



Tax Scams Getting More Sophisticated: How to Recognize Them

Have you been a victim of a tax scam? Make sure that you don't become one.

Tax scam messages are more sophisticated or realistic than last year, according to new research from McAfee. Nearly half (48%) of people surveyed have received a fake IRS message via text, email, social media, or phone, and 79% reported that the sender attempted to collect personal information, made demands, or issued threats. 23% of Americans say they or someone they know has lost money to a tax scam. And 35% of people say they or someone they know received a scam email or text about a "tax refund" or "tax refund e-statement" containing a malicious link.

Artificial intelligence (AI) is making it easier for scammers to create emails and texts that look so legitimate that you'd swear they came from the IRS. Taxpayers need to be hyper-vigilant these days about clicking links or opening attachments. We've always been warned about that, but it's more important than ever now. And fraudsters aren't just sending emails and texts. You may encounter potential danger on social media sites.

These scams aren't limited to tax filing season. They occur year round, according to the IRS. The agency recently released its annual "Dirty Dozen" list of tax scams for 2025. Here are some of the ways scammers may try to contact or interact with you.

2024		OMB No. 1545-0074	IRS Use Only—Do not write or staple in this space.
, 2024, ending _____, 20 _____		See separate instructions.	
		Your social security number	
		Spouse's social security number	
		Apt. no.	Presidential Election Campaign Check here if you, or your spouse if filing jointly, want \$3 to go to this fund. Checking a box below will not change your tax or refund. <input type="checkbox"/> You <input type="checkbox"/> Spouse
ow.	State	ZIP code	
Province/state/county		Foreign postal code	
<input type="checkbox"/> Head of household (HOH)			

Scammers may try to get personal information from you, like your social security number. Don't fall for it.

Phishing scams. Scammers sometimes pose as legitimate organizations in the tax and financial community, including the IRS, state tax agencies and tax software companies. Clicking the links they provide may introduce malware, or even ransomware. These unsolicited communications are of two main types:


- **Phishing**, emails sent by scammers claiming to come from the IRS or other organization. They might try to entice you by promising a phony tax refund or threaten you with false legal or criminal charges for tax fraud.
- **Smishing**, a text or smartphone SMS message that may, for example, say that your accounts has been put on hold, and which contain a bogus "Solutions" link to restore your account. It may also promise an unexpected tax refund.

Bad social media advice. You may encounter incorrect tax information on platforms like TikTok that can mislead you with wildly inaccurate advice, potentially leading to identity theft and tax problems. Only follow social media advice from trusted parties like the IRS, tax professionals, and other reputable sources.

Fake charities. When a crisis or natural disaster strikes, scammers descend on unsuspecting, generous individuals who want to help. They solicit money and personal information, which can be used to

further exploit victims through identity theft. If you're tempted, do your homework to make sure the organization is a qualified tax-exempt organization recognized by the IRS. You can search [here](#).

Describe the suspected tax scheme being promoted*

How did you become aware of the promotion or promoter 

e.g., seminar, internet, email, TV, flyer, newspaper, magazine, friend, relative, etc.

If you encounter a "ghost" tax preparer, as described below, complete the [Form 14242](#) on the IRS website.

"Ghost" tax return preparers. Be wary of shady tax professionals and watch for common warning signs, including charging a fee based on the size of the refund and being unwilling to sign the return. Never sign a blank or incomplete return. You can report such scam artists by completing the [Form 14242](#) Report Suspected Abusive Tax Promotions or Preparers.

False Fuel Tax Credit claims. A major concern during the past year involved taxpayers who were misled into believing they were eligible for the [Fuel Tax Credit](#). The credit is meant for off-highway business and farming use and is not available to most taxpayers. Scammers, though, are enticing taxpayers into inflating their refunds by erroneously claiming the credit.

What Can You Do?

Stay vigilant. McAfee offers these three guidelines:

Ignore unexpected communication from the IRS. Keep in mind that the IRS does not send unsolicited texts or emails, and it doesn't make phone calls out of the blue. The agency sends letters through the U.S. Mail.

Pause and think before you click. Scammers use urgency and fear to trick you. If a message demands quick action, skip the link and go directly to the [IRS](#) site or your tax provider's official website.

Use good cyber hygiene. Scammers are using AI to craft convincing fraud, but you can avoid being hacked. Keep your computer systems safe. Use two-factor authentication and a trusted password manager. Create unique passwords for every website, and don't share your login details with anyone else.

Consider Year-Round Tax Planning

We hope that by now you've completed and filed your 2024 income taxes. We'd be happy to take that task on for you in the future. And there's no better time to start your 2025 tax prep than after April 15, 2025. You'll find that year-round tax planning will make next year's preparation so much easier, less stressful, and more organized.

Year-round planning can also actually shave some dollars off of your tax obligation because you can take smart financial actions in 2025 that can get you a bigger refund (or not such a large tax bill). In the meantime, we hope you take the information we've provided here about tax scams to heart and avoid the pain that a skilled scammer can cause.

SOCIAL MEDIA POSTS

- The IRS does not send unsolicited email or texts, nor unexpected phone calls. Be on the lookout for scammers year-round.

- AI is making it easier for tax scammers to create convincing emails and texts from the IRS. Don't be fooled.
- Don't be fooled by scammers promoting income tax deductions for fake charities. Look them up [here](#).
- Were you dismayed by your income tax liability this year? We can help you with year-round tax planning.