Seven Steps to Keep Your Tax Information Secure Online

During the online holiday shopping season, the Delaware Division of Revenue is joining with the IRS, other state tax agencies and the tax industry to mark “National Tax Security Awareness Week.” From November 27 through December 1, we’d like to remind people to be vigilant with their personal information. While you are shopping for gifts, criminals are shopping for credit card numbers, financial account information, Social Security numbers and other sensitive data that could help them file a fraudulent tax return.

Cyber criminals 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. Anyone who has an online presence should take a few simple steps that could go a long way to protecting their identity and personal information.

Here are seven steps to help with online safety and protecting tax returns and refunds in 2018:

- Shop at familiar online retailers. Generally, sites using the “s” designation in “https” at the start of the URL are secure. Look for the “lock” icon in the browser’s URL bar. But remember, even bad actors may obtain a security certificate so the “s” may not vouch for the site’s legitimacy.
- Avoid unprotected Wi-Fi. Beware of making purchases at unfamiliar sites or clicking on links from pop-up ads. Unprotected public Wi-Fi hotspots also may allow thieves to view transactions. Do not engage in online financial transactions if using unprotected public Wi-Fi.
- Learn to recognize and avoid phishing emails that pose

as a trusted source such as those from financial institutions or the IRS. 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 or an attachment may download malware that tracks keystrokes.

- 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. If you can’t remember all your passwords, use a password manager, which securely stores the passwords for you.
- Use multi-factor authentication. Some financial institutions, email providers and social media sites allow users to set accounts for multi-factor authentication, meaning users may need a security code, usually sent as a text to a mobile phone, in addition to usernames and passwords. For added protection, some financial institutions also will send email or text alerts when there is a withdrawal or change to the account. Generally, users can check account profiles at these locations to see what added protections may be available.
- 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. When disposing of computers, mobile phones or tablets, make sure to wipe the hard drive of all information before throwing it away.

There are also a few additional steps people can take a few times a year to make sure they have not become an identity theft victim. Receive a free credit report from each of the three major credit bureaus once a year. Check it to make sure there are no credit changes that don't look familiar. Create a "My Social Security" account online with the Social Security Administration which can be used to see how much income is attributed to your SSN annually. This can help determine if someone else is using your SSN for employment purposes.

The Division of Revenue, the IRS, and the tax industry are committed to working together to fight against tax-related identity theft and to protect taxpayers. Visit the "Taxes. Security. Together." awareness campaign, or review IRS Publication 4524, Security Awareness for Taxpayers for additional information.