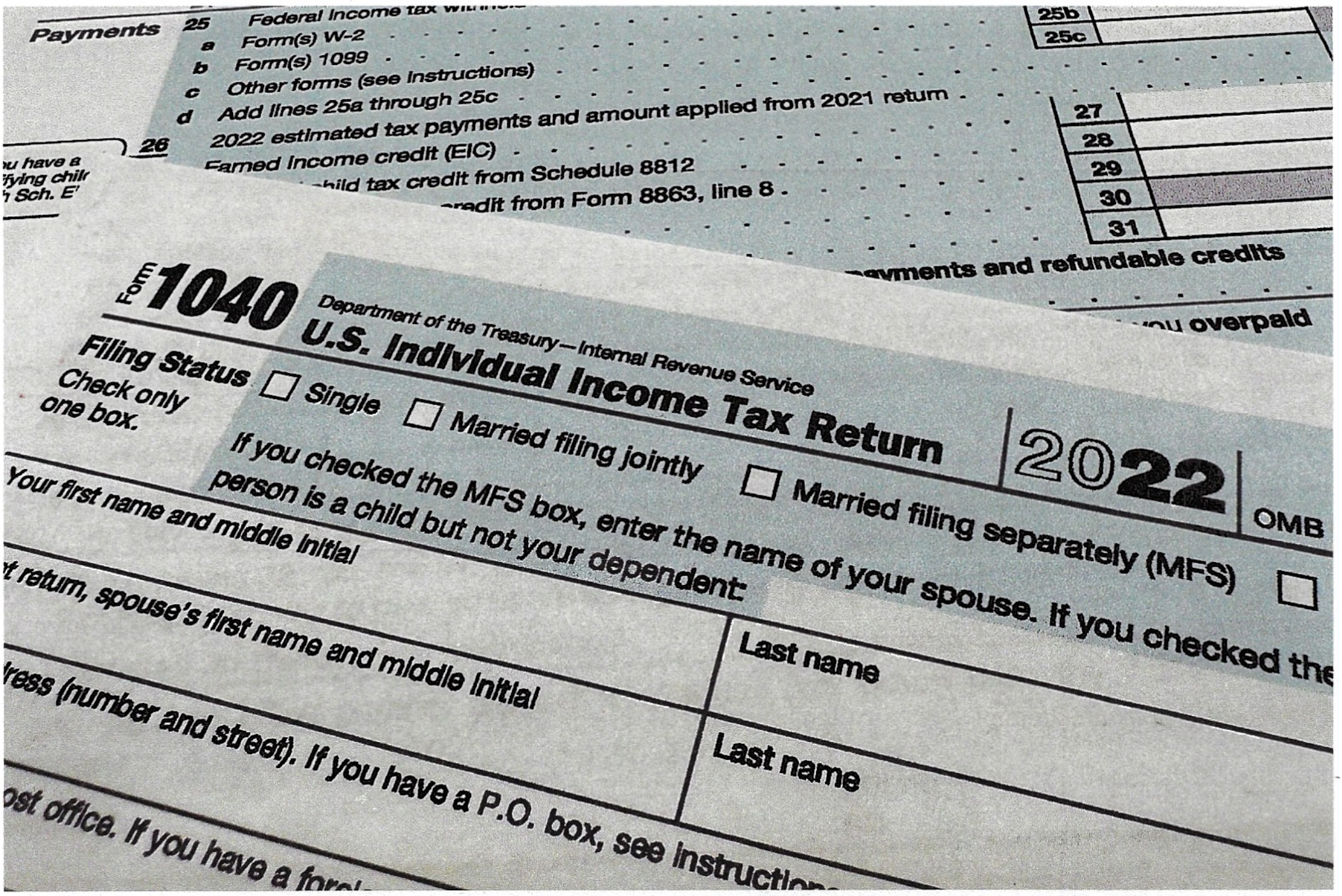
2026-4-5
GTK

Scams are on the rise. Here's what to know



The Internal Revenue Service 1040 tax form for 2022 is seen in 2023. JON ELSWICK — ASSOCIATED PRESS FILE

BY CORA LEWIS

THE ASSOCIATED PRESS

Robocalls, texts, and phishing emails from scammers are up this tax season compared to previous years, with artificial intelligence likely increasing fraud attempts, according to the consumer protection bureau of the Federal Trade Commission. Consumer advocates and government officials urge the public to stay wary, to stop and think before engaging with phone or text messages, and to remember the IRS will not contact you directly by text or phone.

