Tax Topics

Be Smart About Security At Tax Time

(NAPSA)—Although the Internal Revenue Service (IRS) reports a 400 percent surge in phishing and malware incidents during the 2016 tax season, there are simple steps you can take to help protect yourself.

Here are nine hints that can help:

1. **Beware of IRS Impersonators.** Some crooks call taxpayers to say they must settle their "tax bill." These are fake calls and often demand payment on prepaid debit cards, gift cards or wire transfers. Also, students should know there's no "Federal Student Tax." If you get any unexpected calls, e-mails, letters or texts from someone claiming to be from the IRS, remember, the IRS never calls to demand immediate payment using a specific method nor will it threaten you with local law enforcement.

2. **Understand and Use Security Software.** Security software helps protect computers against digital threats online. Generally, the operating system will include security software or you can access free security software from well-known companies or Internet providers. Essential tools include a firewall, virus and malware protection, and file encryption. Don't buy security software offered as an unexpected pop-up ad on your computer or e-mail. It's likely from a scammer.

3. **Let Security Software Update Automatically.** Malware—malicious software—evolves constantly and your security software suite updates routinely to keep pace.

4. **Look for the "S."** When shopping or banking online, 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. Additionally, make sure the https carries through on all pages, not just the sign-on page.

5. **Use Strong Passwords.** Use passwords of eight or more characters, mixing letters, numbers and special characters. Don't use your name, birth date 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 passwords with anyone. Calls, texts or e-mails pretending to be from legitimate companies or the IRS asking to update accounts or seeking personal financial information are almost always scams.

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

You can save money and trouble if you follow professional advice and your own good sense when taking care of taxes.

7. **Be Cautious When Using Public Wireless Networks.** Public Wi-Fi hot spots are convenient but often not secure. Tax or financial information you send through websites or mobile apps may be accessed by someone else. If a public Wi-Fi hot spot doesn't require a password, it's probably not secure.

8. **Avoid E-mail Phishing Attempts.** Never reply to e-mails, texts or pop-up messages asking for 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. They ask for Social Security numbers and other personal information, which could be used to file false tax returns. The sites may also infect your computer. 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.

9. **Get Professional Advice.** To make sure you can take advantage of all allowable tax-deferred savings, tax credits and deductions without risk, consult with a licensed tax professional, such as an enrolled agent (EA). EAs are the only federally licensed tax professionals with unlimited rights of representation before the IRS. EAs abide by a code of ethics and must complete many hours of continuing education each year to ensure they are up-to-date on the constantly changing tax code. To find one nearby, visit the searchable "Find a tax expert" directory at www.EAtax.org.