

Taxpayer Guide to Identity Theft

 [irs.gov/newsroom/taxpayer-guide-to-identity-theft](https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft)



For 2017, the IRS, the states and the tax industry joined together to [enact new safeguards](#) and take additional actions to combat tax-related identity theft. Many of these safeguards will be invisible to you, but invaluable to our fight against these criminal syndicates. If you prepare your own return with tax software, you will see new log-on standards. Some states also have taken additional steps. See your [state revenue agency's web site](#) for additional details.

We also know identity theft is a frustrating process for victims. If you become a victim, we are committed to resolving your case as quickly as possible.

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses your stolen Social Security number to file a tax return claiming a fraudulent refund.

You may be unaware that this has happened until you efile your return and discover that a return already has been filed using your SSN. Or, the IRS may send you a letter saying we have identified a suspicious return using your SSN.

Know the warning signs

Be alert to possible tax-related identity theft if you are contacted by the IRS or your tax professional/provider about:

- More than one tax return was filed using your SSN.
- You owe additional tax, refund offset or have had collection actions taken against you for a year you did not file a tax return.
- IRS records indicate you received wages or other income from an employer for whom you did not work.

If you suspect you are a victim of identity theft, continue to pay your taxes and file your tax return, even if you must do so by paper.

Steps to take if you become a victim

If you are a victim of identity theft, the Federal Trade Commission recommends these steps:

- File a complaint with the FTC at [identitytheft.gov](https://www.ftc.gov/identitytheft).

- Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:
 - Equifax, www.Equifax.com, 800-525-6285
 - Experian, www.Experian.com, 888-397-3742
 - TransUnion, www.TransUnion.com, 800-680-7289
- Contact your financial institutions, and close any financial or credit accounts opened without your permission or tampered with by identity thieves.

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

- Respond immediately to any IRS notice; call the number provided.
- Complete IRS [Form 14039](#), Identity Theft Affidavit, if your efiled return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach the form to your return and mail according to instructions.

If you previously contacted the IRS and did not have a resolution, contact us for specialized assistance at 1-800-908-4490. We have teams available to assist.

About data breaches and your taxes

Not all data breaches or computer hacks result in tax-related identity theft. It's important to know what type of personal information was stolen.

If you've been a [victim of a data breach](#), keep in touch with the company to learn what it is doing to protect you and follow the "Steps for victims of identity theft." Data breach victims should submit a Form 14039, Identity Theft Affidavit, **only** if your Social Security number has been compromised and your efile return was rejected as a duplicate or IRS has informed you that you may be a victim of tax-related identity theft.

How to reduce your risk

Join efforts by the IRS, states and tax industry to protect your data. [Taxes. Security. Together.](#) We all have a role to play. Here's how you can help:

- Always use security software with firewall and anti-virus protections. Use strong passwords.
- Learn to recognize and avoid phishing emails, threatening calls and texts from thieves posing as legitimate organizations such as your bank, credit card companies and even the IRS.
- Do not click on links or download attachments from unknown or suspicious emails.
- Protect your personal data. Don't routinely carry your Social Security card, and make sure your tax records are secure.

See [Publication 4524](#), Security Awareness for Taxpayers, to learn more .

The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

Report suspicious online or emailed phishing scams to: phishing@irs.gov. For phishing scams by phone, fax or mail, call 1-800-366-4484. Report IRS impersonation scams to the Treasury Inspector General for Tax Administration's [IRS Impersonation Scams Reporting](#).

See the main [Identity Protection](#) page for more information.