ADV 2019-15
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
JULY 17, 2019

Tax professionals urged to deploy 'Security Six' for basic protection

Security Summit asks tax preparers to take key steps to protect data from criminals

PROVIDENCE — The Rhode Island Division of Taxation, the Internal Revenue Service, and other members of the Security Summit urge tax preparers and other tax professionals to use six security steps to help ensure that they are fully protecting their computers and email. The steps will also help safeguard sensitive taxpayer data.

The steps – known as the "Security Six" – will also help keep sensitive taxpayer data from falling into the hands of international criminal syndicates that stalk the internet.

"These six steps are simple actions that anyone can take," said IRS Commissioner Chuck Rettig. "The important thing to remember is that every tax professional, whether a sole practitioner or a partner in a large firm, is a potential target for cybercriminals. No tax business should assume they are too small or too smart to avoid identity thieves."

Although the Security Summit is making major progress against tax-related identity theft, cybercriminals continue to evolve, and data thefts at tax professionals' offices continue, said Rhode Island Tax Administrator Neena Savage. Thieves use stolen data from tax practitioners to create fraudulent returns that are harder to detect, she said.

The Security Summit partnership urges tax professionals across the nation to bear in mind the following basic steps to help in the battle against identity theft.

The 'Security Six'

The following are the basic protections that everyone, especially tax professionals handling sensitive data, should deploy:

1. ANTI-VIRUS SOFTWARE

Although details may vary between commercial products, anti-virus software scans computer files or memory for certain patterns that may indicate the presence of malicious software (also called malware).

Anti-virus software (sometimes more broadly referred to as anti-malware software) looks for patterns based on the signatures or definitions of known malware from cyber criminals. Anti-virus vendors find new issues and update malware daily, so it is important that people have the latest updates installed on their computer, according to the U.S. Computer Emergency Readiness Team (US-CERT), a

division of the Department of Homeland Security. Once users have installed an anti-virus package, they should scan their entire computer periodically by doing:

- **Automatic scans –** Most anti-virus software can be configured to automatically scan specific files or directories in real time and prompt users at set intervals to perform complete scans.

- **Manual scans** – If the anti-virus software does not automatically scan new files, users should manually scan files and media received from an outside source before opening them. This manual process includes:
    - Saving and scanning email attachments or web downloads rather than opening them directly from the source.
    - Scanning portable media, including CDs and DVDs, for malware before opening files.

Sometimes the software will produce a dialog box with an alert that it has found malware and asks whether users want it to "clean" the file (to remove the malware). In other cases, the software may attempt to remove the malware without asking first.

When selecting an anti-virus package, users should learn about its features, so they know what to expect. Keep security software set to automatically receive the latest updates so that it is always current.

A reminder about spyware, a category of malware intended to steal sensitive data and passwords without the user's knowledge: Strong security software should protect against spyware. But remember: Never click links within pop-up windows, never download "free" software from a pop-up, and never follow email links that offer anti-spyware software. The links and pop-ups may be installing the spyware they claim to be eliminating.

A reminder about phishing emails: A strong security package also should contain anti-phishing capabilities. Never open an email from a suspicious source, click on a link in a suspicious email, or open an attachment – or else you could be a victim of a phishing attack and your data and your clients' data could be compromised.

2. FIREWALLS

Firewalls provide protection against outside attackers by shielding your computer or network from malicious or unnecessary web traffic and preventing malicious software from accessing your systems. Firewalls can be configured to block data from certain suspicious locations or applications while allowing relevant and necessary data through, according to US-CERT.

Firewalls may be broadly categorized as hardware or software. While both have their advantages and disadvantages, the decision to use a firewall is far more important than deciding which type you use:

- **Hardware** – Typically called network firewalls, these external devices are positioned between a computer and the internet (or another network connection). Hardware-based firewalls are particularly useful for protecting multiple computers and control the network activity that attempts to pass through them.

- **Software** – Most operating systems include a built-in firewall feature that should be enabled for added protection even if using an external firewall. Firewall software can also be obtained as separate software from a local computer store, software vendor, or ISP. If downloading

firewall software from the internet, make sure it is from a reputable source (such as an established software vendor or service provider) and offered via a secure website.

