6 Safeguards for Ensuring Accounting Cyber Security

March 20, 2022

With all the news about accounting cybersecurity threats, there's another angle that's less talked about: the opportunity these breaches create for CPAs and accountants. Clients increasingly see accountants as trusted advisors for all aspects of finance. By developing a comprehensive security plan, you'll increase the value you bring to your relationship with clients.

The situation may sound overwhelming. The list of threats is endless. Ransomware. Password guessing software. Vulnerable technology. Public WiFi. Phishing attacks. Thankfully, you don't need to be a cybersecurity whiz with three Ph.D.'s to protect your firm and your clients. Those security geniuses are busy around the clock. You can leverage their work to build a practical but effective security program for your accounting team or CPA firm.

The IRS released a six-step guide for accounting cybersecurity. Let's explore these steps and learn some practical ways you can protect your firm and your clients in the coming months and years.

1) Install and Update Antivirus Software that Scans Files and Memory for Malware

The IRS requires malware protection on any system that stores, processes, or transmits Federal Tax Information. While the IRS does not mandate any specific malware/virus

detection software, it has approved Symantec Antivirus for use on Windows systems internal to the IRS. Be sure to set it up to automatically update so you have the most current protection at all times.

2) Use Firewalls to Shield Your Computer or Network from Malicious Traffic or Malware

Firewalls come in two broad categories: hardware and software. Hardware firewalls are physical devices that can be integrated on home or office routers. Some internet service providers (ISPs) offer these directly, or they can be purchased through a vendor. Firewall software typically comes with operating systems or can be downloaded from a reputable website. Both types of firewalls help prevent unauthorized access to computers, but they cannot protect data in case a user downloads malware through a phishing attack.

3) Use Two-Factor Authentication to Secure Email, Accounting Software, or Any Password-Protected Product

Accounting professionals should always use two-factor authentication when it’s available. Two-factor authentication requires both a user name and password, and a second authentication method sent by text or through an app. Bad actors may uncover your username and password, and can spoof your mobile phone texts, but it’s nearly impossible for them to breach both these technologies at the same time.

4) Routinely Backup Critical Files to a Secure External Hard Drive or Cloud Storage Service

It may seem counterintuitive to create an additional copy of the data you’re trying to protect, but the public cloud providers like Microsoft and Google have tens of thousands of security professionals working to secure that data. As long as you upload the data through a secure connection, it’s relatively safe in a public cloud environment. The point is if something happens to your business-critical data, such as losing a computer, human error, or something more malicious, you’ll have a copy of the data that’s secure and can be restored.

5) Encrypt Files on Computers and Removable Media

Some accountants and CPAs believe encryption is too complicated or that an attack won’t happen to them. However, even the smallest accounting firms store sensitive data like social security numbers and bank account information, so they are attractive targets for cybercriminals who can sell this information on the black market. Ensure your data is encrypted both where it’s stored and when it’s transmitted across a network.

6) Write Down Your Data Security Plan as Required by the Federal Trade Commission's Safeguards Rule 5

A comprehensive security plan includes the security measures you'll be implementing within your organization. Perhaps more importantly, it includes a playbook for the role everyone in the organization plays in security. At the least, an accounting data security plan should account for how you'll educate team members about the methods used by hackers to breach data as well as security best practices for counteracting these threats.

Closing Thoughts on Accounting Cybersecurity

This talk about data breaches and ransomware attacks can seem overwhelming — after all, you want to focus on helping clients and growing your business. But cyber threats aren't going away, so it's helpful to reframe this as part of your fiduciary responsibility to your clients. They come to you, after all, because they want to focus on the core aspects of their own businesses or personal lives. So think of cybersecurity as another way to serve your clients beyond just number crunching.

Interested in learning more about accounting cybersecurity threats, and how you can respond? Read our guidebook, The Security Threats Facing Accountants, CPAs, and Bookkeepers in 2021.