Key Wealth

Key Wealth Institute

IRS Releases Its Dirty Dozen Tax Scams and Schemes for 2026

Paul Kieffer, CFP®, CPA, PFS, CLU, Senior Wealth Planner, Key Private Bank

The IRS has again compiled its annual list of common tax scams to remind taxpayers to use caution to protect themselves from potentially abusive arrangements ranging from preparer fraud to identity theft and bogus tax maneuvers. These schemes put people at financial risk (including taxes, penalties, and interest), not to mention the increased chances that they could become victims of identity theft. The reason the IRS puts this list together annually is to highlight the ever-changing methods that fraudsters use to trick taxpayers into identity theft and other scams.

Some of the topics are repeated from last year, there is one new scam, and others have been updated. The list is not a legal document or a formal listing of agency enforcement priorities; it is intended to alert taxpayers and the tax professional community about various scams and schemes at large. Taxpayers are encouraged to review the "Dirty Dozen" list and be alert to these scams throughout the year. Remember, always be vigilant and wary of anything that seems too good to be true.

1. Phish or smish: Avoid getting hooked by either

IRS impersonation by both methods is getting more common. Be alert to fake communications from those posing as legitimate organizations in the tax and financial community, including the IRS and states.

Phishing is an email sent by fraudsters claiming to come from the IRS or another legitimate organization, including state tax organizations or a financial firm. The email lures the victims into the scam by a variety of ruses, such as enticing victims with a phony tax refund or frightening them with false legal/criminal charges for tax fraud.

Smishing is a text or smartphone SMS message that uses the same technique as phishing. Scammers often use alarming language like, “Your account has now been put on hold,” or “Unusual Activity Report,” with a bogus “Solutions” link to restore the recipient’s account. Unexpected tax refunds are another potential target for scam artists.

Never click (or use a QR code) on any unsolicited communication claiming to be the IRS. This can also be a way for malicious hackers to load ransomware that keeps the legitimate user from accessing their system and files. The IRS initiates most contact through regular mail. The agency reported more than 600 social media impersonators during their 2025 fiscal year.

2. IRS impersonation by phone using AI

With the development of AI, robocalls, voice mimicry, and spoofed caller ID are becoming both more common and believable. The IRS continues to contact taxpayers primarily by mail first, and it does not leave threatening messages, demand immediate payment, or threaten arrest. Regarding AI, taxpayers should not rely on AI-generated answers to complex tax questions. Any such answers should be independently verified for correctness.

3. Fake charities

Beware of scammers using fake charities, especially following major disasters. Scammers often try to prey on well-intentioned donors by posing as fake charities, hoping to steal money but also personal and financial data that can be used in tax-related identity theft. Taxpayers should never feel pressured to give immediately. Legitimate charities are happy to get a donation at any time, so people should feel no rush. Donors are encouraged to take time to do their own research. Taxpayers should never make donations using a gift card or by wiring money. It is safest to pay by credit card or check.

4. Beware of inaccurate or misleading social media tax advice

Be careful of relying on what you read on social media, including anything tax related. The IRS warns taxpayers to be wary of trusting internet advice, which could be a fraudulent tactic promoted by scammers or a false tax-related scheme trending across popular social media platforms. The IRS is aware of various filing season hashtags and social media topics leading to inaccurate and potentially fraudulent information. The central theme involves people trying to use legitimate tax forms for the wrong reason. Taxpayers who knowingly file fraudulent tax returns could face civil and criminal penalties.

5. IRS online account help from third-party scammers

In this scam targeting individuals, swindlers pose as a helpful third party and offer to help create a taxpayer’s IRS online account at IRS.gov. Third parties making these offers will try to steal a taxpayer’s personal information that they sell to others to use to file fraudulent tax returns, obtain loans, or open credit card accounts. People should remember they can set these accounts up themselves and should not use third-party assistance, other than the approved IRS authentication process through IRS.gov, to create their own online IRS account.

