



Identity protection tips

Tax-related identity theft occurs when someone uses your stolen Social Security number (SSN) to file a tax return claiming a fraudulent refund. You may be unaware you are a victim until you receive an IRS notice or try to file your return. It's important that you take steps to protect all of your personally identifiable information (PII).

Identity theft occurs when someone uses your (PII) without your permission. Examples of PII include your:



- Name, address and telephone number
- Social Security number
- Employer Identification number
- Credit card or bank account numbers
- Email or Internet Protocol (IP) address
- Driver's license number
- Passport number

Tips to protect your SSN and PII

- Keep your card and any other document that shows your SSN in a safe place.
- **DO NOT** routinely carry your card or other documents that display your number.
- **ONLY** share your SSN when absolutely necessary.
- **Protect your personal financial information at home and on your computer.**
- **Check your credit report often.**
- Check your Social Security Administration earnings statement annually.
- Protect your personal computers by using firewalls, anti-spam/virus software, update security patches and change passwords for Internet accounts.
- Protect your PII; keep it private. Only provide your SSN when YOU initiate contact, or you are sure who you know is asking for it.


Don't fall for common **scams**

- An unexpected email pretending to be from the IRS is always a scam. The IRS does not initiate contact with taxpayers by email or social media to request personal or financial information. If you receive a scam email claiming to be from the IRS, [forward the email](mailto:phishing@irs.gov) to phishing@irs.gov.

- An unexpected phone call from someone claiming to be an IRS agent, threatening you with arrest or deportation if you fail to pay immediately, is a scam. In another scam, the caller requests your financial information in order to send you a refund. Do not provide any information and report these calls and other IRS impersonation schemes to the Treasury Inspector General for Tax Administration at [800-366-4484](tel:800-366-4484) or online at [IRS Impersonation Scam Reporting](#) .
- If you discover a website that claims to be the IRS but does not begin with 'www.irs.gov,' forward the link to phishing@irs.gov .

Data breach information

A [data breach](#) is the intentional theft or unintentional release of secure information. Not all data breaches or computer hacks result in identity theft. It's important to know what type of PII was stolen. For example, did a data breach compromise your credit card, or did it compromise your SSN?

- If your credit card information was compromised it is not considered tax-related identity theft and you should follow the steps at www.identitytheft.gov .
- If your SSN was compromised, follow the steps outlined in the [Identity theft guide for individuals](#).

Other resources:

[Identity theft central](#)

[Identity Theft, Publication 5423](#) 

[Identity Theft Information for Taxpayers, Publication 5027](#) 

[Security Awareness for Taxpayers, Publication 4524](#) 

Page Last Reviewed or Updated: 06-Feb-2025