be found at www.ic3.gov. You should also report the scam to the Treasury Inspector General for Tax Administration at www.treasury.gov/tigta.
- You can also report the scam to the Federal Trade Commission (FTC) by calling 1.877.FTC.HELP (1.877.382.4357) or by visiting the FTC's Web site at www.ftc.gov.
- If you have questions or need additional information, call the Office of the Attorney General Consumer Assistance Unit at 860-808-5420 or email attorney.general@ct.gov.

Last Updated: October 24, 2014