CYBER SECURITY

FOR TAX PROFESSIONALS

BY MARSHALL J. HEAP, EA

In the "Capitol Corner" column of the January/February 2017 *EA Journal*, Robert Kerr acknowledged that enrolled agents "did not become enrolled agents because of a deep and abiding passion for information technology, firewall construction, and/or secure remote access." Kerr, however, added a warning to tax practitioners not to delude themselves: "The bad guys are out there, and they are after information that modestly sized practices hold."

This is good advice, because tax practitioners' responsibilities to their clients include safeguarding their confidential data, both in paper and digital form. It is wise to become familiar with applicable digital data privacy rules, regulations, and best practices and be aware of the popular Internet scams currently targeting tax practitioners. Additionally, there are measures tax practitioners can take for safely storing and communicating digital client data as well as rules and actions to follow in the event of a data breach.

CYBER SECURITY

Data Privacy Rules and Regulations

Oddly, Circular 230 (Regulations Governing Practice before the Internal Revenue Service), contains no specific rules for safeguarding taxpayers' personal data. Instead, this requirement is stated in IRC Sec. 7216, which says that tax return preparers who knowingly or recklessly disclose or use tax return information can be sanctioned. Treas. Reg. Sec. 301.7216-1(b)(5) states that "the term disclosure means the act of making tax return information known to any person in any manner whatever. To the extent that a taxpayer's use of a hyperlink results in the transmission of tax return information, this transmission of tax return information is a disclosure by the tax return preparer subject to penalty under Section 7216 if not authorized by regulation [emphasis added]." Treas. Reg. Sec. 301.7216-1(b)(6) defines a hyperlink as "a device used to transfer an individual using tax preparation software from a tax return preparer's webpage to a webpage operated by another person without the individual having to separately enter the web address of the destination page."

Tax preparers are permitted to use tax return information only for preparing federal and state tax returns and declaring estimated tax.[1] Any other disclosure or use of this information requires the client's consent[2] and must be in the format specified by Rev. Proc. 2013-14. However, there are two important exceptions to this rule:

1. required disclosures to the IRS governed by Circular 230, Sec. 10.20(a) and
2. Treas. Reg. Sec. 301.7216-2(b) or to a court pursuant to IRC Sec. 7216(b).

Offenders who engage in unauthorized disclosure or use of tax return information may face a fine of up to $1,000 and/or imprisonment of up to one year.

Official Recommendations and Standards for Digital Data Security

The Gramm-Leach-Bliley Act[3] (GLBA) includes the "safeguards rule," which provides detailed recommendations for securely storing confidential client information, whether in paper or digital form, including the recommendation that digital client information be held in encrypted files.[4] Thus, digital client data is protected both in case of theft of the device and when connected to unsecured networks.

Since the passage of the GLBA in 1999, there have been significant advances in data encryption, including the commonplace usage of virtual private networks (VPNs), which will be discussed later. Because encryption is such a processor-intensive task, these advances have been facilitated by marked improvements in computer processor speeds in the last two decades.

In IRS Publication 1345 (Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns) the IRS promulgates data safety standards that supplement the GLBA—for example, the use of AES-128-bit as a minimum encryption standard for electronic transmission of tax return data, which will also be discussed later. This is a minimum standard, so encryption keys can exceed this, for example AES-256 bit. In fact, data security is directly correlated to length of encryption key used—the longer it is the more difficult it is to decrypt the data.

The Security Summit Initiative,[5] a partnership of the IRS, state tax agencies, and the private-sector tax industry, was formed to combat cybercrime. In November 2015, Security Summit participants announced new standards for logging on to all tax software products, including minimum password requirements, new security questions, and standard lockout features.[6] Tax software providers, such as Intuit ProSeries and Drake Software, have instituted these features for 2016 tax products.

