







# Prepare for Tax Scams



Tax season tends to be stressful and has a built-in sense of urgency for everyone. Some taxpayers are so afraid of the IRS that they are easy prey for predatory criminals who use the cover of the tax season to target them in an attempt to steal their information, their tax refunds, and even their identities. To protect themselves from these criminals, taxpayers need to learn how to recognize fraudulent tax offers.

[Norton Lifelock](#) warns against tax-related identity theft, which is when scammers steal your personal information or buy it from the dark web and use your Social Security number (SSN), address, birthdate, and other information to file an income tax return in your name in order to steal your tax return. If the IRS does any of the following, you may be a victim of this form of identity theft:

-  Informs you that a return for your SSN has already been filed
-  Rejects your electronic return
-  Sends you a transcript that you haven't requested
-  Sends you a letter informing you that you have created an online profile when you haven't



You can report tax-related identity theft by completing [IRS Form 14039, Identity Theft Affidavit](#) and attaching a hard copy to your return. You should also report the theft to the [Federal Trade Commission](#) and place a fraud alert and freeze on your credit reports by contacting the three national credit bureaus [Experian](#), [Equifax](#), and [TransUnion](#). You can request a copy of the fraudulent tax return from the IRS. For more information, visit the [IRS' page on dealing with fraudulent returns](#).



The federal government sent stimulus payments to taxpayers during the pandemic, but mailed the most recent stimulus payments in late 2021 and early 2022. If you receive an email claiming to be from the IRS stating that you are due a stimulus payment, it's a scam. These emails typically ask you to click on a link to receive your payment. This link takes you to a page requesting personal and financial/bank information, everything from your Social Security number to your birth date and driver's license number. If you provide this information, you'll be sending it to criminals who can use it to steal your identity.

For more tips on protecting yourself from tax-related identity theft and other tax-related scams, visit [Norton Lifelock](#).

[Nerdwallet](#), a personal finance company that provide information to educates users in making financial decisions, describes multiple scams that criminals use to try to steal taxpayer information, money, or identities. These include the following scams that you should watch out for:



- ❖ A letter claiming to be from the Bureau of Tax Enforcement asserting that you have a tax lien or tax levy and that you had better pay the “Bureau of Tax Enforcement” or else is a scam. This “Bureau” does not exist.
- ❖ Fraudulent emails may display the IRS logo and use subject lines such as “Tax Refund Payment” or “Recalculation of your tax refund payment.” They usually request that you provide information to help the IRS recalculate your refund. These emails contain links to a fake IRS page with a form that allows the criminal to collect users’ personal information like Social Security number, birthday, address, and driver’s license number allegedly to help those users claim their refunds. These scammers may also sometimes use a “.edu” email address to target college students.

❖ One scam that preys on people who may not speak English well and fear the IRS is sending a message claiming that the recipient must complete Form W-8BEN, which is called a “Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding.” Although this is a legitimate IRS form, criminals have been modifying it to ask for personal information such as mother’s maiden name, passport numbers, and PIN numbers. (The real form is available through the IRS official web site’s [forms page](#).)



❖ Anyone you pay to prepare your tax return must have a valid preparer tax identification number and must sign your tax return. Reluctance to sign your return is a red flag that the person is not a legitimate preparer, but just wants to charge you a fee and disappear.

❖ Phone calls claiming that if you don’t act immediately, the caller will suspend or cancel your Social Security number. Criminals can make a caller ID phone number look like it’s coming from

anywhere — including from the IRS, the local police, or some other intimidating source. But the IRS doesn’t leave prerecorded voicemails, especially ones that claim to be urgent or are threatening. Also, the IRS can’t revoke your Social Security number, driver’s license, business licenses, or immigration status. The IRS says that “if taxpayers receive a call threatening to suspend their SSN for an unpaid tax bill, they should just hang up.”

Visit <https://www.nerdwallet.com/article/taxes/avoid-irs-scams> to see their entire list of tax scams to be aware of as well as ten ways to spot scams or IRS impersonators.



If anyone contacts you offering to help you lower your tax burden by helping you move funds to an offshore or overseas account, the account they mean is their own. If you give them your bank information, they will drain your account, and it's likely you'll never see your money again. Note that even if the person delivered exactly the off-shore tax shelter service they were offering, the IRS frowns upon tax evasion, and you could end up paying fines and spending time in prison.



The [Internal Revenue Service \(IRS\)](#) provides the following indicators of tax scams along with actions taxpayers can take if they receive a scam call.

### The IRS will never:

- ❏ Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card, or wire transfer. Generally, the IRS will first mail a bill to any taxpayer who owes taxes.
- ❏ Threaten to immediately bring in local police or other law enforcement groups to have the taxpayer arrested for not paying.
- ❏ Demand that taxes be paid without giving taxpayers the opportunity to question or appeal the amount owed.
- ❏ Call unexpectedly about a tax refund or contact you through social media.



### Taxpayers who receive fraudulent IRS phone calls should:

- ❏ Report impersonation scams to the [Treasury Inspector General for Tax Administration](#). Taxpayers can also call 800-366-4484 to report impersonation scams or report to them by mail at:  
Treasury Inspector General for Tax Administration  
Hotline Team  
Ben Franklin Station  
P.O. Box 589  
Washington, D.C. 20044-0589
- ❏ Report any unsolicited email claiming to be from the IRS or an IRS-related system like the Electronic Federal Tax Payment System to the IRS at [phishing@irs.gov](mailto:phishing@irs.gov).
- ❏ Protect your community by reporting fraud, scams, and bad business practices. Report fraud to [Report Fraud FTC](#). Include "IRS Telephone Scam" in the notes.
- ❏ For a comprehensive listing of recent tax scams, consumer alerts and how to report them, visit [Tax Scams/Consumer Alerts](#).



Please contact [cybersecurity@ihs.gov](mailto:cybersecurity@ihs.gov) with any questions or comments about this newsletter.

*(Note: The links in this document are for informational purposes only and do not signify an endorsement of any products contained within the linked sites.)*