TIPS TO HELP AVOID TAX-REFUND SCAMS

At tax time, law-abiding U.S. citizens are sharpening their pencils, gathering receipts and scrambling to find the correct forms to fulfill their duties as taxpayers. At the same time, identity thieves and scammers are sharpening their devious skills, coming up with new schemes to defraud the government and you. While such activity increases during tax season, fraudsters and Internal Revenue Service (IRS) impostors can strike any time of year. Learn about some common tax refund–related scams and tips to help avoid becoming a victim.

PHISHING, VISHING AND SMISHING

Scammers pretend to be IRS agents and contact taxpayers directly, demanding payment for taxes they claim are owed. They often threaten you with fines, arrest or garnishing of wages if you fail to cooperate. They may use official-sounding titles and sprinkle in some of your personal information, which is easily harvested from the internet. This scamming may be done with a phone call **(vishing)**, an email **(phishing)** or a text message **(SMiShing)** on your smartphone.

GOAL OF PHISHING SCHEMES

- Scare you into giving them money
- "Fishing" for personal data and information that may be used for identity theft
- Infect your device with malicious code designed to capture keystrokes, such as those you used to log in to your online bank account

DON'T TAKE THE BAIT OF THESE IRS PHISHING SCHEMES

- If you have not previously been notified in writing by the IRS of an issue, hang up phone calls and delete emails if they claim to be from an IRS agent. The IRS will first contact you in writing through the mail regarding any tax information. To avoid potential issues, do not take phone calls from unknown phone numbers.
- Do not open email attachments or click on email links claiming to be from the IRS.

THE U.S. IRS WILL NOT:

- Call to demand immediate payment without first mailing you a bill
- Demand that you pay taxes without allowing you to question or appeal the amount
- Require you to use a specific method of payment, such as a prepaid debit card
- Ask for PINs, passwords or confidential access information for credit cards or bank accounts over the phone or email.
- Threaten to arrest you for not paying

PNC BANK

TAX REFUND IDENTITY THEFT

Tax refund identity theft happens when bad actors get their hands on your personal information, such as your name, date of birth and/or Social Security number and use that information to file a fraudulent tax return and obtain a refund, redirecting it to their account. It does not matter if your legitimate tax return indicates that you owe taxes or that the government owes you a refund.

COMMON WARNING SIGNS

- **Rejected return:** If an identity thief files a fake tax return for a refund, any additional returns filed using the same Social Security number will be rejected. You may be the victim if the IRS or tax preparer notifies you that your return has been rejected due to a previously filed return under the same Social Security number.
- **Fake wages/employer:** Identity thieves will file false tax returns using employer data that does not match your true employer.
- **Collection attempts:** The IRS or a tax professional may notify you **in writing** about additional taxes owed, collection action taken against you or a refund reduction due to unpaid debts known officially as a refund offset. While honest mistakes happen among legitimate taxpayers, it could also indicate a fraudster using your Social Security number.
- **Unpaid taxes in your minor child's name:** If you receive an IRS notification about unpaid taxes in your child's name, it may indicate his or her identity has been stolen. Identity thieves can use a child's Social Security number to file fraudulent tax returns and secure fraudulent credit and debt that can often go undetected for years.

HELP PROTECT YOUR IDENTITY

- File early! The IRS will reject any duplicate returns filed under a Social Security number. Submit your legitimate tax return and secure a refund before an identity thief files a fraudulent one with your Social Security number.
- Do not use public Wi-Fi when filing your tax returns.
- Use security software with firewall and anti-virus protections when accessing the internet.
- Use strong passwords for online accounts — at least 10 characters, alpha-numeric, mixed case and special characters. Never repeat passwords across multiple accounts.
- Spot and avoid phishing emails, SMiShing text messages and vishing phone calls.
- Keep your Social Security cards and tax records safe and secure at all times.

TAX PREPARER FRAUD

Dishonest tax preparers can take advantage of you through refund fraud and identity theft. But there is also a new threat that targets tax preparers and their clients: Cybercriminals are posing as potential clients with the goal of gaining access to the tax preparer's existing client database. The scammer poses as a client and sends an email containing malware to infect the preparer's computer and can access all of the files and information on the preparer's device.

TAKE PRECAUTIONS

- Ask for recommendations and research a tax preparer thoroughly before you hand over financial documents and personal information.
- Also ask what steps the preparer takes to protect and secure your files from unauthorized access.
- Inquire if your tax preparer/firm has ever been hacked.
- Ask if employees are trained on security protocols such as not clicking on links or opening attachments from unknown email senders who may be posing as prospective clients or the IRS.

To stay up to date with the latest details on these (and other) tax scams, you can visit **irs.gov**.

Please report IRS-related fraud with an email to **phishing@irs.gov** or report online at **treasury.gov/tigta/contact_report_scam.shtml**.

CON PDF 0520-0111

PNC BANK