Are You Making Your Firm Vulnerable to Cyberattacks?

SmartVault

Whitepaper

SmartVault

CHAPTER 1

CHAPTER 2

CHAPTER 1

Your Database is a Cybercriminal's Goldmine

Accounting and tax professionals are considered high risk when it comes to cyberattacks. This is because of the data you handle and the type of clients you serve. And, if you're a small-to-mid-size firm, you're at an even greater risk of being targeted by a cyber thief. Let's discuss why.

Hackers Think Smaller Firms are the Best Targets

"It may seem counterintuitive, but the risk of cyberattacks is disproportionately higher for smaller and medium-sized organizations, which tend to be much more reactive than proactive," says Vijay Rathour, partner in the Digital Forensic Group. Cybercriminals think that small and medium-sized firms are easier to hack since they often lack the sophisticated cybersecurity programs larger businesses have, like virus detection software and dedicated IT teams.

It can be easy to overlook cybersecurity and think you'll never be a victim to an attack. Don't make that mistake at your firm. "Identity thieves always seem to find a hook to lure victims, and we increasingly see tax professionals as a target given the sensitive client data they handle," warns IRS Commissioner Chuck Rettig.

Your Risks of a Breach are Increasing

Cyberattacks, tax fraud, and scams are rampant, and each year, criminals only get bolder and cleverer. Unfortunately, the costs to accountants and taxpayers are enormous. Here's an example to put "enormous" into perspective: The government estimates billions of dollars were stolen by fraudsters from programs meant to help taxpayers during the pandemic. In fact, they're calling the massive amount of theft "the biggest fraud in a generation."

Worse still, reports have shown that scams are on the rise: there were eight million reports of tax scams and fraud, according to the 2022 Annual Report of the Identity Theft Tax Refund Fraud Information Sharing Mission and Analysis center. This number is **four times greater than the number of reports in 2021,** and it's not expected to drop anytime soon. "The number of attacks is large and increasing, both in volume and sophistication, and has expanded to...more complex tax scams," the report claims.

One of the most sophisticated schemes is recent: In March 2023, a federal grand jury indicted a group of seven individuals who allegedly filed over 370 false tax returns and attempted to claim over $110 million in tax refunds using stolen identities. The criminals used their victims' information to register with the IRS and change their victims' mailing addresses. They then accessed their tax information, like tax transcripts and wage records, and used the information to electronically file tax returns and claim fraudulent refunds.

Opening an Email Attachment Cost Accounting Firm $84,000

An employee at a small accounting firm opened an email attachment and immediately became victim to a ransomware attack. The document contained a virus that encrypted the data on the network and displayed a message demanding $8,000 on all of the firm's computers. The firm spent nearly $84,000 to recover. One of the biggest takeaways? Everyone involved in your practice must understand cybersecurity risks and their responsibilities in protecting data. After all, you're only as strong as your weakest link. Hear what experts say all firms should do to protect themselves from attacks like these.

WATCH THE WEBINAR

Cybersecurity Stats

Just How Damaging Are Cyberattacks and Criminals?

There were **8 million reports** of tax scams and fraud in 2022 (ISAC)

In 2022, the IRS found more than **$31 billion was lost** to tax fraud and financial crimes (IRS)

On average, every **11 seconds**, a company is victim to a ransomware attack (Cyber Security Ventures)

95% of breaches are caused by human error (World Economic Forum)

The average cost of a data breach in the United States in 2022 was over **$9.4 million** and over $5 million in the UK (IBM)

22 billion records were exposed in 2021 breaches (RiskBased Security)

Over 70% of US tax-filing adults are concerned about data breaches when filing income taxes online (PC Mag Tax Survey 2021)

In 2020, malware **increased by 358%** and ransomware by **435%**, compared to 2019 (Help Net Security)

Your Clients Expect Data Security

Your clients trust you to keep their information safe. When you take proactive steps to protect data, it shows potential and current clients that you take data security seriously. This builds trust and credibility, which can lead to increased referrals, higher loyalty and retention, and more positive reviews. It also gives you a competitive advantage. Clients are more likely to choose a firm that prioritizes their privacy and security over one that does not.

In fact, taxpayers have high expectations for secure, online collaboration with their tax professionals, according to Intuit's 2022 Taxpayer Insights & Intelligence Brief. The report found that: 73% **want a** secure place to upload documentation to their tax professional throughout the year and 86% expect their tax documents and information to be stored with industry-standard security. How can you meet these expectations? It all comes down to your accounting tech stack.

