their clients from the risks that are lurking in their own offices?

Dave DuVal • Mar. 15, 2019

Many tax practitioners are familiar with how to assist their clients who have been a victim of tax identity theft, but how many tax professionals know how to safeguard their clients from the risks that are lurking in their own offices? No tax professional wants to be the common denominator when clients begin calling to look for advice on what to do when their identity has been stolen.

It is not only the theft of client data that tax professionals need to be wary of; it is the vulnerability of employee files and their own tax credentials such as our PTIN and EFIN numbers. Many tax professionals have lulled themselves into a false sense of security that they are too small to be hacked. After all, why would a cyber thief

bother with a small practice? In reality, it is the small practices that can have the

breach than what was reported during the 2017 filing season.[2] Listed on the IRS website is a bevy of pertinent information for tax practitioners on the importance of securing sensitive data. IRS Publication 4557, *Safeguarding Taxpayer Data,* guides tax practitioners on how to implement and maintain a written data security plan as required by the Federal Trade Commission by the Gramm-Leach-Bliley Act of 1999. Additionally, IRS Publication 5293, *Data Security Resources Guide for Tax Professionals,* is a quick guide that informs tax professionals of tips and resources to protect their practices from a cyber attack.

With the 2019 tax filing season in full swing, you may be tempted to put off implementing a formal security plan (if you don't currently have one), or even wait to peruse the vast amount of information on the IRS website on cybersecurity. To help protect your practice's computer system from a cyber attack, you may have already purchased antivirus software, placed password protections on sensitive documents, and invested in a router. Although these steps are a good start, securing a tax office from cyber attacks goes way beyond these safeguards. There are quick, practical steps that can be implemented quickly to help reduce your exposure to a cyber attack.

1) WIFI is not your friend: These days, many tax professionals have mobile tax practices where they may meet a client at a local coffee shop or even at your client's home. Although it may be tempting and easy to utilize your client's home WIFI or a public WIFI connection to access your tax software or other sensitive data, WIFI connections are easily hacked. No matter how "safe" you may think the connection is, it is never as safe as a wired internet connection. Better to gather the documents and prepare the return back at your office than risk a potential breach.

2) Do not receive or send Personal Identifiable Information (PII) via email or text: It's hard to deny that it is fast, easy, and convenient for our clients to snap a picture of their tax document or their signed Form 8879s with their phones and forward the

information to us without a second thought. Whenever information is sent

system by clicking on the link or opening an attachment. Forwarding the attachment or link to a tablet or old computer that is not connected to your work would be a safer option.

3) Be on the lookout for phishing emails: Cyber thieves have become very clever in sending emails that appear to be from a legitimate source but are not. In the frenzy of tax season, it is easy to open a phishing email unintentionally. A real-life example of this is hackers who pose as third-party payroll companies. Many tax professionals use a third-party payroll company to process payroll for their clients and their practice. Cyber thieves are aware of this and have been sending out what look like legitimate emails from payroll providers, especially around the times when quarterly and annual payroll reports are due. Before opening an attachment or link from what seems like a legitimate source, hover over the email address and make sure it is spelled correctly and does not have any suspicious additions to the address. Sometimes the address is off by just one letter.

4) Accessing the internet: Whether conducting research about a complicated tax situation or clearing our heads with a video game or by watching a YouTube video, there is a continual need to utilize the internet in our line of business. Unfortunately, surfing the internet, even when doing tax research, can be a prime gateway for hackers and thieves to gain access to sensitive data. As with email attachments, it may be good to invest in an inexpensive laptop or tablet that is not connected to the practice network that you can use to access the internet.

5) Cybersecurity also extends to your staff: It is important that your staff practices good cyber-hygiene. Accessing social media sites, surfing the web, or checking personal emails on devices connected to the office network should be emphatically disallowed. Additionally, staff should refrain from using the USB portals on office computers to charge their cellphones or other portable electronic devices, as viruses

and spyware may inadvertently be transferred into the office workstation. This is

your client list for any purpose other than the tax practice is absolutely forbidden, even if it seems harmless. It is not only a breach of data and confidentiality; it can potentially leave a stain on your reputation that can be hard to get out.

7. Invest in privacy screen filters: With clients coming in and out of your office, it is easy for someone to glance at just the right time to see another client's PII on a screen. Privacy screen filters are an inexpensive and easy way to help safeguard sensitive data.

8) Lock your workstation when you need to step away: It is important to get into the habit of locking your computer when you step away. This is especially true when you are in an appointment with a client.

When it comes to securing the data in your office, remember to trust your gut. If an email does not seem right, or you have a "bad feeling" about opening an attachment, trust yourself and refrain from the action. Sadly, breaches will happen, even when we take all the steps we can to protect our client and employee data. However, if we take the proper precautions, we may be able to retain something we have spent years building, and that is our reputation.

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.