Protect yourself and your parents from tax fraud

Keep an eye out for warning signs and reduce your vulnerability with a few simple tips.

Identity thieves steal other people's personal information and use it to file tax returns. These criminals often file fraudulent tax returns as early as possible to have the bogus return processed before you can file your own legitimate return. You may therefore be unaware you've been victimized until you attempt to file your taxes.

These scammers are stealing money from the government while also hindering your ability to file a genuine tax return, not to mention creating undue stress as you take efforts to rectify the situation. It's important to be aware of this scheme and take steps to prevent this from happening to you and your loved ones.

Prevention tips

There are several ways to reduce your family's chances of becoming a victim of tax return identity fraud:

- Keep your Social Security number, as well as other personal information, stored in a secure place (i.e., not your wallet), and avoid mentioning it on the phone or online unless necessary.
- Consider installing extra security on your computer.
- Be sure to check your credit report and Social Security Administration earnings regularly, looking for anything suspicious or irregular.
- Be aware that the IRS does not routinely email, make phone calls or communicate through social media. Any communication from those sources is likely to be fraudulent and should immediately be reported to phishing@irs.gov.
- Assume that unexpected calls from the IRS urging you to give or confirm financial information are fraudulent. They should be reported to treasury.gov.

Warning signs

Be on the lookout for IRS notices that appear to be inaccurate. These may include notices that more than one tax return was filed with your Social Security number, that you owe an additional tax that appears to be inappropriate or that you've received wages from an unknown employer.

IRS FAQs

Will the IRS contact me via email? The IRS will never initiate contact with you via e-mail, text messages or social media with a request for personal or financial data. Be extremely careful with any unsolicited email that claims to be from the IRS.

What should I do if I receive an email or text message claiming to be from the IRS or another tax service that asks for sensitive information? Do not reply. Do not click on any links or download any attachments. Forward any IRS-related emails to phishing@irs.gov.

What should I do if I discover a website claiming to be the IRS that I suspect is not legitimate? Do not click any links, download any files, or submit any information. Send the URL to phishing@irs.gov.

Are there any trusted resources I can use to identify email scams or websites claiming to be the IRS? The IRS website highlights examples of email scams and bogus websites. Find this information online at www.irs.gov/uac/report-phishing.

What should I do if I receive an unsolicited phone call or letter claiming to be from the IRS that I suspect may not be legitimate? Contact the IRS yourself to confirm any requests made via phone or letter, particularly those that are threatening or demand immediate payment. Visit www.irs.gov/uac/report-phishing for phone numbers and other tips.

Consider an IP PIN

In some instances, you may be eligible for a number called an Identity Protection PIN (IP PIN). An IP PIN is a six-digit number given to qualified taxpayers to help prevent the filing of false tax returns. Once a taxpayer obtains his or her unique IP PIN, all his or her tax returns must be filed using this number, which can help ensure that no other fraudulent returns are filed. Please note that this PIN is different than the four-digit e-file signature PIN, which is used for filing online returns.

If you are interested in obtaining an IP PIN, you can register your PIN by following the steps at irs.gov/Individuals/Get-An-Identity-Protection-PIN.

For more information on IRS tax return fraud and prevention methods, visit irs.gov.

This resource includes content created by EverSafe. Raymond James is not affiliated with EverSafe.