



Safeguarding Your Personal Information

February 12, 2016

Earlier this week the IRS announced identity thieves successfully hacked into the IRS computer system in an attempt to gain information that could be used to steal tax refunds. The agency said the thieves used personal data of taxpayers that was stolen elsewhere in an attempt to generate E-file PIN numbers that could be used to file fraudulent tax returns. Of the 464,000 Social Security Numbers involved, a total of 101,000 successfully generated an E-File PIN number. No personal data was compromised or disclosed by the IRS. If your social security number was affected by this attack, the IRS will notify you via mail and has marked the accounts affected to prevent against additional fraudulent behavior.

As we head into tax season, this is a good reminder of the importance of safeguarding your personal information.

How can you protect your personal information?

- 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 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.
- If you are eligible, establish an IRS Identity Protection PIN. An IP PIN is a six-digit number assigned to eligible taxpayers that helps prevent the misuse of your Social Security number on fraudulent federal income tax returns. Currently, only taxpayers who have had their tax data compromised are eligible to receive an IP PIN. The IRS also has a pilot program in Florida, Georgia and the District of Columbia whereby taxpayers who filed returns last year in those places can apply for an IP PIN. Eligible taxpayers can file for IP PINs by <https://www.irs.gov/Individuals/Get-An-Identity-Protection-PIN>

For more information from the IRS on Identity Protection <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft>

UPDATE ON TAX SCAMS:

Earlier this month the IRS issued an alert about taxpayers receiving aggressive and threatening phone calls from criminals impersonating IRS agents. In an attempt to collect private information scammers are stating you owe money or you will be receiving a refund from the IRS. If you refuse to pay or provide additional information the scam artists threaten police arrest, deportation, license revocation etc.

IRS Commissioner John Koskinen quotes "if you are surprised to be hearing from us, then you're not hearing from us."

A list of “Dirty Dozen Tax Scams” is compiled annually by the IRS and lists a variety of common scams taxpayers may encounter any time during the year. Many of these con games peak during filing season as people prepare their tax returns or hire someone to do so.

For more information about IRS Phishing Alert <https://www.irs.gov/uac/Newsroom/Phishing-Remains-on-the-IRS-Dirty%20Dozen-List-of-Tax-Scams-for-the-2016-Filing-Season>

For more information about the IRS Dirty Dozen list <https://www.irs.gov/uac/Newsroom/Dirty-Dozen-2016>

It is important to keep in mind the IRS generally does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as email, text messages, and social media channels.

The IRS will never:

1. Call to demand immediate payment, nor will the agency call about taxes owed without first having mailed you a bill.
2. Demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe.
3. Require you to use a specific payment method for your taxes, such as a prepaid debit card.
4. Ask for credit or debit card numbers over the phone.
5. Threaten to bring in local police or other law-enforcement groups to have you arrested for not paying.

What do I do if I receive an alarming phone call or email from someone claiming to be from the IRS?

- Do not give out any information. Hang up immediately.
- Contact the Treasury Inspector General for Tax Administration (TIGTA) by phone at 800-366-4484 or by completing the IRS Impersonation Scam Reporting at https://www.treasury.gov/tigta/contact_report_scam.shtml
- Report it to the Federal Trade Commission by completing the FTC Complaint Assistant at <https://www.ftccomplaintassistant.gov/GettingStarted?NextQID=216&Selected=t%20-%20crnt#crnt>. Please add "IRS Telephone Scam" in the notes.
- Of course, contact us, and we will provide assistance as needed

As always, please feel free to contact us with any questions about your personal situation.



Stephen G. Green, CFP®

Scott M. Lefebvre, CPA/PFS

G. Joseph Votava, Jr., CFP®, CPA, JD

Rochester, NY

Washington, DC