PPL
www.PPLCPA.com

National Tax Security Awareness Week

Identity Theft

The holiday season is in full swing which gives identity thieves the opportunity to try to steal personal financial information. This information could be used to file fraudulent tax returns. Be aware if you are shopping online and using publicly accessible Wi-Fi as this can increase your risk for identity theft. Fictitious text scams with "smishing" schemes continue during this holiday season. Smishing is the practice of sending text messages allegedly from reputable companies to induce you to reveal personal information, such as passwords or credit card numbers.

We urge people to take extra care while shopping online or viewing emails and texts, especially during the holiday season when criminals are very active.

Stay safe while holiday shopping with the following considerations:

Shop at sites where the web address begins with "https" – the "s" is for secure communications and look for the "padlock" icon in the browser window.

- Don't shop on unsecured public Wi-Fi in places like a mall.
- Keep security software for computers, tablets and mobile phones updated.
- Protect the devices of family members, including young children, older adults as well as less technologically savvy users.
- Make sure anti-virus software for computers has a feature to stop malware, and that there is a firewall enabled that can prevent intrusions

Gift Card Scammers

Remember the IRS never asks for or accepts gift cards as payment for a tax bill.

Here is how the scam usually happens:

- The most common way scammers request gift cards is over the phone through a government impersonation scam. However, they will also request gift cards by sending a text message, email or through social media.
- A scammer posing as an IRS agent will call the taxpayer or leave a voicemail with a callback number informing the taxpayer that they are linked to some criminal activity. For example, the scammer will tell the taxpayer their identify has been stolen and used to open fake bank accounts.
- The scammer will threaten or harass the taxpayer by telling them that they must pay a fictitious tax penalty.
- The scammer instructs the taxpayer to buy gift cards from various stores.
- Once the taxpayer buys the gift cards, the scammer will ask the taxpayer to provide the gift card number and PIN.

Here's how you can tell if it's really the IRS calling. The IRS will never:

- Call to demand immediate payment using a specific payment method such as a gift card, prepaid debit card or wire transfer. Generally, the IRS will first mail a bill to any taxpayer who owes taxes.
- Demand that taxpayers pay taxes without the opportunity to question or appeal the amount they owe. All taxpayers should be aware of their rights.
- Threaten to bring in local police, immigration officers or other law enforcement to have the taxpayer arrested for not paying.
- Threaten to revoke the taxpayer's driver's license, business licenses or immigration status.

Any taxpayer who believes they've been targeted by a scammer should:

- Contact the Treasury Inspector General for Tax Administration to report a phone scam. Use their IRS Impersonation Scam Reporting webpage. They can also call 800-366-

4484.

- Report phone scams to the Federal Trade Commission. Use the FTC Complaint Assistant on FTC.gov. They should add "IRS phone scam" in the notes.
- Report threatening or harassing telephone calls claiming to be from the IRS to phishing@irs.gov. People should include "IRS phone scam" in the subject line.

Stay Safe This Holiday Season!