taxnotes®

state

Volume 94, Number 3 ■ October 21, 2019

National Cybersecurity Awareness Month: How's Your Cyber Hygiene?

by Courtney M. Kay-Decker

Reprinted from *Tax Notes State*, October 21, 2019, p. 213

National Cybersecurity Awareness Month: How's Your Cyber Hygiene?

by Courtney M. Kay-Decker

Courtney M. Kay-Decker

Courtney M. Kay-Decker is the former director of revenue for the state of Iowa, and the former state co-chair of the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center Partnership. She recently completed a term on the Electronic Tax Administration Advisory Committee to the IRS. She practices law with Lane & Waterman LLP in Davenport, Iowa.

In this inaugural installment of Dispatches From Davenport, Kay-Decker discusses cybersecurity challenges and tips for tax practitioners.

Maybe cybersecurity awareness isn't something that piques your interest like, say, the deductibility cap on state and local taxes on the federal return, or maybe some state taking the position that small seller thresholds are unnecessary after *South Dakota v. Wayfair Inc*. But it should. And since the U.S. Department of Homeland Security has declared October National Cybersecurity Awareness Month, this is a good time to talk about some basics for tax practitioners. Let me take a moment to tell you why you should care.

What Is Cyber Hygiene?

I picked up this catchphrase from a dear colleague during my tax administrator days. It isn't novel anymore, but the phrase succinctly captures what tax professionals need to do. In a nutshell, cyber hygiene consists of those practices you incorporate into your daily routine to help keep your devices, and any network they connect to, safe from cybercriminals. The critical point here is that cyber hygiene must be part of your daily routine, just like brushing your teeth. When I bring up cyber hygiene at speaking engagements or at cocktail parties, most people immediately tell me that they have a top-notch IT department or that they contract for the best and the brightest cybersecurity experts around. "That's great!" I say. Don't get me wrong, it is very important to use competent cybersecurity professionals. But it's not enough.

It's Not If, but When

The mantra in the security community is "not if, but when." If you or your firm hasn't experienced some sort of cyber compromise yet, you likely will. Disabuse yourself of the notion that it won't happen to you. Every time I speak about cyber hygiene, I hear new stories of cyber catastrophes and near misses. The common element in every story? Humans. Whether the story ends well always depends on cyber hygiene.

According to the Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanac, nearly all successful hacks and data breaches stem from phishing scams.[1] Think about that. Odds are, it won't be a software bug that will let in a criminal. It will be someone in your office who will unwittingly *open the door* for a cybercriminal to steal your firm's and your clients' confidential

[1] Steve Morgan, "2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics," Cybersecurity Ventures (Feb. 6, 2019).

information or hold that information hostage with ransomware.

Phishing is very advanced these days. Gone are the days of phishing emails riddled with typos and incorrect grammar and a gobbledygook email address. Now, phishers use social engineering to target *you* in particular. They have learned enough about you through all the data breaches over the years, and all the information you have volunteered publicly. Sometimes the sender's email address even looks as if it could really be the sender you know! The most convincing phishing emails appear to come from a source you know and are about a subject that is not out of the ordinary, either personally or professionally.

Tax practitioners have increasingly become the targets of cyberattacks. During the 2018 tax return filing season, the IRS received five to seven reports per week from tax firms that had experienced a data theft.[2] Tax firm data loss reports were up 29 percent over the same period in 2017.[3] In all, the IRS estimated that tens of thousands of taxpayers were affected by the data losses reported by tax firms.[4] And we know that not all data losses were reported, or even detected.

After a compromise has been discovered, a firm must put its incident response plan into action. That will necessarily include the laborious work of stopping any ongoing intrusion, identifying the scope and cause of the compromise, and determining which clients and governments (and insurance carriers) must be notified. There are tons of resources out there to help you develop or update your incident response plan. The IRS has recovery tips tailored for tax professionals in Step 5 of its latest security awareness campaign, Tax Security 2.0 — A "Taxes-Security-Together" Checklist.[5]

Cyber incident recovery and remediation is something that none of us wants to have to do for ourselves. Developing good cyber hygiene is the ounce of prevention that can minimize the risk of compromise resulting from our own human error.

Don't Be the Weakest Link!

I had the privilege of working with the IRS Security Summit and was the first state co-chair of the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center Partnership, a collaboration among the IRS, state revenue agencies, and the tax software industry tasked with detecting and preventing identity-theft-related tax refund fraud. Through these efforts, teams of analysts across the country work to identify new and evolving identity theft tax refund fraud schemes and prevent tax dollars from ending up in the hands of criminals. What I learned is this: Cybercriminals are super-smart and resourceful. When one path becomes difficult, the criminals find a new one. They are always in search of the weakest link. Good cyber hygiene will keep you from being the weakest link.

It's the Right Thing to Do

Back in the old days, it was easy to keep all those paper files secure. We locked our file cabinets and our offices and were careful when taking files out of the office. We learned to shred everything we no longer needed. With that, we were good at security. We rarely thought about the possibility of strangers looking at a client's file. They'd have to break in to the office or steal our transmittals from the U.S. mail. Hard work for the bad guys. Old-fashioned security was a physical infrastructure sort of thing, requiring common sense and not much more. Until relatively recently, even folks who were tech-savvy didn't think much about cybersecurity. But the world has changed.

