All One CREDIT UNION

Partnership • Trust • Community

March 2026

Keeping An Eye Out for Tax Fraud Scams

Overview

The 2026 tax season has seen a sophisticated surge in fraud, characterized by the use of AI and high-pressure tactics. With the IRS reporting record levels of identity theft, staying informed on these specific trends is the best line of defense.

Can you spot the "Red Flags?"

2026 Tax Fraud Trends

- **AI-Enhanced Phishing:** Scammers use generative AI to create near-perfect imitations of IRS emails and texts (smishing), making them harder to distinguish from official notices.
- **"Tax Resolution" Scams:** Fraudsters pose as federal "mediation" agents, demanding immediate payment for "back taxes" via untraceable methods like gift cards or cryptocurrency.
- **Early-Season Identity Theft:** Criminals use stolen Social Security numbers to file fraudulent returns the moment the filing window opens, intercepting refunds before the real taxpayer files.
- **Social Media Misinformation:** Viral "tax hacks" on social platforms often encourage illegal filing practices (like falsifying credits) to inflate refunds, leaving the taxpayer liable for fraud.

Could it be a Tax Scam? Ask Yourself These Questions:

1. **Who is Really on the Other End?**

   Is that "IRS agent" providing a name and badge number a little *too* quickly? If the voice sounds slightly off, could it be an AI-generated clone designed to mimic authority? Does the IRS usually start the conversation with a phone call, or is there a paper trail you should have seen first?

2. **Why the Sudden Panic?**

   Does the caller claim you'll be arrested, deported, or lose your license the moment you hang up? Why would a legitimate government agency use fear as its primary negotiation tactic? Is the "urgency" real, or is it just a tool to stop you from thinking clearly?

3. **Since When Does the IRS Take Gift Cards?**

   Would a federal agency truly ask for payment via gift cards, Bitcoin, or a wire transfer? Why are they avoiding official banking channels? If the payment method feels more like a retail transaction than a tax settlement, isn't that a massive red flag?

4. **Where is That Link Actually Taking You?**

   That "secure portal" in your inbox looks official, but have you looked closely at the URL? Does the IRS typically send unsolicited texts with clickable links? Is it a gateway to your refund, or a trap designed to harvest your login credentials?

5. **Is a "Surprise Refund" Too Good to Be True?**

   Why would the IRS reach out to you out of the blue to tell you they owe *you* money? If you didn't file for it, where did this "extra" refund come from? Is it possible that the promise of a windfall is just bait to get your Social Security number?

Proactive Protection Steps

The IRS never initiates contact via telephone, text, email, or social media to request personal or financial information.

- **File Early:** Beating scammers to the punch is the most effective way to lock your Social Security number for the season.
- **Get an IP PIN:** Use the IRS "Identity Protection PIN" system to add a mandatory six-digit security code to your return.
- **Verify Your Preparer:** Ensure any professional you hire has a valid Preparer Tax Identification Number (PTIN).
- **Ignore "Immediate" Demands:** Legitimate IRS tax bills are sent by mail and provide options for appeal; they never demand wire transfers or prepaid cards.

If You Are a Victim

- Stop interacting with the scammer immediately!
- Notify All One Credit Union at 800-649-4646.
- If you feel your identity has been stolen, report it to IdentityTheft.gov.
- Report the incident to the Internet Crime Center.
- Report the incident to the Federal Trade Commission.
- Contact the IRS.