

IRS Dirty Dozen Tax Scams

TAX SCAM QUICK FACTS



In 2023,
1M+ tax returns were flagged
for potential identity fraud with \$6B in refunds requiring additional review.



The IRS used
236 filters
to identify possible fraud in 2023.

TOP 12 TAX SCAMS



1 Employee Retention Credit (ERC)

You may be blasted with aggressive ads saying you can get a massive refund via the ERC. These promotions are often exaggerated. You may not be eligible for the ERC, or you may be eligible for much less than the scammer says. Don't share personal info with these scammers in exchange for false promises.



2 Phishing & Smishing

You may get fake communications from fraudsters posing as legit organizations, including the IRS. These messages arrive in the form of an unsolicited text (smishing) or email (phishing). The IRS will reach out first through regular mail and will never initiate contact with you by email, text or social media.



3 Online IRS Account Help from Third Parties

Swindlers pose as a "helpful" third party and offer to help you create an IRS Online Account at IRS.gov in an attempt to steal your personal info. In reality, no help is needed. You can and should establish your own online account through IRS.gov.



4 Fake Charities

Bogus charities and fake organizations try to take advantage of generosity, especially during a crisis or natural disaster. They want your money and personal info, which can be used to steal your identity. Charitable donations only count if they go to a qualified tax-exempt organization recognized by the IRS. Check the organization's status before donating or sharing personal info.



5 Shady Tax Return Preparers

Be careful of shady tax professionals and watch for common red flags, including charging a fee based on the size of the refund or a tax preparer who is unwilling to sign the dotted line. Avoid "ghost" preparers, who prepare a return but refuse to sign or include their IRS Preparer Tax Identification Number (PTIN). Never sign a blank or incomplete return.



6 Social Media: Fraudulent form filing and bad advice

The IRS has seen examples of social media content encouraging people to submit false, inaccurate info in hopes of getting a bigger refund. Always remember that if something sounds too good to be true, it probably is.



7 Offer in Compromise Mills

"Offers in Compromise" help people who can't pay to settle their federal tax debts. But "mills" aggressively promote Offers in Compromise in misleading ways to ineligible people. Check your eligibility using the IRS's free Offer in Compromise Pre-Qualifier tool.



8 False Fuel Tax Credit Claims

Sketchy tax return preparers may try to entice you to unknowingly inflate your refund by erroneously claiming the fuel tax credit, which is meant for off-highway business and farming use. Research and vet your tax preparer and double-check the tax credits they recommend.



9 Spearphishing and tax professional cybersecurity

"Spearphishing" is a phishing attempt to a specific org or business. Make sure you vet your tax preparer's cybersecurity protections and verify that messages from your preparer are real before engaging.



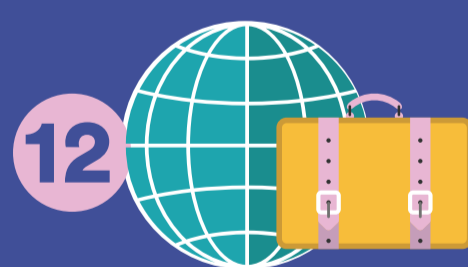
10 Schemes Aimed at High-Income Filers

Avoid promoters and advisors who encourage misuse of Charitable Remainder Trusts. And watch out for promoters who recommend Monetized Installment Sales to defer the recognition of gain on the sale of appreciated property in exchange for a fee.



11 Bogus Tax Avoidance Strategies

A micro-captive is an insurance company whose owners elect to be taxed on the captive's investment income only. Keep an eye out for abusive micro-captives, involving schemes that lack many of the attributes of legitimate insurance. Also watch out for abusive syndicated conservation easement arrangements, which generate high fees for promoters.



12 Schemes with International Elements

The top 3 international tax offenders involve offshore accounts & digital assets, Maltese individual retirement arrangements misusing treaty, and Puerto Rican and foreign captive insurance. Offshore accounts and crypto are not out of reach of the IRS. Don't misconstrue treaty provisions to improperly claim an income tax exemption. Watch out for claiming deductions on insurance arrangements with a Puerto Rican or other foreign corporation because these arrangements often lack attributes of legitimate insurance.

PROTECT YOURSELF AGAINST TAX IMPOSTERS



Be Suspicious

Be skeptical of any call from a government agency asking for money or information. Government agencies don't call you with threats, or promises of – or demands for – money. Scammers do.



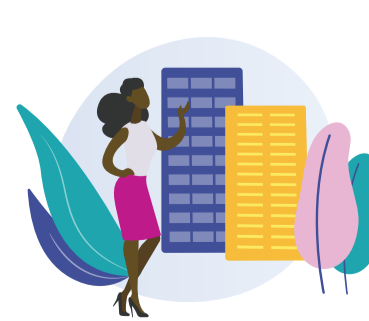
Don't trust caller ID

Caller ID can be faked. Even if it might look like a real call, don't trust it.



Never pay with a gift card or wire transfer

If someone tells you to pay this way, it's a scam.



Check with the real agency

Look up their number. Call them to find out if they're trying to reach you – and why.