NAEA Strategic Partner

360° CoveragePros

Cybersecurity for Enrolled Agents and Tax Preparers 101

As the demand for tax professionals grows by 9% from 2016 to 2026, more tax workers become targets for sophisticated, well-funded, and highly technical cybercriminal attacks and cybersecurity for tax preparers is becoming increasingly important.

Cybercriminals love to target tax professionals and enrolled agents as they possess tons of personal information on their clients - from email addresses and phone numbers to EFINs or CAF numbers. In 2016, cybercriminals successfully stole an estimated $1.68 billion to $2.31 billion of federal income tax before the Internal Revenue Service (IRS) stepped in with defensive measures. Between 740,000 and 810,000 tax returns were compromised. If criminals can successfully breach stringently protected government tax files, they can successfully target small and medium-sized businesses. In this article, we'll share more about tax preparer cybersecurity.

How Cybercriminals Attack Tax Preparers

Cybercriminals attack tax preparers and enrolled agents in many ways, but there are common attacks to mitigate against. However, new techniques and strategies always pop up, making it difficult for the average small business or independent contractor to stay fully aware of every new threat.

Ransomware

With ransomware attacks becoming increasingly damaging, criminals can gain complete control of an entire computer system and hold it in exchange for monetary compensation. 66% of organizations were attacked by ransomware in 2021, accounting for total financial losses of $49.2 million.

Criminals can hold a tax professional's entire data system containing sensitive personally identifiable information (PII) and confidential tax returns. This breaks client trust and can cause a severe loss of reputation, which eventually translates into lost revenue for tax preparers.

Phishing

Phishing schemes are sophisticated email attacks with fraudulent links; employees might harmlessly click on a link, input sensitive information, and suddenly expose data to cybercriminals. This might look like an email from the IRS saying, "your account has been put on hold," or that another type of action is required. The IRS even warns against these types of scams every year.

Man-in-the-Middle Attacks

These attacks typically happen over public WiFi; a user harmlessly logs on to what they think is a secure public WiFi network, and it's actually a cybercriminal in disguise. This allows the criminal to access confidential files, documents, and software. An employee might log into a fake website, click on an intrusive popup, or begin filling out the information for a "security certificate."

Cyber Claim Example

A Small Tax Prep business learns from a handful of clients that they were unable to file their returns because a hacker has already filed under their SSN/ TIN. The investigation continues on and the tax preparer learns that the direct effect of this breach remains limited to this handful of clients. However, after this occurred, the owner called their cyber policy provider and IT provider to learn more about the breach. The breach hotline and IT vendor let the firm know that even though only a handful of clients were affected, they cannot rule out the possibility that more protected information of those individuals has been accessed. With that being said, this triggered the need for credit monitoring, breach response and notification involving the firm's total book of business. Credit monitoring rules vary per state and so does other breach notice compliance that comes after this. The cost of a breach can add up quickly, especially securing the monitoring. According to Small Business Trends, the average cost of a cyber-attack to a small business is $25,612. Does your firm have the protection needed to handle this? Would your firm have the right resources like a claims/ breach hotline to take on the investigation?

What Can Tax Preparers Do To Avoid A Cyber Breach?

There are several strategies tax preparers/enrolled agents can deploy to avoid a cyber breach. To prevent a cyber breach, begin with employee security training. Team members are the first line of cyber defense, and 88% of data breaches are caused by human error. Also, a simple install of antivirus software protects against invasive viruses that can infiltrate an entire data system in minutes. Additionally, employing multifactor authentication (MFA) forces employees to log in to sensitive systems using several different devices, and it's unlikely cybercriminals will be able to bypass multiple types of authentication. To avoid a data breach, make sure employees use encrypted WiFi networks and never use public WiFi.

Cyber Liability Insurance

A Written Information Security Plan (WISP) is the formal documentation of a business's safeguards to protect personally identifiable information. A WISP typically covers three critical areas around employee training, IT systems and technology, and the process for identifying and managing failures. The IRS provided a WISP template to make it easier for tax professionals to create their own plans.

One key component of a WISP involves information about cyber liability insurance. This is essential coverage for tax preparers as firm data breaches have increased by 80% over the last few years. Do you know if your business is protected?

First, your tax clients deserve the best coverage and peace of mind. Your customers can trust you to handle their information securely. Also, keeping up-to-date with the last security standards can be used in marketing messages to differentiate your firm from others. You'll protect yourself against hundreds of thousands of dollars in potential loss, the headache of sticky legal situations, and the anxiety over an attack happening again.

With comprehensive cyber liability and data breach insurance, you're prepared for the worst-case scenario and won't suffer the adverse effects of a data or security breach. Also, you won't have to pay out-of-pocket for any first- or third-party costs, which can quickly add up to hundreds of thousands of dollars. 360 Coverage Pros will take care of any damage assessment and repair, lawyer bills, operational expenses, extortion, regulatory penalties, and more.

Protect Your Tax Business with 360 Coverage Pros Cyber Liability Insurance

Cyber liability insurance is low-cost protection against a potentially business-destroying attack on small businesses and independent contractors. Make sure you and your clients are both protected today.

Ready for peace of mind and protection? Explore the coverage options at 360 Coverage Pros, A Gallagher Affinity Company, prices start at $299 for $500,000 in coverage.