

SWC

Tax planning and financial strategy.
Simplified.©

# IRS Dirty Dozen for 2026: 12 Tax Scams to Watch Out For

©2026 SWC (Stees. Walker & Company, LLP) | All rights reserved. | No portion of this singlet may be used without the express and written permission of SWC

**Start Here:** The IRS Dirty Dozen for 2026 identifies tax scams and schemes that can put your money, personal information, real property, or identity at risk. This year's list includes AI-enabled IRS impersonation, misleading tax advice on social media, identity theft involving IRS Online Accounts, and questionable tax strategies promoted as easy ways to generate refunds or reduce tax bills. Here, we explain each of the 12 schemes, the warning signs that should get your attention, and what you can do when a suspicious call, message, tax claim, post on social media, or financial offer comes your way.

Scammers and bad faith actors are always looking for ways to separate you from your hard earned money, personal information, real property, and identity. And when one scam stops working, they rarely pack up and find a new line of work.

That's one reason that the Internal Revenue Service (IRS) publishes its annual Dirty Dozen, a list of tax scams and schemes that taxpayers, businesses, nonprofits, and even tax professionals like the team here at SWC, should watch out for. The 2026 list covers familiar threats *and* reflects how fraud is changing, with AI-enabled scams and other increasingly sophisticated attempts to steal from you.

The IRS issued its initial Dirty Dozen alert in January of 2002 and now, as part of a partnership with state tax agencies and the tax industry, continues to warn business and individual tax filers about the ever-evolving nature of tax scams and schemes. Although such deceptions often receive more attention in the spring when we're fully engaged in tax filing season, we encourage our clients to remain cautious throughout the year.

In this singlette, we bring you up to speed on the 12 scams and schemes on the IRS Dirty Dozen list for 2026, explain the warning signs, and offer practical guidance for protecting yourself and your business. We'll start with the fraudsters who impersonate the IRS using Artificial Intelligence.

*Continued onto next page*

## 1. AI-Enabled IRS Impersonation by Phone

Artificial intelligence is giving an old scam some new tricks. Fraudsters can now use computer-generated tactics, voice mimicry, and spoofed caller ID to make a phone call sound and appear more convincing. A call may look as though it's coming from a legitimate source and may use urgency or threats to pressure you into responding.

The IRS points out several important warning signs:

- It generally contacts taxpayers by mail first.
- It doesn't leave urgent phone messages.
- It doesn't leave threatening prerecorded messages.
- It doesn't call to demand immediate payment or threaten taxpayers with arrest.

Caller ID isn't proof of identity, as today's technology can make a fraudulent call appear to come from a legitimate source.

▶ **What to do:** If you receive a suspicious IRS-related call, hang up rather than providing information or making a payment.

Related: We here at SWC — as well as officials at the IRS — caution taxpayers against relying on AI-generated responses for complicated tax questions. Any tax information or calculations produced by AI should be verified by a CPA.

## 2. IRS Impersonation by Email and Text

Phishing emails have been around for years, but scammers continue to find new ways to make them convincing. They may send an email, text, or direct message (DM) through a social media platform that appears to come from the IRS and use alarming language to convince you to act quickly.

Some messages contain links or QR codes that send you to fake IRS websites, where you're asked to "verify" an account and provide personal information. They may even say you can claim an unclaimed refund from a previous year. Others may contain attachments or links capable of installing malware, including ransomware, on your desktop computer, lap top, tablet, or phone.

▶ **What to do:** Don't click links or open attachments in unexpected messages claiming to be from the IRS. Treat unsolicited IRS-related emails, texts, and DMs with suspicion and report questionable communications to the IRS using the avenues provided at the end of this singlette.

**Remember:** A logo, official-looking website, or "IRS" or "Internal Revenue Service" name in a message doesn't prove the communication is legitimate.

*Continued onto next page*

## 3. Abusive Undistributed Long-Term Capital Gains Claims

New to the Dirty Dozen for 2026 is the abuse of IRS Form 2439, Notice to Shareholder of Undistributed Long-Term Capital Gains.

The form allows shareholders of certain investment funds or real estate trusts to claim a refundable credit for taxes paid on undistributed capital gains. The IRS says it has noticed an increase in schemes involving overstated or completely fabricated Form 2439 claims.

Some claims involve organizations that aren't legitimate investment funds or real estate trusts. Others falsely associate the claim with legitimate, well-known organizations.

Improper claims can result in refund delays, audits, penalties, or IRS enforcement action.

- **What to do:** Be skeptical if someone encourages you to claim a credit involving Form 2439 when your actual investments and tax documents don't support the claim.

## 4. Fake Charities

Natural disasters such as earthquakes, fires and floods, national tragedies, and other crises often inspire us to want to help. Unfortunately, they also provide opportunities for scammers.