We all know that tax professionals have a legal obligation to protect their clients' confidential information. IRC section 7216 sets forth that requirement for tax return preparers. Similar laws exist in each of the states. Also, the Gramm-Leach-Bliley Act[6] gave the Federal Trade Commission authority to establish information safeguards for various entities, including professional tax return preparers. Under the FTC Safeguards Rule, return preparers must create and enact security plans to

[2] Internal Revenue Service, IR-2018-245 (Dec. 7, 2018).

[3] *Id.*

[4] *Id.*

[5] IRS, IR-2019-143 (Aug. 13, 2019).

[6] Financial Services Modernization Act of 1999. See the Federal Trade Commission's website.

protect client data. Violation of the FTC rule may also be treated as a violation of the IRS rules for e-file providers.[7] Lawyers also have an ethical obligation to protect their clients' electronic data. The rules of professional conduct in most states require lawyers to have an appropriate level of competence in technology. In 2018 the American Bar Association issued guidance for lawyers in the event of a data breach.

It is no secret that many practitioners don't have the foggiest idea how our technology works or have the slightest idea how to recover from a breach. We tap an icon and the software does what we expect. We don't think about the zeros and ones behind the interface, or what it takes to encrypt a document or tax return that travels through cyberspace to ultimately land in the hands of the IRS, a state revenue agency, or your client. And for the most part, we don't need to know those inner workings. But what do we need to know to meet our legal and ethical requirements? Cyber hygiene.

Cyber Hygiene — Some Basic Tips

I hope you are now thoroughly convinced that maintaining good cyber hygiene is essential for your tax practice. A number of excellent resources offer easy-to-use, and relatively comprehensive, guidance for non-IT folk. At the top of the list is the National Cybersecurity Awareness Month 2019 Toolkit from DHS.[8] For cyber tips tailored to tax professionals, my favorites are the awareness campaigns created by our colleagues at the IRS. The IRS has compiled a full range of easy-to-use information, from basic cyber hygiene to developing an incident response plan. The information is under the umbrella of "Protect Your Clients, Protect Yourself" on the IRS website.[9] In the meantime, here are a few tips that anyone can implement into his or her individual routine without too much fuss. It is important to remember that cyberthreats are always evolving, so what works today may not work in the future, and nothing is foolproof.

1. Use long passphrases. Not passwords. Not passcodes. Passphrases. This is just math. The longer the passphrase, the harder it is to crack. All the devices connected to your network need a passphrase. The TV. The thermostat. The refrigerator. If an internet-connected device doesn't allow you to create a passphrase, think hard about whether you want to have it connected to the same network that you use for confidential client matters. Use a password assistant to help you.
2. Don't use the same passphrase for multiple accounts. Using the same passphrase at multiple sites makes it easier for the bad guys. If they crack one, they crack them all.
3. Use multifactor authentication methods. This means that you need two (or more) keys to log in, not just one. Two-factor authentication has become pretty common, and often you can choose among alternative methods. Check the security settings in your accounts and turn on a method that works for you.
4. Avoid unsecured public Wi-Fi for anything remotely confidential. You never know who else is lurking on an unsecure network, capturing your keystrokes, usernames, and passphrases. If you must use an unsecured network, use a VPN or use your phone's hotspot.
5. Be careful on social media. Very careful. Check your sharing settings. Don't overshare. Are you sharing only with people you actually know in real life? Or do your settings allow friends of friends, or even everyone, to see your posts? If the latter, anything you share can be used by a criminal to socially engineer you. Did you get a new dog? Hmm, pet names are common passwords! Did you complete one of those funny surveys that asks your favorite movie or some other trivia about you and then share it with the world? Not good. Those trivia questions are often the same questions that can be used as

[7] See IRS, Rev. Proc. 2007-40 (June 25, 2007), which establishes the rules for tax professionals participating as authorized e-file providers.

[8] Department of Homeland Security, "National Cybersecurity Awareness Month 2019 Toolkit."

[9] IRS, "Protect Your Clients; Protect Yourself," last reviewed or updated Aug. 23, 2019.

security questions when you forget your passphrase.

6. Develop an internal phishing radar. Pause for a beat before clicking on a link or attachment in an email or text message, or otherwise doing what the email asks you to do. Think: Does this email make sense? Am I expecting it? Did I talk with someone about it in real life? Is the sender's email address the one I'm used to seeing from the sender? Does it seem similar to any schemes going around? When in doubt, confirm by phone or in person.
7. Know your IT security team. Make sure they are trustworthy and competent to start; send them to training; and give them the tools to stay on top of emerging threats and best practices in safeguarding your systems. Make sure they arm all your connected devices with the latest versions of firewalls, antivirus software, malware detection, and so forth. Then, when they suggest a new safeguard, grumble for a minute if you must but listen to them!

Finally, remember that this list is a good start, but it only scratches the surface. There are references to resources throughout this article. Use them and the many other resources out there. And make cyber hygiene a routine in your tax practice. ■