Unfortunately, while protecting the "front door," this initiative does not prevent "backdoor" access to client tax files stored on a tax practitioner's computer. For example, Intuit ProSeries stores client data files in a subdirectory entitled "YYData" ("YY" is the last two digits of the year). A cybercriminal can steal these files and possibly import them into his or her own copy of ProSeries.

Current Cyber Scams of Concern to Tax Professionals

Two current scams attempting to steal taxpayer identity information start with an e-mail claiming to be from the practitioner's tax preparation software provider.

The first scheme exploits the fact that tax preparation software is frequently updated and advises the recipient to download and install an alleged "important software update" using a hyperlink provided in the e-mail.[7] After clicking on the embedded hyperlink, the recipient is directed to a website prompting them to download a file that is supposed to be an update of their software. The file name uses the actual name of their software followed by an ".exe" extension. In reality, the link causes the tax practitioner to download a program designed to track his or her key strokes. This common technique is used to steal log-in information, passwords, and other sensitive data.

The second scam[8] involves an e-mail with the subject line "Access Locked" and informs the tax practitioner that access to his or her tax prep software account has been "suspended due to errors in your security details." The scam asks the recipient to resolve the issue by using an "unlock" hyperlink provided in the e-mail. Clicking the hyperlink takes the recipient to a bogus website where they are asked to log in with their user name and password. Instead of unlocking

his or her account, the tax professional has inadvertently handed his or her log-in details to cybercriminals, who then can access the preparers' tax return software accounts and potentially steal client information.

Ransomware is particularly concerning to tax professionals and their clients. A spam campaign first reported in late 2015[9] involves an e-mail that claims to be a refund notification from the IRS. Attached to the e-mail is a zip file that, when opened, infects the host computer with malware. Data is harvested from the host computer before the hard drive and any connected drives are encrypted. The victim is then instructed to pay a ransom in bitcoins to regain access to his or her data.

Signing up for IRS e-mail practitioner alerts (www.irs.gov/uac/join-e-news-for-tax-professionals) is a good way to stay abreast of IRS news, including information on the latest cyber scams.

Safely Storing Client Data on a Computer

The first step in safeguarding digital data is ensuring that your computer is password-protected. Ideally, passwords should consists of seemingly random characters and be as long as possible. This makes passwords difficult to break. However, this is only a first line of protection, because an awake, unattended computer is nevertheless vulnerable.

The next line of defense is to further protect clients' sensitive information stored on the computer through encryption. Encrypting each file would be troublesome, so a better solution is to encrypt a directory or volume on the computer.

Some operating systems support directory/file encryption directly (e.g., Microsoft Windows 10 Pro). An alternative is to encrypt a user-specified computer volume. Microsoft Windows users are accustomed to working on the C: drive. Free, easy-to-use software for encrypting a volume on a computer, such as VeraCrypt, is available on the Internet. These software applications create an encrypted volume on the computer with a user-specified size and drive letter (e.g., a 10Gb Z: drive). Then, it is easy for the user to cut and paste files containing tax return and other sensitive client data to the encrypted volume using a file utility such as Windows Explorer.

It is recommended that the encrypted volume's capacity be several gigabytes so that tax preparation software can also be installed there. Thus, client files generated by tax preparation software are also protected from "back-door" access from increasingly savvy cybercriminals.

Access to the encrypted volume is password-protected. Again, the password should ideally consist of 20 or more seemingly random characters. When access to the encrypted volume is not needed, the user should dismount the volume (render it inaccessible), which is a one-click operation.

Interestingly, VeraCrypt uses AES-256-bit encryption, which is an NSA standard for "top secret" classified data.[10] The AES-128-bit minimum e-file data standard promulgated by the IRS eight years ago[11] is rapidly becoming dated as computer processors become more powerful and better able to decrypt such data.

The first step in safeguarding digital data is ensuring that your computer is password-protected.

Safe Internet Access and Client Communications

These days, anyone accessing the Internet should ensure that his or her computer is protected by a firewall and antivirus software that are regularly updated. Even when taking these precautions, there are some digital communication situations in which tax professionals need to be particularly careful—namely, unsecured public Wi-Fi networks and digital communications from and to clients.

