CPA
Practice Advisor

Dec. 05, 2018

With the holiday shopping season in full swing, the Internal Revenue Service and Security Summit partners warn taxpayers to take extra steps to protect their tax and financial data from identity thieves.

The holidays offer cybercriminals a chance to steal financial account information, Social Security numbers, credit card information and other sensitive data to help them file a fraudulent tax return in 2019.

The Internal Revenue Service, state tax agencies and the tax community, partners in the Security Summit, are marking "National Tax Security Awareness Week" Dec. 3 -7, with a series of reminders to taxpayers and tax professionals. In part one, the topic is online shopping.

"With tax season quickly approaching, people should be extra careful during the holidays to protect their sensitive tax and financial data," said IRS Commissioner Chuck Rettig. "Taking a few simple steps can protect this valuable information and help prevent someone from stealing a tax refund. Taxpayers guarding their information also helps strengthen protections against identity thieves taken by the IRS, the states and the tax industry."

In part one of a weeklong series of tips, the Summit partners warn people shopping online or in public places to remember a few basic tips that can go a long way to protecting their identity and personal information. This is part of the Summit's "Taxes.Security.Together." campaign.

Cybercriminals seek to turn stolen data into quick cash, either by draining financial accounts, charging credit cards, creating new credit accounts or even using stolen identities to file a fraudulent tax return for a refund.

Here are seven steps to help with online safety and protecting tax returns and

on links from pop-up ads.

- *Learn to recognize and avoid phishing emails that pose as a trusted source such as those from financial institutions or the IRS.* The IRS has seen an increase in these schemes this year. These emails may suggest a password is expiring or an account update is needed. The criminal's goal is to entice users to open a link or attachment. The link may take users to a fake website that will steal usernames and passwords. An attachment may download malware that tracks keystrokes — putting personal information at risk.
- *Keep a clean machine.* This applies to all devices – computers, phones and tablets. Use security software to protect against malware that may steal data and viruses that may damage files. Set it to update automatically so that it always has the latest security defenses. Make sure firewalls and browser defenses are always active. Avoid "free" security scans or pop-up advertisements for security software.
- *Use passwords that are strong, long and unique.* Experts suggest a minimum of 10 characters but longer is better. Avoid using a specific word; longer phrases are better. Use a combination of letters, numbers and special characters. Use a different password for each account. Use a password manager, if necessary.
- *Use multi-factor authentication.* Some financial institutions, email providers and social media sites allow users to set accounts for multi-factor authentication. This means users may need a security code, usually sent as a text to a mobile phone, in addition to usernames and passwords.
- *Encrypt and password-protect sensitive data.* If keeping financial records, tax returns or any personally identifiable information on computers, this data should be encrypted and protected by a strong password. Also, back-up important data to an external source such as an external hard drive. And, when disposing of computers, mobile phones or tablets, make sure to wipe the hard drive of all information before trashing.

The IRS, state tax agencies and the tax industry are committed to working together to

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.