



Watch Out for These Common Tax Scams

According to the Internal Revenue Service (IRS), tax scams tend to increase during tax season and/or times of crisis.¹ Now that tax season is in full swing, the IRS is reminding taxpayers to use caution and avoid becoming the victim of a fraudulent tax scheme. Here are some of the most common tax scams to watch out for.

Phishing and text message scams

Phishing and text message scams usually involve unsolicited emails or text messages that seem to come from legitimate IRS sites to convince you to provide personal or financial information. Once scam artists obtain this information, they use it to commit identity or financial theft. The IRS does not initiate contact with taxpayers by email, text message, or any social media platform to request personal or financial information. The IRS initiates most contacts through regular mail delivered by the United States Postal Service.

Phone scams

Phone scams typically involve a phone call from someone claiming that you owe money to the IRS or you're entitled to a large refund. The calls may show up as coming from the IRS on your Caller ID, be accompanied by fake emails that appear to be from the IRS, or involve follow-up calls from individuals saying they are from law enforcement. These scams often target more vulnerable populations, such as immigrants and senior citizens, and will use scare tactics such as threatening arrest, license revocation, or deportation.

Tax-related identity theft

Tax-related identity theft occurs when someone uses your Social Security number to claim a fraudulent tax refund. You may not even realize you've been the victim of identity theft until you file your tax return and discover that a return has already been filed using your Social Security number. Or the IRS may send you a letter indicating it has identified a suspicious return using your Social Security number. To help prevent tax-related identity theft, the IRS now offers the Identity Protection PIN Opt-In Program. The Identity Protection PIN is a six-digit code that is known only to you and the IRS, and it helps the IRS verify your identity when you file your tax return.

Tax preparer fraud

Scam artists will sometimes pose as legitimate tax preparers and try to take advantage of unsuspecting taxpayers by committing refund fraud or identity theft. Be wary of any tax preparer who won't sign your tax return (sometimes referred to as a "ghost preparer"), requires a cash-only payment, claims fake deductions/tax credits, directs refunds into his or her own account, or promises an unreasonably large or inflated refund. A legitimate tax preparer will generally ask for proof of your income and eligibility for credits and deductions, sign the return as the preparer, enter a valid preparer tax identification number, and provide you with a copy of your return. It's important to choose a tax preparer carefully because you are legally responsible for what's on your return, even if it's prepared by someone else.

False offer in compromise

An offer in compromise (OIC) is an agreement between a taxpayer and the IRS that can help the taxpayer settle tax debt for less than the full amount that is owed. Unfortunately, some companies charge excessive fees and falsely advertise that they can help taxpayers obtain larger OIC settlements with the IRS. Taxpayers can contact the IRS directly or use the IRS Offer in Compromise Pre-Qualifier tool at irs.treasury.gov/oic_pre_qualifier/ to see if they qualify for an OIC.

Unemployment insurance fraud

Typically, this scheme is perpetrated by scam artists who try to use your personal information to claim unemployment benefits. If you receive an unexpected prepaid card for unemployment benefits, see an unexpected deposit from your state in your bank account, or receive IRS Form 1099-G for unemployment compensation that you did not apply for, report it to your state unemployment insurance office as soon as possible.

Fake charities

Charity scammers pose as legitimate charitable organizations in order to solicit donations from unsuspecting donors. These scam artists often take advantage of ongoing tragedies and/or disasters, such as a devastating tornado or the COVID-19 pandemic. Be wary of charities with names that are similar to more familiar or nationally known organizations. Before donating to a charity, make sure it is legitimate and never donate cash, gift cards, or funds by wire transfer. The IRS website has a tool to assist you in checking out the status of a charitable organization at [irs.gov/charities-and-nonprofits](https://www.irs.gov/charities-and-nonprofits).

Protecting yourself from scams

Fortunately, there are some things you can do to help protect yourself from scams, including those that target taxpayers:

- Don't click on suspicious or unfamiliar links in emails, text messages, or instant messaging services — visit government websites directly for important information
- Don't answer a phone call if you don't recognize the phone number — instead, let it go to voicemail and check later to verify the caller
- Never download email attachments unless you can verify that the sender is legitimate
- Keep device and security software up-to-date, maintain strong passwords, and use multi-factor authentication
- Never share personal or financial information via email, text message, or over the phone

1) Internal Revenue Service, 2022

This material has been provided for general informational purposes only and does not constitute either tax or legal advice. Although we go to great lengths to make sure our information is accurate and useful, we recommend you consult a tax preparer, professional tax advisor, or lawyer.