Seven Tips to Protect Your Computer Online

The Internal Revenue Service, the states and the tax industry urge you to be safe online and remind you to take important steps to help protect yourself against identity theft.

Taxes. Security. Together. Working in partnership with you, we can make a difference.

Scammers, hackers and identity thieves are looking to steal your personal information – and your money. But there are simple steps you can take to help protect yourself, like keeping your computer software up-to-date and giving out your personal information only when you have a good reason.

We all have a role to play to protect your tax account. There are just a few easy and practical steps you can take to protect yourself as you conduct your personal business online.

Here are some best practices you can follow to protect your tax and financial information:

1. Understand and Use Security Software. Security software helps protect your computer against the digital threats which are prevalent online. Generally, your operating system will include security software or you can access free security software from well-known companies or Internet providers. Other options may have an annual licensing fee and offer more features. Essential tools include a firewall, virus/malware protection and file encryption if you keep sensitive financial/tax documents on your computer. Security suites often come with firewall, anti-virus and anti-spam, parental controls and privacy protection. File encryption to protect your saved documents may have to be purchased separately. Do not buy security software offered as an unexpected pop-up ad on your computer or email! It's likely from a scammer.

2. Allow Security Software to Update Automatically. Set your security software to update automatically. Malware – malicious software – evolves constantly and your security software suite is updated routinely to keep pace.

3. Look for the "S" for encrypted "https" websites. When shopping or banking online, always look to see that the site uses encryption to protect your information. Look for https at the beginning of the web address. The "s" is for secure. Unencrypted sites begin with an http address. Additionally, make sure the https carries through on all pages, not just the sign-on page.

4. Use Strong Passwords. Use passwords of at least 10 to 12 characters, mixing letters, numbers and special characters. Don't use your name, birthdate or common words. Don't use the same password for several accounts. Keep your password list in a secure place or use a password manager. Don't share your password with anyone. Calls, texts or emails pretending to be from legitimate companies or the IRS asking you to update your accounts or seeking personal financial information are generally scams.

5. Secure your wireless network. A wireless network sends a signal through the air that allows you to connect to the Internet. If your home or business wi-fi is unsecured it also allows any computer within range to access your wireless and steal information from your computer. Criminals also can use your wireless to send spam or commit crimes that would be traced back to your account. Always encrypt your wireless. Generally, you must turn on this feature and create a password.

6. Be cautious when using public wireless networks. Public wi-fi hotspots are convenient but often not secure. Tax or financial Information you send though websites or mobile apps may be accessed by someone else. If a public Wi-Fi hotspot does not require a password, it probably is not secure. If you are transmitting sensitive information, look for the "s" in https in the website address to ensure that the information will be secure.

7. Avoid phishing attempts. Never reply to emails, texts or pop-up messages asking for your personal, tax or financial information. One common trick by criminals is to impersonate a business such as your financial institution, tax software provider or the IRS, asking you to update your account and providing a link. Never click on links even if they seem to be from organizations you trust. Go directly to the organization's website. Legitimate businesses don't ask you to send sensitive information through unsecured channels.