Unsecured Public Wi-Fi Networks

When accessing a public Wi-Fi network, not only should the computer be protected by a firewall and antivirus software, but file sharing and public-folder sharing should be turned off. And even then, data can be intercepted using a "man-in-the-middle"[12] attack (typically an eavesdropper who manipulates communications between two parties). Using a VPN keeps digital communications safe by encrypting traffic between the computer and the VPN server that connects to the Internet. This makes it very difficult for would-be intruders to access data. There are many VPN software applications available, and they are generally easy to install. CNET's article "Staying Safe on Public Wi-Fi" (https://www.cnet.com/how-to/tips-to-stay-safe-on-public-wi-fi/) provides information on safely connecting to the Internet using public Wi-Fi connections.

Receiving Digital Data from Clients

Clients commonly provide digital data to their tax practitioners using e-mail attachments or cloud-based data storage websites such as DropBox. The obvious advice here is to scan these files with antivirus software before opening them so that the antivirus software can neutralize any viruses it detects.

USB sticks are particularly dangerous virus-delivery devices. The Spora worm[13] is ransomware that is known to use USB sticks as an infection vector. Simply scanning the

USB stick with antivirus software may be insufficient, because malware can propagate as soon as the USB stick is plugged in. A better solution is to politely ask the client to use e-mail, cloud-based data sharing, or a client portal (detailed below).

A good solution for safely transmitting sensitive data by e-mail is to place this data in an encrypted e-mail attachment.

Sending Digital Data to Clients

Most tax practitioners prepare tax returns using commercial proprietary software, and many of these software providers now offer client portals to practitioners. These portals allow safe delivery of digital documents to and from clients. For example, Lacerte and Proseries both partner with SmartVault,[14] a client portal offering AES-256-bit encryption. However, practitioners who prefer not to delegate their data security to a cloud-based provider can create and locally store their own private encryption keys. Viivo (a PKWARE product) allows the user to take complete control of file encryption and works with most popular cloud-based data storage providers (again by using the AES-256-bit encryption standard).[15]

The e-mail phishing scams discussed earlier trap the unwary by using hyperlinks from supposedly legitimate sources. To be on the safe side, it is best not to click on e-mail-embedded hyperlinks as a matter of policy. The hyperlinks discussed earlier illustrate just how much responsibility tax return preparers statutorily assume for computer-stored client information.

Many tax practitioners frequently communicate with their clients by e-mail, which may be stored through their route by a chain of computers before reaching the recipient. When intercepted, unencrypted e-mails are easily read. E-mail accounts have been frequent targets of hackers too. Consequently, practitioners should avoid openly including sensitive personal data in e-mail communications.

A good solution for safely transmitting sensitive data by e-mail is to place this data in an encrypted e-mail attachment. The access password should be as strong as possible and could be based on information known to the practitioner and client (for example, social security numbers, dates of birth, address information, tax return information, or some combination of this data). Alternatively, the practitioner and client can arrange to physically meet in a secure location to communicate passwords.

Tax practitioners looking for more information on protecting themselves and their client data can refer to www.irs.gov/individuals/protect-your-clients-protect-yourself.

Responding to a Data Breach

Neither Circular 230 nor IRC Sec. 7216 and the associated Treasury regulations mention how a tax professional should respond to inadvertent unauthorized data disclosure. Should affected clients be advised of the breach? Ultimately, this is up to the tax professional and his or her liability insurer. Client engagement letters and any relevant data privacy policy documents should be consulted to determine whether the tax professional has any legal and contractual obligations. When appropriate, affected clients should be urged to ask major credit bureaus to put fraud alerts on their accounts. Tax professionals should also consider reporting the matter to law enforcement. A useful IRS resource in this situation is https://www.irs.gov/uac/newsroom/tax-return-preparers-data-thefts-and-protecting-client-tax-information.

