# CLIENT MEMO: Don’t get hooked by a tax scam

The IRS has made preventing identity theft and tax refund fraud a top priority. An important part of the agency’s fraud prevention program is its campaign to inform taxpayers about the many varieties of tax fraud and how they can keep from becoming victims.

## ■ Typical telephone fraud scenario

Picture this: You’re relaxing at home when your phone rings. You don’t recognize the number on the caller identification, but it’s from your area code, so you answer.

“I’m with the IRS,” the caller says. “You owe back taxes. A warrant will be issued if you do not pay, and your local police will arrest you.”

The caller knows your name and may even know the last four digits of your social security number. He tells you how much you owe, and adds that this is a serious matter. “You must submit a payment voucher within the next hour to avoid arrest. We suggest you buy a prepaid debit card immediately.”

The caller gives you a phone number to call once you have acquired a prepaid card so you can settle your debt and the arrest warrant can be canceled.

Can you identify four indicators in the above scenario that tell you this call is the latest addition to the “Dirty Dozen” list of tax scams compiled by the IRS?

***Here are the tip-offs:***

- ***An unexpected phone call.*** The IRS makes initial contact regarding tax issues in a written letter, sent to you via U.S. postal mail.
- ***The threat of arrest.*** Warnings of arrest or other police action are designed to frighten you into agreeing to send money or disclose personal financial information such as your social security number. Local police departments will not threaten to arrest you for federal tax-related issues.
- ***Request for immediate payment.*** If you actually owe money for any type of federal tax, payment options are available. You’ll receive notices in the mail detailing the amount due and you’ll have time to respond.
- ***Payment via prepaid debit card.*** The IRS does not require you to purchase prepaid cards to pay any tax you may owe, and will not call to ask for personal identification numbers.

The “red flags” seem obvious as you read this. However, tax-related fraud plays on your natural inclination to avoid trouble with official agencies, and the actual phone call will come from a practiced con artist armed with a script and the element of surprise. Under those circumstances, your skepticism might take a back seat to understandable confusion and fear.

***How can you protect yourself?***

- ***Advance warning gives you an advantage.*** Being aware of tax fraud schemes makes it likely you’ll recognize common techniques used by fraudsters, such as threats, multiple calls, and repeated demands for an immediate decision.

- ***Be assertive.*** You have no obligation to answer your phone, engage in conversation, or provide information to anyone who calls you. Let contacts from unknown numbers go to voicemail. If you do answer and the caller's requests make you uncomfortable, disconnecting immediately is neither rude nor impolite.
- ***If you choose to contact the IRS directly*** concerning the call, do not use the phone number the caller gave you. Why? In this latest scam, the number provided will connect you with another con artist in the same organization.

## ■ Phony IRS e-mails and websites

The crooks create IRS e-mails and websites that appear to be legitimate. They are designed to look like genuine IRS communications, but they are schemes designed to steal your identity. One of the newest scams is tax refund fraud where your personal data is stolen and used to file a tax return in your name in order to claim a refund. When you then file your return, the IRS rejects it and notifies you that you have already filed.

Another example of these bogus e-mails: You receive a message confirming IRS receipt of your tax return, but the IRS needs more information to process your return. The e-mail looks official and completely legitimate. But it isn't.

***Here's what the IRS wants you to know about bogus e-mails:***

- ***The IRS does not initiate*** contact with taxpayers by e-mail or social media to request financial information.
- ***The IRS never asks*** taxpayers for detailed personal financial information.
- ***The address of the official IRS*** website is *www.irs.gov*; don't be misled by sites claiming to be the IRS but ending in *.com*, *.net*, *.org*, or anything else.
- ***If you receive an e-mail*** claiming to be from the IRS or directing you to an IRS site, do not reply to the message, open any attachments, or click on any links.
- ***To help the IRS fight*** identity theft and refund fraud, report any bogus correspondence and forward any suspicious e-mail to *phishing@irs.gov*.

## ■ The IRS strategy

The IRS has developed a comprehensive identity theft strategy that is focused on preventing, detecting, and resolving identity theft cases as soon as possible. Though these scams proliferate during tax filing season, they continue throughout the year as the thieves continue to create new ways to steal identities for financial gain.

The IRS has made numerous announcements in the past to help protect taxpayers from these scams. It repeats the message that it never uses an e-mail, text message, social media, or a phone call to initiate a contact about your tax information. So if you receive what looks like an official IRS e-mail, you should forward it to *phishing@irs.gov*. Do not reply to the sender, and do not open any attachments. And if you get a scam phone call, hang up.

Please let us know any time you're contacted about your tax information. We're here to keep you safe and informed.