



Identity Theft and Your Taxes

Sprague & Jackson

ACCOUNTANTS AND ENROLLED AGENTS

The Seneca Building • 121 E Seneca St • Ithaca, NY 14850

Identity Theft and Your Taxes

Your identity and money can be stolen in a tax-related scam via email (“phishing”), fax, phone, or letters. Some common examples of identity theft scams are:

- **Phone scam.** A bogus phone call or text message where you are told you owe the IRS money and threatened that a warrant will be issued for your arrest. Variations include the threat of other law-enforcement agency intervention, deportation, or revocation of licenses. Some scam artists program their computers to display IRS phone numbers on your caller ID.
- **Email phishing scam.** A bogus email that appears to be from the IRS or a program closely related to the IRS, such as the Electronic Federal Tax Payment System (EFTPS), that attempts to trick you into revealing personal and financial information. The email includes links to bogus websites intended to mirror the official IRS website.
- **Tax transcript.** The bogus email carries an attachment labeled “Tax Account Transcript” or something similar, and the subject line uses some variation of the phrase “tax transcript.” The attachment may contain a computer virus or malware.
- **IRS refunds.** A bogus email, claiming to come from the IRS, tells you that you are eligible to receive a tax refund for a given amount if you just follow the instructions in the email.

Notify the IRS

If you receive a tax-related phishing email, do not click on the links or open any attachments. Forward the email to phishing@irs.gov or call the Treasury Inspector General for Tax Administration at 800-366-4484.

David W. Sprague, EA, ABA Principal
Angie Jackson, EA, MSA Principal

Phone: (607) 273-5322

Fax: (607) 273-8138

Email: Admin@sprjac.com

How the IRS Contacts Taxpayers

- The IRS will never initiate contact with you by email, text message, or any social media channels to request personal or financial information.
- It is unusual for the IRS to initiate contact by fax or phone call. You can call the IRS at 800-829-1040 to verify that an unexpected fax or phone call is legitimate.

Fraudulent Tax Returns

An identity thief might use your Social Security Number to fraudulently file a tax return and claim a refund. You could be completely unaware that your identity has been stolen until your return is rejected for e-filing or you get an IRS notice or letter.

Rejected e-File

Your electronically-filed return is rejected because the Social Security Number belonging to you, your spouse, or a dependent has already been used on a tax return.

- This situation can occur because of a mistyped number or dispute about claiming a dependency exemption. Such cases do not necessarily indicate identity theft.
- If your return has been rejected because of a previously used Social Security Number, it cannot be e-filed. You must file a paper return.

IRS Notice

You receive an IRS notice or letter stating that:

- More than one return was filed in your name for the year,
- You have a balance due, refund offset, or initiation of collection action for a year when you did not file a return, or
- IRS records indicate that you received wages from an employer you didn't work for.