Tax Identity Theft Awareness Week

Tax Identity Theft Awareness Week is a campaign run by the Federal Trade Commission (FTC) from January 30 to February 3 to spread awareness of tax-related identity theft and IRS imposter scams. The FTC, IRS, Department of Veteran Affairs, and others are hosting various events throughout the week to educate the public on these threats.

In 2016, 34 percent of the identity theft complaints to the FTC involved taxes, employment, or wages. There was a 22 percent increase in the number of complaints regarding IRS imposters – scam callers threatening to arrest or fine victims unless they are paid immediately for taxes they claim the victims owe. The IRS will never call demanding immediate payment of taxes owed or a specific method of payment, such as a prepaid debit card, gift card, or wire transfer.

Here are the best ways to avoid tax identity theft:

- File your tax return as early as possible.
- Use a secure internet connection to file electronically, or mail your tax return directly at the post office.
- Never respond to emails, texts, or social media communications claiming to be from the IRS. The IRS will only contact you by mail. Report any suspicious or unsolicited emails claiming to be sent from the IRS to phishing@irs.gov.
- Never provide personal information to anyone purporting to be an IRS representative who contacts you via an unsolicited telephone call. Instead record the caller's name, badge number and a call back number. Hang up and then contact the IRS at 1-800-366-4484 to determine if the caller is an IRS employee with a legitimate need to contact you.
- Monitor your credit report to verify there is no unauthorized activity.
- Enroll in the IRS Identity Protection Pin (IP PIN) program to obtain a 6-digit pin.

Company payroll and human resources departments should remain vigilant in safeguarding employee tax records. Cybercriminals target HR and payroll departments using various social engineering schemes designed to trick them into believing upper management has made an urgent request for employee W-2 forms. Because these schemes are often very sophisticated and convincing, many targets act on the request quickly without taking additional steps to verify the source. Payroll and HR officials should be wary of any

requests for employee W-2 forms or Social Security numbers and security procedures should be implemented that require the written approval of multiple people before a request for personal information is fulfilled. Tax season has only just begun and the IRS is already receiving notifications about this email scam.

- IR-2016-107: Scammers are contacting college students or recent graduates, demanding payment for a supposed “Federal Student Tax.”
- IR-2016-123: Fraudulent CP2000 notices are sent by mail or email requesting payment for an “Affordable Care Act bill” and instructions to mail a check to the IRS.
- IR-2016-40: Scammers posing as IRS agents requesting taxpayers to verify details on their tax return. The scammer will attempt to obtain sensitive information such as Social Security and credit card numbers.

IR-2016-103: Tax professionals may receive emails supposedly from tax software companies requesting the individual to download and install an important software update via a link in the email. This link allows the cybercriminals to log the tax professional’s keystrokes in order to steal sensitive data.