6. Undistributed long-term gains claims

This scam is new to the list this year, as the IRS has seen a significant increase in the abuse of Form 2439, Notice to Shareholder of Undistributed Long-Term Capital Gains. This form allows shareholders of certain investment funds/real estate trusts to claim a refundable tax credit for taxes paid on undistributed capital gains. Typical scams include overstated or even fabricated claims, including claims related to organizations that are not even legitimate investment funds/real estate trusts. Additionally, bogus claims falsely linked to real, well-known organizations are also increasing. Improper claims may result in refund delays, audits, penalties, and/or enforcement action.

7. Bogus self-employment tax credit promotions

Fraudsters use misleading claims about this credit, which most taxpayers do not quality for, encouraging inaccurate filings that generate improper refunds. Since most taxpayers do not qualify, the IRS is closely reviewing tax returns that claim this credit. The IRS reminds taxpayers to rely on trusted sources and qualified tax professionals (not social media) when determining eligibility for tax credits.

8. Ghost preparers

Taxpayers should be on the lookout for unscrupulous tax preparers who could encourage people to file false tax returns and steal valuable personal information. One such type is a "ghost preparer," who encourages taxpayers to take advantage of tax credits and benefits for which they do not quality. These preparers can charge a large percentage of the refund (or even steal the entire refund). After the return is prepared, these "ghost preparers" simply disappear. Taxpayers should look for warning signs, including charging a fee based on the size of the refund, the preparer refusing to sign a tax return, or being asked to sign a blank or incomplete return. The IRS warns people to choose a tax professional carefully and never use one who refuses to sign the return or provide a preparer tax identification number.

9. Noncash charitable contribution schemes

These include inflated appraisals of donated property, including syndicated conservation easements or art. Promoters often promise big tax savings by inflating the value of donated property to reduce/eliminate a taxpayer's tax liability. Tax refunds can be held up by the IRS while they verify claims.

10. Overstated/fabricated wage withholding data ploy

Fraudsters encourage taxpayers to inflate withholding amounts to trigger larger refunds by reporting zero or minimal income. The IRS verifies withholding, so this can result in penalties and/or enforcement action. These ploys can come in several varieties involving W-2, W-2G, 1099R, 1099-NEC, and other forms.

11. Be cautious of ongoing spearfishing attacks to gain sensitive information, especially targeting tax professionals

Through spear phishing emails, cybercriminals impersonate real taxpayers seeking help with their taxes. They use fake emails to get sensitive data or gain access to a tax professional's client information from their computer systems. While these scams can peak around tax season, they remain a year-round threat. Criminals accessing tax-preparer credentials, or their client's tax-related information, can affect multiple victims. Of specific concern are "new client" scams in which identity thieves pose as potential clients using fake emails.

12. Watch out for Offer in Compromise mills

An Offer in Compromise (OIC) is a program in which a taxpayer works with the IRS to settle a tax debt for less than the full amount owed. These agreements are made directly between the taxpayer and the IRS without a third party. However, so-called Offer in Compromise "mills" often mislead taxpayers into believing that they can settle a tax debt for pennies on the dollar. They are promoted to people that don't even meet the qualifications for the Offer in Compromise program and frequently charge taxpayers excessive fees. Taxpayers can make the same deal with the IRS on their own, without paying an OIC mill. Taxpayers can check their OIC eligibility for free by using IRS's Offer in Compromise Pre-Qualifier tool.

IRS Releases Its Dirty Dozen Tax Scams and Schemes for 2026

The IRS places a high priority on preventing abusive transactions and schemes and is always on the lookout for promotors and participants of them. Where appropriate, the IRS will challenge them and impose penalties. As part of the Dirty Dozen awareness effort regarding tax schemes and unscrupulous tax return preparers, the IRS urges individuals to report those who promote abusive tax practices and tax preparers who intentionally file incorrect returns.

Protect yourself: Security reminders for taxpayers

Do what you can to protect yourself. Here are some basic security steps to protect yourself and your sensitive tax and personal information:

Use security software. Always use security software with firewall and anti-virus protection. Make sure the security software is always turned on and can automatically update. Encrypt sensitive files, such as tax records stored on the computer, and use strong passwords.