While properly configured firewalls may be effective at blocking some cyber-attacks, don't be lulled into a false sense of security. Firewalls do not guarantee that a computer will not be attacked. Firewalls primarily help protect against malicious traffic, not against malicious programs (malware), and may not protect the device if the user accidentally installs malware.

However, using a firewall in conjunction with other protective measures (such as anti-virus software and safe computing practices) will strengthen resistance to attacks.

The Security Summit reminds tax pros that anti-virus software and firewalls cannot protect data if computer users fall for email phishing scams and divulge sensitive data, such as usernames and passwords. The Summit reminds the tax community that users, not the software, is the first-line of defense in protecting taxpayer data.

About the Security Summit

The Security Summit consists of the IRS, state tax agencies, and the tax community -- including tax preparation firms, software developers, processors of payroll and tax financial products, tax professional organizations, and financial institutions.

Partners in the Security Summit work together to combat identity theft and fight other scams to protect the nation's taxpayers.

3. TWO-FACTOR AUTHENTICATION

Many email providers now offer customers two-factor authentication protections to access email accounts. Tax professionals should always use this option to prevent their accounts from being taken over by cybercriminals and putting their clients and colleagues at risk.

Two-factor authentication helps by adding an extra layer of protection beyond a password. Often two-factor authentication means the returning user must enter credentials (username and password) plus another step, such as entering a security code sent via text to a mobile phone. The idea is that a thief may be able to steal the username and password but it's highly unlikely they also would have a user's mobile phone to receive a security code and complete the process.

The use of two-factor authentication and even three-factor authentication is on the rise, and tax preparers should always opt for a multi-factor authentication protection when it is offered, whether on an email account or tax software account or any password-protected product. IRS Secure Access, which protects IRS.gov tools including e-Services, is an example of two-factor authentication. Tax pros can check their email account settings to see if the email provider offers two-factor protections.

4. BACKUP SOFTWARE/SERVICES

Critical files on computers should routinely be backed up to external sources. This means a copy of the file is made and stored either online as part of a cloud storage service or similar product. Or, a copy of the file is made to an external disk, such as an external hard drive that now comes with multiple terabytes of storage capacity. Tax professionals should ensure that taxpayer data that is backed up also is encrypted – for the safety of the taxpayer and the tax pro.

5. DRIVE ENCRYPTION

Given the sensitive client data maintained on tax practitioners' computers, users should consider drive encryption software for full-disk encryption. Drive encryption, or disk encryption, transforms data on the computer into files that cannot be read by an unauthorized person accessing the computer to obtain data. Drive encryption may come as a stand-alone security software product. It may also include encryption for removable media, such as a thumb drive and its data.

6. VIRTUAL PRIVATE NETWORK

If a tax firm's employees must occasionally connect to unknown networks or work from home, establish an encrypted Virtual Private Networks (VPN) to allow for a more secure connection. A VPN provides a secure, encrypted tunnel to transmit data between a remote user via the Internet and the company network. Search for "Best VPNs" to find a legitimate vendor; major technology sites often provide lists of top services.

How to get started with the 'Security Six'

All tax professionals also should review their professional insurance policy to ensure the business is protected should a data theft occur. Some insurance companies will provide cybersecurity experts for their clients. These experts can help with technology safeguards and offer more advanced recommendations. Also, having the proper insurance coverage is a common recommendation from tax professionals who have experienced data thefts.

➢ **ADDITIONAL RESOURCES:** Tax professionals also can get help with security recommendations by reviewing the recently revised IRS Publication 4557, Safeguarding Taxpayer Data (PDF), and Small Business Information Security: the Fundamentals (PDF) by the National Institute of Standards and Technology. Publication 5293, Data Security Resource Guide for Tax Professionals (PDF), provides a compilation data theft information available on IRS.gov.

The Rhode Island Division of Taxation office is at One Capitol Hill in Providence, R.I., diagonally across from the Smith Street entrance of the State House, and is open to the public 8:30 a.m. to 3:30 p.m. business days. To learn more, see the agency's website: www.tax.ri.gov.