Self Defense For Taxpayers: Five Common Scams Targeting U.S. Taxpayers

PITTSBURGH, Feb. 15, 2017 -- Tis the season - Tax Time. Law-abiding residents across the nation are sharpening their pencils, gathering receipts and scrambling to find the correct forms, in order to fulfill their duties as tax-paying citizens. At the same time, identity thieves and scammers are sharpening their devious plans and inventing new schemes to defraud you and the government. Learn to defend yourself against some common tax fraud scams: block the attack with knowledge, deliver a response when faced by the threat (see tips below), and speed up your tax filing.

Trevor Buxton, Fraud Awareness & Communications Manager, PNC Bank

"At the heart of many tax fraud scams is using fear and intimidation with law-abiding citizens who follow the rules, suggesting that they are in big trouble with the IRS [Internal Revenue Service]," said Trevor Buxton, fraud awareness and communications manager at PNC Bank. "Tax payers need to remember -- if you owe taxes, the IRS will first contact you in writing through the United States Postal Service - not by telephone and not by email."

PNC offers a list of the most prevalent scams targeting U.S. taxpayers:

1. **Identity Theft** – Topping the list is the unauthorized use of an individual's Social Security number to file a tax return and claim a bogus refund. The internet is a rich source of personal information about you, including valuable personally identifiable information such as birthdates, addresses, telephone numbers and driver's license numbers, to name a few. What's not readily available on the web, such as bank account information and social security numbers, may be bought on the black market or retrieved from your garbage and recycling bins set out on the curb one day each week.
2. **Phone Scams** – Scammers impersonate IRS agents and call taxpayers claiming taxes are owed, often threatening fines, arrest, garnishing of wages, etc., for failure to collaborate. They may use official-sounding titles and sprinkle in some of the taxpayer's personally identifiable information (easily harvested on the worldwide web) to make themselves sound legitimate.
3. **Phishing** – Scammers impersonating IRS agents via email – same as phone calls described above. Caution! These emails also may contain malware to infect the taxpayer's computer by capturing keystrokes, accessing personal files on the device, etc.
4. **Fake Charities** – Bogus charities unfortunately exist, often cropping up following a major natural disaster, such as the spring 2016 floods in Louisiana or the pre-Christmas Tennessee wild fires. Taxpayers are urged to visit the Exempt Organizations Select Check on the IRS website to ensure a charity is legitimate and qualifies for deductible contributions.
5. **Tax Preparer fraud** – Dishonest tax preparers exploit taxpayers perpetrating refund fraud and identity theft.

But there is also a new threat: It's a phishing scam. Posing as a potential client, the scammer sends an email containing malware to infect the tax preparer's computer, gaining access to all of the files and information on the preparer's device.

Defend yourself and your family from these tax fraud schemes with the following tips:

- **File early!** Who would have imagined that you have to race the bad guys to pay your taxes. Play it smart. Submit your legitimate tax return and secure a refund before the identity thief gets one in using your social security number to file a fraudulent claim/refund.

- **Do not use public Wi-Fi** when filing your tax returns. In fact, it's a good idea to avoid using public networks when conducting any business that involves your finances and personal information such as online banking and job applications. The information you enter can be harvested and used by identity thieves.

- Unless notified first in writing by the Internal Revenue Service (IRS),**hang up on phone callers claiming to be an IRS agent.**

- **Do not open files attached to emails claiming to be from the IRS.**

- **Do not click on links in emails claiming to be from the IRS.**The IRS does not make initial contact with taxpayers or request personal information via email.

- **Ask questions before turning over bank account or credit card information.**The IRS also does not ask over

the phone for PINs, passwords, or confidential access information for credit cards or bank accounts.

- **Ask for recommendations and research a tax preparer** thoroughly before you hand over financial documents and personal information.

For more information on identity theft, visit the Security and Privacy website on www.pnc.com. Report IRS imposter scams to the FTC at ftc.gov/complaint.

PNC Bank, National Association is a member of The PNC Financial Services Group, Inc. (NYSE: PNC). PNC is one of the largest diversified financial services institutions in the United States, organized around its customers and communities for strong relationships and local delivery of retail and business banking; residential mortgage banking; specialized services for corporations and government entities, including corporate banking, real estate finance and asset-based lending; wealth management and asset management. For information about PNC, visit www.pnc.com.

CONTACT:
Amy Vargo
(412) 762-1535
amy.vargo@pnc.com

Additional assets available online: Video (1) Photos (1)

https://pnc.mediaroom.com/2017-02-15-Self-Defense-For-Taxpayers-Five-Common-Scams-Targeting-U-S-Taxpayers