Watch out for scams. Learn to recognize and avoid phishing emails, threatening phone calls, and texts from thieves posing as legitimate organizations such as banks, credit card companies, and government organizations, including the IRS. Do not click on links or download attachments from unknown or suspicious emails.

Protect personal data. Don't routinely carry a Social Security card and make sure tax records are secure. Treat personal information like cash: Don't leave it lying around.

Work with financial institutions that have implemented processes to protect your private, banking, and financial information (such as multi-factor authentication, call-back verification for certain transactions, and email encryption programs to secure sensitive personal information). Multi-factor authentication allows users to better protect online accounts. One way this is accomplished is by requiring a security code sent to a mobile phone in addition to the username and password used to access the account.

Choose return preparers carefully. Avoid fly-by-night preparers. Ask if the preparer has an IRS Preparer Tax Identification Number (PTIN). Inquire whether the tax return preparer has a professional credential (enrolled agent, certified public accountant, or attorney).

Check preparer's qualifications. Use the IRS Directory of Federal Tax Return Preparers with Credentials and Select Qualifications available on the IRS website to search for a tax preparer listed with the IRS.

Be wary of charities with names that are similar to familiar or nationally known organizations. IRS.gov has a search feature called Exempt Organizations Select Check that allows people to find legitimate, qualified charities to which donations may be tax-deductible.

Don't give out personal financial information such as Social Security numbers or passwords to anyone who solicits a charitable contribution.

Use IP PINs. The IP PIN is a six-digit code known only to the taxpayer and to the IRS. It helps prevent identity thieves from filing fraudulent tax returns using a taxpayer's personally identifiable information. Using an IP PIN is, in essence, a way to lock a tax account. The IP PIN serves as the key to opening that account. Electronic returns that do not contain the correct IP PIN will be rejected, and paper returns will go through additional scrutiny for fraud.

Check privacy settings on social media. One way to circumvent these scams via social media is to review privacy settings and limit data that is publicly shared.

Practice good cyber hygiene. Practice proactive prevention to defend against ransomware attacks through effective cyber hygiene, cybersecurity controls, and other best practices.

For more information about preventing tax fraud, contact your advisor.

Key Wealth

The Key Wealth Institute is a team of highly experienced professionals representing various disciplines within wealth management who are dedicated to delivering timely insights and practical advice. From strategies designed to better manage your wealth, to guidance to help you better understand the world impacting your wealth, Key Wealth Institute provides proactive insights needed to navigate your financial journey.

About the Author

As a Senior Wealth Planner for Key Private Bank, Paul focuses on ensuring his clients' wealth management plans are carried through to meet their unique financial objectives and grow and preserve wealth.

Paul most recently served as a Regional Planning Strategist for Key Private Bank. Prior to joining Key, Paul was the director of Wealth Planning at Wilmington Trust and was responsible for the delivery of planning services and the planning platform, including scalable advice-oriented solutions, thought leadership, and direct planning where appropriate. Paul contributed thought leadership and solutions to the Corporate Executive Practice Group, including direct planning for corporate executives. Prior to joining M&T Bank, which acquired Wilmington Trust in 2011, Paul was a tax manager with a CPA firm.

He holds an MBA from SUNY Buffalo and completed their Graduate Tax program. Paul is a Certified Public Accountant and a Chartered Global Management Accountant and has the Certified Financial Planner®, Personal Financial Specialist™, Chartered Life Underwriter, Retirement Income Certified Professional®, Certified Advisor in Philanthropy, Chartered Advisor in Senior Living, Chartered Financial Consultant, and Certified Retirement Counselor designations. Paul instructed courses in the Certified Financial Planner Program as an adjunct faculty member of Canisius College in Buffalo New York. He is currently the treasurer and member of the board of directors for Musicalfare Theater in Amherst, New York. Previously, he served on the board of directors and as the treasurer of the Make-A-Wish Foundation of Western New York and BNSME. Paul is a member of the FPA, AICPA, and NYSSCPA.

260514-4469438