Identity Protection Tips

Top tips every taxpayer should know about identity theft

Identity theft often starts outside of the tax administration system when someone's personal information is stolen or lost. Identity thieves may then use a taxpayer's identity to fraudulently file a tax return and claim a refund. In other cases, the identity thief uses the taxpayer's personal information in order to get a job. The legitimate taxpayer may be unaware that anything has happened until they file their return later in the filing season and discover two returns have been filed using the same Social Security number.

These are the IRS' top tips to help you avoid becoming the victim of an identity thief.

1. The IRS does not initiate contact with taxpayers by email or social media tools to request personal or financial information. The IRS does not send emails stating you are being electronically audited or that you are getting a refund. This includes any type of electronic communication, such as text messages and social media channels.

2. If you receive a scam email claiming to be from the IRS, forward it to the IRS at phishing@irs.gov.

3. Identity thieves access your personal information by many different means, including:
   - Stealing your wallet or purse
   - Posing as someone who needs information about you through a phone call or email
   - Looking through your trash for personal information
   - Accessing information you provide to an unsecured Internet site.

4. If you discover a website that claims to be the IRS but does not begin with 'www.irs.gov', forward that link to the IRS at phishing@irs.gov.

5. To learn how to identify a secure website, visit the Federal Trade Commission's website.

6. If your SSN is stolen, another individual may use it to get a job. That person's employer may report income earned by them to the IRS using your SSN, thus making it appear you did not report all of your income on your tax return.

   When this occurs, you should contact the IRS to show the income is not yours. After the IRS authenticates who you are, your tax record will be updated to reflect only your information. The IRS will use this information to minimize future occurrences.

7. Your identity may have been stolen if a letter from the IRS indicates more than one tax return was filed for you or the letter states you received wages from an employer you don't know. If you receive such a letter from the IRS, leading you to believe your identity has been stolen, respond immediately to the name, address or phone number on the IRS notice. If you believe the notice is not from the IRS, contact the IRS to determine if the letter is a legitimate IRS notice.

8. If your tax records are not currently affected by identity theft, but you believe you may be at risk due to a lost wallet, questionable credit card activity, or credit report, you need to provide the IRS with proof of your identity. You should submit a copy of your valid government-issued identification, such as a Social Security card, driver's license or passport, along with a copy of a police report and/or a completed IRS Form 14039, Identity Theft Affidavit, which should be faxed to the IRS at 1-855-807-5720. Please be sure to write clearly.

   As an option, you can also contact the IRS Identity Protection Specialized Unit, toll-free at 1-800-908-4490. IPSU hours of Operation: Monday - Friday, 7:00 a.m. - 7:00 p.m. your local time (Alaska & Hawaii follow Pacific Time).

   You should also follow FTC's guidance for reporting identity theft

9. Show your Social Security card to your employer when you start a job or to your financial institution for tax reporting purposes. Do not routinely carry your card or other documents that display your SSN.

10. For more information about identity theft, including information about how to report identity theft, phishing and related fraudulent activity, visit the IRS Identity Theft Protection page, which you can find by searching ***identity theft*** on the IRS.gov home page.

11. IRS impersonation schemes flourish during tax season and can take the form of email, websites, even tweets. Scammers may also use a phone or fax to reach their victims. If you receive a paper letter or notice via mail claiming to be the IRS but you suspect it is a scam, check the IRS phishing page at IRS.gov/phishing to determine if it is a legitimate IRS notice or letter. If it is a legitimate IRS notice or letter, reply if needed. If the caller or party that sent the paper letter is not legitimate, contact the Treasury Inspector General for Tax Administration at 1-800-366-4484. You may also fax the notice/letter you received plus any related or supporting information to TIGTA. **Note:** This is not a toll-free FAX number 1-202-927-7018.

12. While preparing your tax return for electronic filing, make sure to use a strong password to protect the data file. Once your return has been e-filed, save the file to a CD or flash drive and then delete the personal return information from your hard drive. Store the CD or flash drive in a safe place, such as a lock box or safe. If working with an accountant, you should query them on what measures they take to protect your information.

13. If you have information about the identity thief that impacted your personal information negatively, file an online complaint with the Internet Crime Complaint Center. The IC3 gives victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. IC3 sends every complaint to one or more law enforcement or regulatory agencies that have jurisdiction over the matter.