Summary

Tax professionals who have an adequate data privacy policy in place will be able to distinguish themselves from the more languid. Explaining to clients the measures the tax professional has taken to safeguard financial and personal data can only increase clients' trust.

To reiterate, here are the key ingredients of a sound data privacy policy:

- Use strong passwords (the longer and more random, the better).
- Use good antivirus software and a firewall.
- Disable file and public folder sharing when using public Wi-Fi.
- Connect to unsecured networks with a VPN.
- Store client files in secure folders/volumes.
- Employ strong encryption (e.g., AES-256-bit).
- Scan incoming digital data for viruses and avoid using client-provided USB sticks.
- Communicate client data via safe client portals or encrypted e-mail attachments.

Acknowledgment

The author wishes to thank Carolyn J. Schimpler, CPA (assistant director, tax materials and managing editor, University of

Illinois Tax School) for her helpful suggestions and editing.

Disclaimer

The author has no relationship with any of the organizations mentioned in this article. Readers use the mentioned software applications at their own risk. **EA**

About the Author

Marshall J. Heap EA, is a tax content development and instruction specialist at the University of Illinois Tax School (www.TaxSchool.Illinois.edu). An EA since 1984, Marshall is an ex-senior manager of PwC and has seven years' recent experience as an approved IRS continuing education provider. Marshall's academic background is in computing and associated fields with degrees from the following UK universities: The Open University (BSc), London, Birkbeck College (MSc), and Reading (PhD).

ENDNOTES

1. IRC §7216.
2. Treas. Reg. §301.7216-3.
3. The Gramm-Leach-Bliley Act (GLBA) is also known as the Financial Services Modernization Act of 1999, Public Law 106–102, 113 Stat. 1338. (Nov. 12, 1999).
4. *Financial Institutions and Customer Information: Complying with the Safeguards Rule*. FTC. 2006. [https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying] Accessed on Apr 03, 2017.
5. *Security Summit*. Feb. 21, 2017. IRS. [https://www.irs.gov/uac/security-summit] Accessed on Apr 03, 2017.
6. IR-2015-129 (Nov. 19, 2015).
7. IR-2016-103 (Aug. 11, 2016).
8. IR-2017-39 (Feb. 17, 2017).
9. *Security Alert: Fileless Kovter Teams Up with Modular CoreBot Malware in IRS Spam Campaign*. Zaharia, Andra. Dec. 21, 2015. Heimdal Security. [https://heimdalsecurity.com/blog/security-alert-fileless-kovter-teams-modular-corebot-malware-irs-spam-campaign/] Accessed on Apr 03, 2017.
10. *Key Size*. Ed. Wikipedia Contributors. Jan. 02, 2017. Wikipedia, The Free Encyclopedia. [https://en.wikipedia.org/wiki/Key_size] Accessed on Apr. 03, 2017.
11. IRS Announcement 2009-56, IRB 2009-28 (Jul. 13, 2009).
12. *Man-in-the-middle attack*. Ed. Wikipedia Contributors. March 16, 2017. Wikipedia, The Free Encyclopedia. [https://en.wikipedia.org/w/index.php?title=Man-in-the-middle_attack&oldid=770676213] Accessed on Apr. 03, 2017.
13. *[ALERT] USB Sticks Could Infect Your Network With New Spora Ransomware Worm*. Sjouwerman, Stu. Jan. 22, 2017. KnowBe4. [https://blog.knowbe4.com/alert-usb-sticks-could-infect-your-network-with-new-spora-ransomware-worm] Accessed on Apr. 03, 2017.
14. *Effortless Document Collection For CPAs, Accountants, and Tax Pros*. SmartVault Corporation. [http://www.smartvault.com/integration/filethis/] Accessed on Apr. 03, 2017.
15. *How Our Security Works*. 2016. PKWARE Inc. [https://viivo.com/how-our-security-works] Accessed on Apr. 03, 2017.