You Must Comply With the Law

Cybersecurity isn't just a matter of doing what's best for your clients and business. It's also about compliance: Tax and accounting professionals are legally obligated to secure their data from breaches.

The Federal Trade Commission requires paid tax and accounting professionals to have a robust data security plan called a Written Information Security Plan (WISP). Firms are also required to comply with portions of the Gramm-Leach-Bliley (GLB) Act, which requires you to outline how you will protect your clients' personal information. Firms that fail to comply may lose their business licenses and damage their reputation. And then there are the financial penalties: Section 7216 of the Internal Revenue Code (IRC) imposes criminal penalties on tax preparers who make unauthorized disclosures or uses of information furnished to them in connection with the preparation of an income tax return. IRC Section 6713 imposes monetary penalties on the unauthorized disclosures or uses of taxpayer information by any person engaged in the business of preparing or providing services in connection with the preparation of tax returns.

Download this free checklist to confirm you're writing a compliant WISP.

DOWNLOAD THE CHECKLIST

CHAPTER 2

You're Most Likely Putting Your Data at Risk

> **"We need to ensure that we are handling all of our client data in a way that meets all regulations while giving ourselves and our clients peace of mind."**
>
> Robin Johnson, owner
> TaxAssist Accountants Norwich North
> Read the Case Study

You are the first line of defense when it comes to protecting your firm's and clients' data. The most effective way to safeguard it is to understand how criminals can access it and how vulnerable your firm is.

Common Attacks and Vulnerabilities

So, what's meant by "vulnerability?" Luke Kiely, a law enforcement veteran and SmartVault's Chief Information Security Officer, says it refers to what a criminal needs to exploit to get what they want. There are attacks that can happen to anyone and any industry, but there are also scams specific to tax and accounting professionals. Let's take a look at this further.

4 Ways Cybercriminals Access Data

To ensure you notice when someone is trying to hack into your system, be aware of the common methods. They include:

Malware

Cybercriminals design malware — short for malicious software — to steal your data and destroy and/or damage your computers and systems. Infections typically happen from clicking on a link or opening an infected email attachment. Malware includes things like viruses, spyware, and ransomware.

Ransomware

That brings us to ransomware. This is a type of malware that makes its victims pay — literally. Ransomware keeps you from accessing your data by encrypting your files, making them unreadable. The criminals give you an ultimatum: Pay up or lose the data indefinitely. Some attackers even demand a second ransom with the promise they won't sell your data online to other criminals. Ransomware is a final step in a larger attack, as the criminal already accessed your network and data through an initial method, like malware or phishing.

Phishing

This type of attack lures people into disclosing their personal information, like passwords and Social Security numbers, and it works well. An estimated 91% of all data breaches and attacks begin with a phishing email, according to the IRS. Criminals accomplish this by making the victim believe the message and request are trustworthy. These attempts are usually performed via email or text message and appear to come from known, trusted sources, like your partner, client, bank, loan provider, credit card company, or even places like big-box stores.

Man-in-the-Middle (MitM)

Also known as eavesdropping, a perpetrator puts themselves between you and an application (i.e., your mobile device and its Internet browser). The victim is completely unaware that all the information they're passing to the application is going straight to the perpetrator. The attacker may even install software to access all of your information. People put themselves at risk for this when they connect to the Internet using an unsecure public Wi-Fi.

3 Scams Specific to Tax and Accounting Professionals

In 2022, the IRS found more than $31 billion was lost to tax fraud and financial crimes. And while attacks can happen any time of the year, criminals tend to take advantage of the busy season. Hackers know you'll be distracted as you work around the clock to meet deadlines. Plus, they know the volume of documents exchanged between tax professionals and clients increases astronomically during tax season, making it the perfect time for criminals to attack. **Here are three common ways criminals scam tax firms and their clients:**

1 Sending texts and emails claiming to be from the government and demanding immediate action.

One popular trick scammers use occurs via text, email, and even social media. They frequently contain links or attachments, and they often come with panic-inducing threats, such as demanding immediate payments to avoid being arrested. The IRS and state tax agencies will only ever contact you by mail. They do not call, email, direct message (DM), or text. Getting any one of these messages is a red flag.

