ADV 2018-28
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
JULY 17, 2018

Tax professionals urged to safeguard computers and email

Security Summit partners outline steps to take to shield sensitive taxpayer data from ID thieves

PROVIDENCE, R.I. – The Internal Revenue Service, the Rhode Island Division of Taxation, and other partners in the Security Summit today outlined critical steps for tax professionals to take to protect their computers and email as well as safeguard sensitive taxpayer data.

The "Security Six" protections fall into several major security categories. The Security Summit partnership urges tax professionals across the nation to avoid overlooking these basic security details as identity thieves increasingly target practitioners in search of valuable taxpayer data.

There is a dizzying array of cyber threats that confront tax professionals and many others. It's not easy to keep up with all the viruses, worms, Trojan horses, bots, or even the terminology. That's why it's essential that all tax professionals deploy strong security software that will do the job for you.

The IRS, the Rhode Island Division of Taxation, and the private-sector tax industry – known as the Security Summit – are trying to help tax professionals decipher the confusing world of security software that is key to safeguarding taxpayer data stored on practitioner's computer networks.

Although the Security Summit is making progress against tax-related identity theft, cybercriminals continue to evolve, and data thefts at tax professionals' offices is on the rise. Thieves use stolen data from tax practitioners to create fraudulent returns that are harder to detect.

Following are the "Security Six"" – the must-have tools to secure taxpayer data on your computers. All tax professionals, whether part of a large firm or a one-person shop, must enact security safeguards. Many of these steps are a good idea not just for tax professionals but for any taxpayer or small business:

Antivirus Software

Although details may vary between packages, anti-virus software scans files or your computer's memory for certain patterns that may indicate the presence of malicious software (i.e., 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.

Anti-virus vendors find new and updated malware daily, so it is important that you have the latest updates installed on your computer, according to the U.S. Computer Emergency Readiness Team (US-CERT), a division of the Department of Homeland Security.

Once you have installed an anti-virus package, you should scan your entire computer periodically:

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

- MANUAL SCANS – If your anti-virus software does not automatically scan new files, you should manually scan files and media you receive from an outside source before opening them. This 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 alerting you that it has found malware and ask whether you want it to "clean" the file (to remove the malware).

In other cases, the software may attempt to remove the malware without asking you first. When you select an anti-virus package, familiarize yourself with its features so you know what to expect. Keep your security software set to automatically receive the latest updates so that it is always current.

This is the second in a series of Security Summit announcements called "Protect Your Clients; Protect Yourself: Tax Security 101."

The Security Summit awareness campaign is intended to provide tax professionals with the basic information they need to better protect taxpayer data and to help prevent the filing of fraudulent tax returns.

✓ *A reminder about spyware*: Strong security software should protect against spyware. But remember, never clink 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*: A strong security package also should contain anti-phishing capabilities, but your email provider and your browser provider also should include anti-phishing protections. Never open an email from a suspicious source, clink on a link in a suspicious email, or open an attachment – or you could be a victim of a phishing attack.

Firewalls

Firewalls provide protection against outside attackers by shielding your computer or network from malicious or unnecessary network traffic and preventing malicious software from accessing the network. Firewalls can be configured to block data from certain 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 your computer and the Internet (or other network connection). Many vendors and some Internet service providers (ISPs) offer integrated small office / home office (SOHO) routers that also include firewall features. Hardware-based firewalls are particularly useful for protecting multiple computers and control the network activity that attempts to pass through them. The advantage of hardware-based firewalls is that they are separate devices running their own operating systems, so they provide an additional line of defense against attacks when compared to system or host-level protections.

- SOFTWARE – Most operating systems include a built-in firewall feature that should be enabled for added protection even if you have an external firewall. Firewall software can also be obtained as separate software from your local computer store, software vendor, or ISP. If you download firewall software from the Internet, make sure it is from a reputable source (i.e., an established software vendor or service provider) and offered via a secure site.

While properly configured firewalls may be effective at blocking some attacks, don't be lulled into a false sense of security. Firewalls do not guarantee that your computer will not be attacked. Firewalls primarily help protect against malicious traffic, not against malicious programs (malware), and may not protect you if you accidentally install malware on your computer. However, using a firewall in conjunction with other protective measures (such as anti-virus software and safe computing practices) will strengthen your 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. You, not the software, are the first line of defense in protecting taxpayer data.

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. 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 your username and password, but it's highly unlikely that the thief also would have your 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. Check your email account settings to see if your email provider offers two-factor protections.

Backup Software/Services

Critical files on your 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. Tax professionals should ensure that taxpayer data that is backed up also is encrypted.

Drive Encryption

Given the sensitive client data maintained on tax practitioners' computers, you should consider drive encryption software for full-disk encryption. Drive encryption, or disk encryption, transforms data on the computer into unreadable files for the unauthorized person accessing the computer. 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.

Data Security Plan

The Security Summit also reminds tax professionals of several other important steps. All professional tax return preparers must have a written data security plan as required by the Federal Trade Commission and its Safeguards Rule. You also can get help with security recommendations and creating a data security plan by reviewing the recently revised IRS Publication 4557, "Safeguarding Taxpayer Data", and "Small Business Information Security: the Fundamentals" by the National Institute of Standards and Technology.

Publication 5293, "Data Security Resource Guide for Tax Professionals", 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 Division's website: www.tax.ri.gov.