INTERNAL REVENUE SERVICE

IRS News Release

Media Relations Office | Washington, D.C. | Media Contact: 202.317.4000

www.IRS.gov/newsroom | Public Contact: 800.829.1040

IRS, Security Summit Partners, Remind Taxpayers to Protect Themselves Online

IR-2016-158, Dec. 5, 2016

WASHINGTON –The Internal Revenue Service, the states and the tax industry today urged taxpayers to take steps to protect themselves online to help in the fight against identity theft.

Scammers, hackers and identity thieves are looking to steal taxpayers' personal information and ultimately their money. But, there are simple steps taxpayers can take to help protect themselves, like keeping computer software up-to-date and being cautious about giving out their personal information.

This is the first reminder to taxpayers during "National Tax Security Awareness Week," which runs through Friday. This week, the IRS, the states and the tax community are joining together to send out a series of reminders to taxpayers and tax professionals as a part of the ongoing Security Summit effort.

Here are some best practices taxpayers can follow to protect their tax and financial information:

- **Understand and Use Security Software.** Security software helps protect computers against the digital threats that are prevalent 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/malware protection and file encryption if you keep sensitive financial/tax documents on your computer. Do not buy security software offered as an unexpected pop-up ad on your computer or email. It's likely from a scammer.
- **Allow Security Software to Update Automatically.** Set security software to update automatically. Malware – malicious software – evolves constantly, and your security software suite updated routinely to keep pace.
- **Look for the "S."** 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.
- **Use Strong Passwords.** Use passwords of eight or more 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 passwords with anyone. Calls, texts or emails pretending to be from legitimate companies or the IRS asking to update accounts or seeking personal financial information are almost always scams.
- **Secure Wireless Networks.** A wireless network sends a signal through the air that allows it

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 potentially 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.

- **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. Remember, if you are transmitting sensitive information, look for the “s” in https in the website address to ensure that the information will be secure.
- **Avoid E-mail 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.

To learn additional steps you can take to protect your personal and financial data, visit Taxes. Security. Together. Also, read Publication 4524, Security Awareness for Taxpayers.

Each and every taxpayer has a set of fundamental rights they should be aware of when dealing with the IRS. These are your Taxpayer Bill of Rights. Explore your rights and our obligations to protect them on IRS.gov.

Additional IRS Resources:

IRS Tax Tip: IRS, Partners Urge Strong Passwords Help Protect Identities at Tax Time and Beyond

IRS YouTube Videos:

- Security Summit: Be Cautious When Using Wi-Fi – English
- Security Summit: Update Your Password Regularly – English
- Phishing- Malware - English | Spanish | ASL