'Tis the season for tax scams

Each year, the IRS releases its "Dirty Dozen" of tax scams that target taxpayers. At the top of the list is impersonation of the agency by email, text, and phone. The IRS reported over 600 social media impersonators during fiscal year 2025, and urges people not to "click links or open attachments from unexpected messages."

(1)

The IRS also reminds taxpayers it "does not leave urgent, threatening prerecorded messages, call to demand immediate payment, or threaten arrest."

Scammers often use alarming language and QR codes to send people to fake websites where they ask the taxpayer to "verify" accounts or enter personal information, according to the IRS. Links may also install malware or malicious software, such as ransomware, which could prevent access to files and private information. "AI-enabled IRS impersonation by phone (robocalls, voice mimicry, and spoofed caller ID)," is also increasing, according to the agency. As phone scams evolve, AI provides new computer-generated tactics and spoofed caller identification to look legitimate.

In this vein, identity theft is one of the most common forms of fraud around tax season, according to Rosario Mendez, an attorney for the bureau of consumer protection at the FTC.

Mendez defines this type of theft as the misuse of one's Social Security number or other personal information, often to collect a tax refund.

"People usually discover this when they go to file their tax returns and discover someone else has already filed," she said. "For the records of the IRS, that is, it's already happened. But it's not the person — it's an identity thief."

A deluge of scams

Eva Velasquez, CEO of the Identity Theft Resource Center, said the ITRC has also tracked an increase in scams and identity theft attempts over the past several years, likely aided by AI-generated messages.

"We're seeing an uptick in phishing emails, fake texts, and even phone calls," Velasquez said. "Scammers are trying to get you to engage in any manner — talk to them, click the link, share your personal data, or share access to your devices or accounts."

The "sheer volume and level of sophistication" suggests AI is being leveraged, according to Velasquez.

"'Deluge' is the best word I can think of, because it's relentless," she said.

'Type, don't tap'

Whenever possible, according to Velasquez, the best practice when receiving any of these messages is, "Type, don't tap." That is, rather than tapping on any link sent in any kind of message, type in the URL of the official website for the IRS (IRS.gov), or whichever agency is supposedly contacting you.

"Go to the source. Don't click any of those links," she said. "If you didn't initiate the contact, don't engage."

Scammers hit all ages

According to Kathy Stokes, director of fraud prevention programs for the AARP, younger people more frequently file reports stating they've been scammed, but older individuals report losing more money than younger consumers.

"That's because they have more money to lose," she said.

If you suspect fraud, or a message seems suspicious, Stokes emphasized the importance of slowing down and talking to someone. When someone receives a notification that sounds strange, scary or urgent, if they stop to talk to a friend or family member or someone they trust, they can typically figure out it's a scam.

"That's also going to inoculate the people you share it with from falling for the scam," she said.

Ask for help if your identity is compromised

If someone has already used your Social Security number to file a tax return before you, it's important to let the IRS know.

You should also go to IdentityTheft.gov to report the theft, according to Mendez. At the end of that reporting process, the government will give you a personal recovery plan.

"If a scammer has used your Social Security number to file a tax return, it's possible the same thief could use it to open bank accounts, credit cards, or file for unemployment," she said. "Another worthwhile step is to monitor your credit report and freeze credit accounts so they can't be misused."

Alan Butler, executive director of the Electronic Privacy Information Center, echoed this, encouraging victims of scams to seek identity theft monitoring going forward as well. That said, he warns people not to pay high costs for these services, which are sometimes shady themselves, but to thoroughly vet the offerings.

"People can be victimized not only once with the theft of their identity, but a second time, because the monitoring services are trying to up-sell them," he said.

A police report also an option

If you've been the victim of a scam and you've lost money, you may also want to file a report with local police, according to Stokes.

"Even if you get pushback from local law enforcement, you should insist on the report," she said. "There may be a means of restitution for fraud victims down the road, and they would want that as a point of proof of what happened."