Fraudsters may create fake charities and crowdsourced campaigns through established platforms like Go-Fund-Me that are designed to collect donations, personal information, or both.

This creates an additional tax concern. You may be able to deduct charitable donations on your federal income tax return if you itemize, but the donation must go to a qualified tax-exempt organization recognized by the IRS to count.

- **What to do:** Check out an organization before donating, particularly when the request arrives unexpectedly or follows a widely publicized tragedy or disaster. Use CharityNavigator.org, GuideStar.org, or the IRS' own Tax Exempt Organization Search tools to verify information about an organization's tax-exempt status and its own tax filings.

## 5. Misleading Tax Advice on Social Media

Social media platforms and YouTube can be great places to find recipes, home improvement tips, vacation destination ideas, political insights, and more. Tax advice? Not so much! You need to be careful.

The IRS continues to warn taxpayers about viral "tax hacks" promoted by social media influencers and hacks alike that encourage people to claim credits they don't qualify for or file returns containing false information.

Following advice from someone who isn't a CPA or tax planning professional who you know and

*Continued onto next page*

trust can lead to delayed refunds, audits, penalties, and potentially more serious consequences. Taxpayers who knowingly file fraudulent returns can face significant civil and criminal penalties.

- **What to do:** Get your tax information and tips from the IRS, a CPA, a qualified tax professional, and other reputable sources instead of assuming a random or popular social media post is accurate.

**Remember:** Going viral doesn't make tax advice legitimate. If a supposed loophole sounds too good to be true, find out whether it's legitimate before putting it on your tax return.

## 6. Identity Theft Involving Your IRS Online Account

Your IRS Online Account contains sensitive tax information, making access to it valuable to identity thieves.

Criminals may use stolen personal information to attempt to gain unauthorized access to your account. Another approach is to pose as someone offering to help you create your IRS Online Accounts, providing the criminal with an opportunity to collect sensitive information.

The IRS recommends creating your account directly through IRS.gov rather than relying on an unsolicited third party offering assistance.

- **What to do:** Create and manage your IRS Online Account yourself through the IRS website, and be wary of strangers offering to "help" you set it up.

## 7. Bogus "Self-Employment Tax Credit" Promotions

Who wouldn't want another tax credit? That appeal is exactly what makes promotions for a supposed broad "Self-Employment Tax Credit" potentially convincing.

According to the IRS, scammers use misleading claims about the credit to encourage taxpayers to file inaccurate returns and generate improper refunds. Many taxpayers don't qualify for the credits being promoted, and the IRS says it is closely reviewing claims filed under this provision.

- **What to do:** Don't determine your eligibility for a tax credit based on a social media promotion or what someone who isn't a CPA or tax planning professional tells us. Check trusted tax sources, and always consult with a qualified tax professional like a Certified Public Accountant.

## 8. Ghost Tax Preparers

Most tax professionals sign the returns they prepare. A "ghost preparer" doesn't.

A ghost preparer produces a tax return but refuses to sign it and/or refuses to include a Preparer Tax Identification Number (PTIN). According to the IRS, that's a major red flag.

*Continued onto next page*

Why should you care who signs the return? Because regardless of who prepared it, you're legally responsible for what gets filed on your behalf.

- **What to do:** Choose a reputable tax professional or CPA, and don't use a preparer who refuses to sign your return or provide a PTIN. Never sign a blank or incomplete tax return.

**Pro Tip:** Always review your personal and/or business tax return before it's filed. Hiring someone to prepare your taxes doesn't transfer responsibility for the information submitted to the IRS.

## 9. Non-Cash Charitable Contribution Schemes

Charitable giving can provide legitimate tax benefits, but fraudsters may try to turn those benefits into something they're not.

The IRS warns about schemes involving inflated appraisals of donated property, including arrangements involving syndicated conservation easements or art. Promoters may claim these strategies can eliminate or dramatically reduce your tax liability, when in reality they may not and could land you in hot water.

Filing a return with fabricated information can have consequences, and the IRS can hold refunds while it verifies questionable claims.

- **What to do:** Be cautious when someone promises unusually large tax benefits from a non-cash charitable contribution, particularly when those benefits depend on inflated valuations.

## 10. Overstated Withholding Schemes

Here's another scheme built around the promise of a bigger refund. Scammers encourage taxpayers to inflate withholding amounts while reporting little or no income on incorrect forms. The objective is to manufacture a refund that you aren't actually entitled to receive.

The IRS identifies several variations involving Forms W-2 and W-2G; Forms 1099-R, 1099-NEC, 1099-DIV, 1099-OID, and 1099-B; Schedule K-1 withholding; and other sources of withholding credits.

