

Your Monthly Money

brought to you by



Watch Out for These 6 IRS Tax Scams

Tax season is stressful enough without adding vulnerability to identity theft to your list of things to worry about. To keep your sensitive personal information safe, however, you should be a little worried, though – or at least alert and informed enough to know a tax scam when you see one.

Tax scammers have several common tricks they use to lure taxpayers into handing over personal information that can be used for identity theft. Knowing what to look for is key to avoiding tax scams this tax season.

1. House calls by “IRS officials”

Most of the IRS’s notices arrive in the mail. So, if you hear a knock on your front door and open it to someone claiming to be an “IRS official,” don’t be fooled. Showing up on your doorstep isn’t the way the IRS contacts taxpayers.

Exceptions to this contact rule include special circumstances where the IRS may come to your home or business, such as discussing an overdue tax bill or obtaining a delinquent tax return. However, the IRS will first send “several notices” in the mail before showing up. The IRS also gives you the opportunity to appeal or ask questions about the amount it says you owe.

2. Calls demanding specific types of payment

The IRS won’t call to demand immediate payment through a specific method such as a prepaid debit card, gift card or wire transfer. If you get such a request, hang up and block the caller. “Generally, the IRS will first mail a bill to any taxpayer who owes taxes,” says the IRS.

3. Social Security number scams

Don’t be intimidated into responding to a robocall message threatening to cancel your Social Security number unless you make immediate payment on what the caller claims is an unpaid tax bill. Never give out sensitive personal information over the phone unless you know the caller is legitimate – if you called the IRS and are speaking with an actual IRS agent, for example.

Report the call to the [Treasury Inspector General for Tax Administration](#). Also report the caller ID and callback number to the IRS at phishing@irs.gov, typing “IRS phone scam” in the subject line. While you’re at it, report the call to the [Federal Trade Commission](#), adding “IRS phone scam” in the notes.

4. Fake taxpayer advocates

Callers who fraudulently claim to represent the IRS can use “spoofing” software to bring up the phone number of the IRS Taxpayer Advocate Service, according to the IRS. Sometimes, the calls are robocalls asking you to call back. If you return the call, however, you could be in trouble.

That’s because the scammer will likely ask for your personal information such as your Social Security number or taxpayer identification number for purposes of identity theft.

5. “Tax transcript” emails

Scammers may send “tax transcript” emails to bait taxpayers into opening an attachment that contains malware posing as a bank or other financial institution, warns the IRS. The IRS doesn’t send unsolicited emails to the public and would never send a sensitive document like a tax transcript via email. Don’t open the attachment. Instead, delete the email immediately.

“The scam is especially problematic for businesses whose employees might open the malware because this malware can spread throughout the network and potentially take months to successfully remove,” says the IRS.

6. Phony tax agencies

Tax scammers may send a letter threatening you with an IRS lien or levy. However, the lien or levy is based on “bogus delinquent taxes owed to a nonexistent agency: “The Bureau of Tax Enforcement,” according to the IRS.

“There is no such agency,” says the IRS. “The lien notification scam also likely references the IRS to confuse potential victims into thinking the letter is from a legitimate organization.”