Dirty Dozen Tax Scams for 2026: IRS Reminds Taxpayers to Watch Out for Dangerous Threats

By Sandra R. Brown

Since 2002, typically during the annual tax filing season, the IRS has released its "Dirty Dozen"[i] list to warn taxpayers and tax practitioners alike of various tax scams as well as abusive transactions that the Service will be focused on in the coming year. The list has evolved over the past 20 years but often includes "repeat offenders" such as reminding taxpayers of identity theft scams and phishing scams directed at tax professionals, as well as individuals.

This year, the IRS released its Dirty Dozen list on March 5, 2026, which it tied, in connection with the Security Summit designed to protect taxpayers and the tax system against identity theft refund fraud, to "National Slam the Scam Day". Following that theme, the IRS reemphasized the need to remain vigilant and watch out for scams and fraud by criminals who are looking for new ways to take advantage of honest taxpayers trying to navigate their tax obligations in an ever changing and increasingly, complex tax system, while also highlighting several investment related abusive schemes and promotions, such as #6 abusive undistributed long-term capital gains claims and two charity scams at #3 fake charities and #9 non-cash charitable contribution schemes.

So, here's the full list of the 12 key scams to watch out for in 2026:

1. IRS Impersonation by Email and Text (Phishing + Mmishing). Scammers send emails, direct messages (DMs), and texts that appear to be from the IRS, often using alarming language and QR codes that direct taxpayers to **fake IRS websites** to "verify" accounts, enter personal information, or claim refunds. The IRS urges taxpayers not to click links or open attachments from unexpected messages and to report suspicious IRS-related emails, DMs, and texts. The IRS reported over 600 social media impersonators during fiscal year 2025.

As a reminder, never click any unsolicited communication claiming to be from the IRS, as it may install malware surreptitiously. These links may install malicious software, including ransomware, on a taxpayer's personal device, potentially preventing access to their files or personal information.

2. AI-Enabled IRS Impersonation by Phone (Robocalls, Voice Mimicry, Spoofed Caller ID). Phone scams continue to evolve, including calls that use computer-generated tactics and **spoofed caller ID** to appear legitimate. The IRS reminds taxpayers that it generally contacts taxpayers by **mail first** and does not leave urgent, threatening prerecorded

messages, call to demand immediate payment, or threaten arrest. Taxpayers should not rely on AI-generated responses to complex tax questions, and they should verify any calculations or information provided by artificial intelligence.

3. Fake Charities. Fraudsters often exploit tragedies and disasters by creating fake charities to collect donations and personal information. The IRS is committed to preventing fraudulent nonprofits from taking advantage of the American taxpayer.

Taxpayers who give money or goods to a charity may be able to claim a deduction on their federal tax return if they itemize deductions, but charitable donations only count if they go to a qualified tax-exempt organization recognized by the IRS.

4. Misleading Tax Advice On Social Media. Viral "tax hacks" can push taxpayers to file returns with false information or claim credits they don't qualify for, leading to refund delays, audits, penalties, or worse. The IRS continues to warn that social media-driven misinformation and disinformation remain a major driver of tax scams.

The IRS and the Coalition Against Scam and Scheme Threats warn taxpayers not to fall for these scams, and urge them to follow trusted advice from the IRS, tax professionals, and other reputable sources. The IRS reminds taxpayers who knowingly file fraudulent tax returns that they could potentially face significant civil and criminal penalties.

5. Identity Theft Involving IRS Online Account Access. Criminals may attempt to use stolen personal information to gain unauthorized access to a taxpayer's IRS online account or may pose as helpers to collect sensitive information during account setup. Taxpayers should create their account directly through IRS.gov and should not rely on unsolicited third parties offering assistance. The IRS provides official guidance to help taxpayers securely establish and protect their accounts.

6. Abusive Undistributed Long-Term Capital Gains Claims. The IRS identified an increase in the abuse of Form 2439. This form allows shareholders of certain investment funds or real estate trusts to claim a refundable credit for taxes paid on undistributed capital gains. Identified schemes involve overstated or fabricated Form 2439 claims, including claims tied to organizations that are not legitimate investment funds or real estate trusts. The IRS has also seen fake claims falsely linked to real, well-known organizations. Improper claims may result in refund delays, audits, penalties, or enforcement action.

7. Bogus "Self-Employment Tax Credit" Promotion. Scammers use misleading claims about a broad "self-employment tax credit" to encourage inaccurate filings and generate improper refunds. The IRS reminds taxpayers to rely on trusted sources and qualified tax professionals, not social media promotions, when determining eligibility for credits.

Many taxpayers do not qualify for these credits, and the IRS is closely reviewing claims coming in under this provision, so taxpayers filing claims do so at their own risk.