The problem for anyone attempting this is that the IRS can verify wages and withholding against information received from third parties. That can result in processing delays, penalties, or worse — enforcement action.

- **What to do:** Never inflate income tax withholding or allow someone to enter fabricated wage or withholding information on your return in an attempt to increase your refund.

*Continued onto next page*

## 11. Spear-Phishing and Malware Targeting Tax Professionals

Individual taxpayers aren't the only targets. Tax professionals and businesses hold large amounts of valuable information, making them attractive targets for criminals.

One approach involves "new client" or "document request" emails containing malicious links or attachments. Clicking one may give a criminal access to systems or sensitive client information they were never intended to have.

Warning signs include:

- Unexpected requests for sensitive information
- Unfamiliar or mismatched sender addresses
- Urgent payment demands
- Links to websites that don't clearly originate from irs.gov

Scammers may even gain access to a legitimate email account and find previous correspondence between a taxpayer and their tax planning professional. That gives the criminal material that can make a fraudulent message much more convincing.

▶ **What to do:** Slow down when an email unexpectedly requests documents, sensitive information, or payment. Check the sender and destination of links before responding, particularly when a message creates a sense of urgency. When in doubt, or if it appears to come from us or a service we use and you're questioning its legitimacy, call us at (858) 487-4580 or email us admin@swc.cpa. If it came from us, we'll let you know.

## 12. Aggressive or Misleading Offer in Compromise Marketing

You've probably heard advertisements promising to settle IRS debt for "pennies on the dollar" or some similarly dramatic amount. The IRS Offer in Compromise program (OIC) is real. For certain eligible taxpayers who are unable to pay their tax debt in full, it can provide a way to resolve that debt.

The problem is what the IRS calls "OIC mills." These businesses may aggressively market the program, overpromise results, and charge substantial fees to taxpayers who don't qualify. In fact, if you Google IRS Office In Compromise, the first three or four search results offer information from entities other than the IRS.

The IRS provides free tools taxpayers can use to determine whether they may qualify for an Offer in Compromise.

▶ **What to do:** Don't let a high-pressure sales pitch convince you that you qualify for a tax debt settlement. As you CPA or tax planning professional to determine your eligibility before paying a company substantial fees to pursue one.

*Continued onto next page*

## Protecting Yourself from Tax Scams

Although the Dirty Dozen covers 12 different threats, many scams depend on the same basic thing: getting you to act before you have time to think. Whatever form the pitch takes, slowing down gives you an opportunity to verify what you're being told.

Do not click unexpected links or open unexpected attachments. If you receive a suspicious IRS-related call, hang up. Suspicious IRS-related phishing emails and messages can be sent to phishing@irs.gov. If you believe your tax identity has been compromised, the IRS provides identity theft guidance and recovery steps through IRS.gov. The agency also provides an online system for confidentially reporting suspected tax fraud, scams, identity theft, abusive tax schemes, and other tax-related wrongdoing.

## How We Can Help

Taxes are complicated enough without fraudsters, scammers, questionable promoters, and social media personalities muddying the waters. A tax strategy that sounds appealing online may not apply to your situation. A credit may be legitimate but unavailable to you. And someone posing as a tax professional promising an enormous refund or dramatic reduction in tax debt may be telling you what you want to hear instead of what the tax law supports.

That's where working with a qualified tax planning professional who is a Certified Public Accountant can make a difference.

At SWC, we help our clients separate legitimate tax-saving opportunities from questionable claims, and make informed decisions based on their specific financial and tax situation. If you receive suspicious tax advice, or you simply want a second opinion before acting, contact us. It's much easier to address a questionable claim before it appears on a filed tax return.

---

**Disclaimer:** *The information in this SWC singlette about tax-related frauds and scams is provided for general informational purposes only and may not reflect current financial thinking or practices. No information contained in this singlette should be construed as financial advice from the staff at SWC (Stees, Walker & Company, LLP), nor is this the information contained in this singlette intended to be a substitute for financial counsel on any subject matter, or intended to take the place of hiring a Certified Public Accountant in your jurisdiction. No reader of this singlette should act or refrain from acting on the basis of any information included in, or accessible through, this singlette without seeking the appropriate financial planning advice on the particular facts and circumstances at issue from a licensed financial professional in the recipient's state, country or other appropriate licensing jurisdiction.*

**Tax planning and financial strategy.**
Simplified.©

**Keep in touch.**
16875 W. Bernardo Drive, Suite. 290
San Diego, CA 92127
**p:** (858) 487-4580 | **f:** (858) 487-8033
**w:** www.SWC.cpa

**Laura A. Stees, CPA**
Co-founder | Partner | Business Strategist
Laura@SWC.cpa

**Marni L. Walker, CPA**
Co-founder | Managing Partner | Estate Strategist
Marni@SWC.cpa