

Finance & Fraud

The “Dirty Dozen” tax scams of 2026

The United States Internal Revenue Service just dropped their Dirty Dozen list of 2026’s biggest tax scams.

So, what should you be watching for this year?

The big one is **IRS or tax services impersonation and phishing**. This could be by email and text phishing (“Your tax bill is overdue! Click this link right now to file for an extension!”) or by phone (“Hi, this is Jane from the IRS. If you don’t pay your tax bill today, your case will be handed to our lawyers!”). These scams rely on urgency and fear, pushing you to act before you have time to think.

Another major scam is **fake charities**. Fraudsters create scam charities, and victims donate in hopes of getting a tax deduction. These “charities” often spread word via social media and use AI-generated videos and testimonials to make themselves look legitimate. Again, the urgency of the tax deadline gets you to act quickly.

Social media is also a common source of **tax credit misinformation**. Fraudsters sell phony “tax hacks” that claim to be able to save you money through special credits or creative bookkeeping. Even well-meaning but misinformed people can spread these fake hacks ... And you end up paying the price through penalties and audits. Always verify tax credit information through official channels.

Check out the full list at

<https://www.irs.gov/newsroom/dirty-dozen-tax-scams-for-2026-irs-reminds-taxpayers-to-watch-out-for-dangerous-threats>

Skimmer scams

The US Secret Service warns that card skimmer usage is on the rise.



Skimmers are small devices which capture payment card information when the card is inserted into an ATM or sale terminal



Thieves use the copied payment information to make fraudulent purchases



Terminals with skimmers attached may show signs of tampering: damaged cases, loose keypads, nonoperative keys or lights



ATMs inside financial institutions are harder to tamper with; avoid outside options



Skimmers steal debit card PINs. Consider using a credit card or gift card, rather than a debit card, to pay at POS terminals

How much is your identity worth?

Tax season is prime time for refund fraud. Hackers use stolen identities to claim fraudulent tax refunds — filing early in the season before the real taxpayer does their forms. Each stolen identity could be used to claim hundreds or thousands of dollars in scam refunds, and some hackers cater to this by selling bulk packages of taxpayer identities. One Malwarebytes report found a threat actor catering to this fraud industry by vending taxpayer 1040s and W2s at just \$20 per identity.

