ADV 2018-30
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
JULY 30, 2018

Tax professionals urged to strengthen passwords

Security Summit also recommends encryption to protect sensitive data, combat cyberthieves

PROVIDENCE, R.I. – The Rhode Island Division of Taxation, the Internal Revenue Service, and other partners in the Security Summit are urging all tax professionals to use strong passwords to protect accounts from cyberthieves. Tax professionals also should consider encryption for all sensitive data.

Strong password and encryption protocols should be standard features of any data security plan that must be created by all professional tax return preparers.

The Electronic Tax Administration Advisory Committee noted in its recent annual report to Congress that many tax pros do not have data security plans that are required by the Federal Trade Commission.

The IRS, the Rhode Island Division of Taxation, other states' tax agencies, and the tax industry are working together as the Security Summit to fight against tax-related identity theft and to protect business and individual taxpayers from cybercriminals.

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.

In recent months, cybersecurity experts' recommendations on what constitutes a strong password has changed. They now suggest that people use word phrases that are easy to remember rather than random letters, characters and numbers that cannot be easily recalled.

For example, experts use to suggest something like "PXro#)30" but now suggest a phrase like "SomethingYouCanRemember@30." By using a phrase, you don't have to write down your password and expose it to more risk. Also, people may be more willing to use strong, longer passwords if it's a phrase rather than random characters.

Strengthen passwords

It is critical that all tax practitioners establish strong, unique passwords for all accounts, whether it's to access a device, tax software products, cloud storage, wireless networks, or encryption technology.

Here's how to get started:

- Use a minimum of eight characters; longer is better.
- Use a combination of letters, numbers and symbols, i.e., XYZ, 567, !@#.
- Avoid personal information or common passwords; opt for phrases.
- Change default/temporary passwords that come with accounts or devices.
- Do not reuse passwords, e.g., changing Bgood!17 to Bgood!18 is not good enough; use unique usernames and passwords for accounts and devices.
- Do not use email addresses as usernames, if that is an option.
- Store any password list in a secure location, such as a safe or locked file cabinet.
- Do not disclose passwords to anyone for any reason.
- Use a password manager program to track passwords but protect it with a strong password.

Multi-factor identification

Whenever it is an option for a password-protected account, users also should opt for a multi-factor authentication process. 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.

This is the third 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.

The idea is a thief may be able to steal your username and password, but it's highly unlikely they also would have your mobile phone to receive a security code and complete the process. Some providers of tax software products for tax professionals offer two-factor or even three-factor authentication. Tax practitioners should use the most secure option available, not only for tax software, but other products such as email accounts and storage provider accounts. Those hosting their own website should also consider some other form of multi-factor authentication to further increase login security.

Password-protected data encryption is also critical to protecting client information. Cybercriminals work hard through various tactics to penetrate networks or trick users into disclosing passwords. They may steal the data, hold the data for ransom or use tax professionals' computers to complete and file fraudulent tax returns.

Basic steps for encrypting client data

Here are a few basic steps about encryption and protecting client data stored on computer systems:

- Use drive encryption to lock all files on computers and on all devices. Drive or disk encryption often is a stand-alone software product. It converts text on files into an unreadable format for anyone who makes an unauthorized access. Entering the password unlocks the files for legitimate users.
- Backup encrypted copies of client data to external hard drives (USBs, CDs, DVDs) or use cloud storage. If using external drives, keep them in a secure location. If choosing cloud storage, encrypt the data before uploading to the cloud.
- Avoid attaching USB drives and external drives with client data to public computers.
- Avoid installing unnecessary software or applications to the business network; avoid offers for "free" software, especially security software, which is often a ruse by criminals; download software or applications only from official sites.

- Perform an inventory of devices where clients' tax data are stored, i.e., laptops, smart phones, tablets, external hard drives, etc.; inventory software used to process or send tax data, i.e., operating systems, browsers, applications, tax software, web sites, etc.
- Limit or disable internet access capabilities for devices that have stored taxpayer data.
- Delete all information from devices, hard drives, USBs (flash drives), printers, tablets or phones before disposing of devices; some security software includes a "shredder" that electronically destroys stored files.
- Physically destroy hard drives, tapes, USBs, CDs, tablets or phones by crushing, shredding or burning; shred or burn all documents containing taxpayer information before throwing away.

In addition to these steps, the Security Summit reminds all professional tax preparers to have a written data security plan as required by the Federal Trade Commission and its Safeguards Rule. Tax professionals can get help with security recommendations 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. See also: Protect Your Clients; Protect Yourself: Tax Security 101.

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.