8. Ghost Preparers. A "ghost" preparer prepares a return but refuses to sign it and/or refuses to include a **Preparer Tax Identification Number (PTIN)**. When a preparer refuses to sign or provide a PTIN, that is a major red flag; the taxpayer is legally responsible for what is filed. The IRS urges taxpayers to avoid preparers who will not sign the return and to choose reputable help. Taxpayers should never sign a blank or incomplete return. Instead, the IRS reminds taxpayers to use a trusted tax professional for help.

9. Non-Cash Charitable Contribution Schemes. Some schemes involve inflated appraisals of donated property using syndicated conservation easements or art. Promoters often promise to eliminate or substantially reduce tax liability. The IRS warns taxpayers not to file returns with made-up information and reminds taxpayers that it can hold refunds while verifying claims.

10. Overstated Withholding Schemes (Fabricated Wage/Withholding Data). Scammers encourage taxpayers to inflate withholding amounts (sometimes described as "other withholding") to manufacture a larger refund by reporting zero or little income on incorrect forms. The IRS may delay processing while it verifies wages and withholding against third-party records. Inaccurate claims can lead to penalties and enforcement action.

There are multiple variations of the overstated withholding credit scheme, including those involving Forms W-2 and W-2G; Forms 1099-R, 1099-NEC, 1099-DIV, 1099-OID, and 1099-B, as well as the Alaska Permanent Fund Dividend, Schedule K-1 with Withholding Reported, and Unspecified Source of Withholding Credit Claimed.

11. Spear-Phishing And Malware Campaigns Targeting Tax Professionals. Tax professionals and businesses remain targets of "new client" or "document request" emails that deliver malicious links or attachments to steal client data or access systems. The IRS and the Security Summit urge preparers to remain vigilant and to strengthen their security practices.

Businesses and individuals, including tax pros, should always be cautious and look out for any suspicious requests or unusual behavior before sharing any sensitive information or responding to an email. Warning signs may include unexpected requests for sensitive information, mismatched or unfamiliar sender addresses, urgent payment demands, or links directing users to websites that do not clearly originate from IRS.gov. Be aware that by gaining access to a hacked email account, scammers can locate a genuine email from a previous victim's email account sent to their tax professional.

12. Aggressive or misleading Offer in Compromise Marketing ("OIC Mills"). The Offer in Compromise program can help certain eligible taxpayers resolve tax debt when they are unable to pay in full, but "OIC mills" often overpromise results and charge high fees to taxpayers who don't qualify. Taxpayers can check eligibility using free IRS tools to avoid high-pressure sales tactics.

The IRS is not only reminding taxpayers of the need to protect sensitive information and exercise caution in sharing data but also encouraging taxpayers to be wary of those who would promote improper returns. As the saying goes , if it's "too good to be true", it is likely to make the IRS's Dirty Dozen at some point.

Taxpayers who find themselves the focus of an IRS audit or investigation resulting from a tax scam or promotion that the IRS has identified as abusive, should consult with a qualified and independent tax controversy professional.

Sandra R. Brown *is a Principal of Hochman Salkin Toscher Perez P.C., where her practice focuses on criminal tax investigations, grand jury matters, litigation, and sentencing matters as well as representing and advising taxpayers involved in complex and sophisticated civil tax controversies, including sensitive-issue audits and administrative appeals and litigation. Ms. Brown's extensive experience and successes have included many notable cases including two U.S. Supreme Court decisions, numerous 9th Circuit rulings and numerous favorable administrative resolutions for taxpayers involved in IRS investigations and audits.*

Prior to joining the firm in 2018, Ms. Brown served as the Acting United States Attorney, First Assistant United States Attorney, and Chief of the Tax Division in the Office of the U.S. Attorney, Central District of California; where, with 27 years as a trial lawyer, she personally litigated over 2,000 tax cases on behalf of the United States.

Ms. Brown obtained her LL.M. in Taxation from the University of Denver, is a fellow of the American College of Tax Counsel, Vice-Chair of the ABA's Section of Taxation's Criminal and Civil Tax Penalties Committee, Co-Chair of the UCLA Tax Controversy Institute, Co-Chair of the ABA Criminal Tax Fraud and Tax Controversy Conference, an ABA Loretta Collins Argrett Fellowship Mentor, and is a frequent lecturer and author on tax controversy topics, including international compliance and criminal tax matters. Ms. Brown has been recognized as one of California's top 100 leading women lawyers, the recipient of USD School of Law's Richard Carpenter Excellence in Tax Award, Chambers High Net Worth in Tax and Tax Fraud, and an honoree of the inaugural Lawdragon 500 Leading Global Tax Lawyers. Additional information is available at http://www.taxlitigator.com

---

[i] IR-2026-30, March 5, 2026. https://www.irs.gov/newsroom/dirty-dozen-tax-scams-for-2026-irs-reminds-taxpayers-to-watch-out-for-dangerous-threats