National Tax Security Awareness Week:
Eight Steps to Keep Online Data Safe

IRS Tax Tip 2017-82
November 27, 2017

During the holiday shopping season, shoppers are looking for the perfect gifts. At the same time, criminals are looking for sensitive data. This data includes credit card numbers, financial accounts and Social Security numbers. Cybercriminals can use this information to file a fraudulent tax return.

This tip is part of National Tax Security Awareness Week. The IRS is partnering with state tax agencies, the tax industry and groups across the country to remind people about the importance of data protection.

Anyone with an online presence can do a few simple things to protect their identity and personal information. Following these eight steps can also help taxpayers protect their tax return and refund in 2018:

- Shop at familiar online retailers. Generally, sites with an “s” in “https” at the start of the URL are secure. Users can also look for the “lock” icon in your browser’s URL bar. That said, some criminals may get a security certificate, so the “s” may not always mean a site is legitimate.

- Avoid unprotected Wi-Fi. Users should not do online financial transactions when using unprotected public Wi-Fi. Unprotected public Wi-Fi hotspots may allow thieves to view transactions.

- Learn to recognize and avoid phishing emails that pose as a trusted source. These emails can come from a source that looks like a legitimate bank or even the IRS. These emails may include a link that takes the user to a fake website. From there, the thieves can steal usernames and passwords.

- Keep a clean machine. This includes computers, phones and tablets. Users should install security software to protect against malware that may steal data. This software also protects against viruses that may damage files.

- Use passwords that are strong, long and unique. Experts suggest a minimum of 10 characters. Use a combination of letters, numbers and special characters. Use a different password for each account.

- Use multi-factor authentication when available. Some financial institutions, email providers and social media sites allow users to set their accounts for multi-factor authentication. This means users may need a security code, usually sent as a text to their mobile phone, in addition to a username and password.

- Sign up for account alerts. Some financial institutions will send email or text alerts to an account holder when there is a withdrawal or change to their accounts. Generally, people can check their account profile to see what added protections may be available.

- Encrypt sensitive data and protect it with a password. People who keep financial records, tax returns or any personal information on their computer should protect this data. Users should also back up important data to an external source. When disposing of a computer, mobile phone or tablet, people should make sure they wipe the hard drive of all information before trashing.

More Information:

Taxes. Security. Together
Protect Your Clients; Protect Yourself
Don’t Take the Bait