2 Stealing taxpayers' identities and applying for fraudulent unemployment benefits.

If your client filed for unemployment but hasn't received the benefits, this may be because a scammer has stolen their identity and ensured the money is sent to their account. This is called "Claim Hijacking" or "Claim Account Takeover." Another red flag: You or your client receive notices saying they filed for unemployment, but they never did. They may even receive unemployment benefits they never asked for. When this happens, criminals make sure they also receive a 1099-G tax form to include the benefits on their tax returns.

3 Stealing tax refunds.

Michael Dexter Little, who was sentenced to nearly 20 years in prison in January 2022, filed false tax returns with the names and information of his victims. He obtained at least $12.3 million in fraudulent tax refunds. And, as we saw in chapter 1, he's not the only one. This scam is extremely popular and leaves millions of hardworking taxpayers high and dry each year. With this ages-old scheme, thieves will steal your identity, file a W-2 in your name, and then have your tax refund deposited into their account. To make things worse, they don't necessarily have to contact you to get the information they need.

4 Ways Firms Put Data at Risk

Cybersecurity is ultimately about the people. Everyone must recognize and embrace their roles and responsibilities in protecting themselves (and others) online. **Here are four common ways firms put their data at risk of attack:**

1 Avoiding System Updates

Too many people increase their vulnerability by ignoring or postponing software updates on their devices. Even though updates can be time-consuming and frustrating, they're necessary because viruses and malware change and adapt all the time. And, if you work in a regulated industry, you're very likely to find yourself staring down the barrel of compliance issues if your system is breached.

2 Not Training Staff

Patrick Schreiner, a business cybersecurity risk advisor at one of America's Big Three Index Fund Managers, says untrained staff are a big source of mistakes that result in data breaches. He warns that cyberattacks frequently start when someone clicks a malicious link in an email or downloads an attachment. Luke Kiely, Chief Information Security Officer at SmartVault, agrees, and he recommends that you remind your team members to examine things like emails carefully.

Consider these tips: Phishing emails often have odd reply addresses, strangely worded content, and a sense of urgency. Ask yourself, 'Am I likely to get an email from a CEO asking to make a change to a bank account at 5pm on a Friday?' And, if one of your team members believes they might have made a mistake, it's crucial that they don't wait to tell you.

3 Not Following Simple Best Practices

Make good security hygiene a regular part of your routine. Use strong, long, complex passwords in addition to multi-factor authentication (or MFA). "MFA in general is a really easy win for a lot of people... [because it can] prevent bad actors from accessing your accounts even if they have your password," says Schreiner. You should also protect yourself against malware by installing recognized, commercial antivirus software.

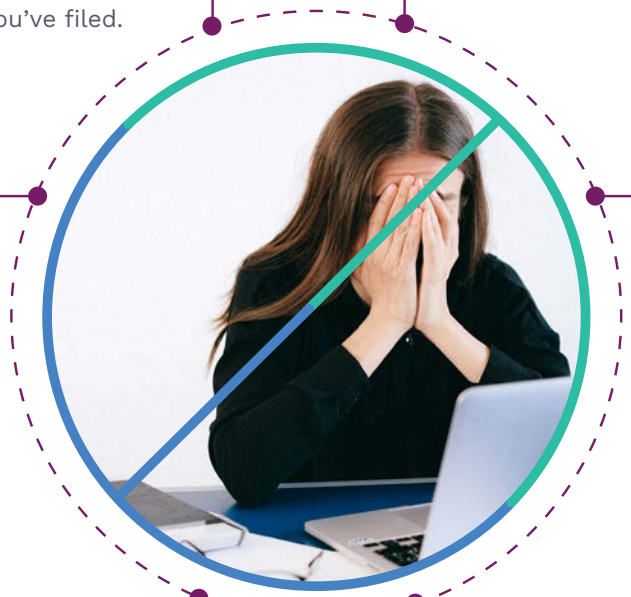
4 Using Email to Share Sensitive Data

Email is one of the most common and riskiest tools used in businesses today. Anyone with know-how can intercept and read your emails. Many of the documents that accountants require include at least one data point that should never be sent via email. Form W-2, for example, has the person's name, Social Security number, address, income, and more. This gives criminals exactly what they need to steal identities or make money selling the information to other criminals.

Know the Signs

Warnings You've Been Hacked

According to the IRS, here are some common signs that you're a victim of an attack.



You receive e-file acknowledgments for tax returns you have yet to file or you receive more acknowledgments than returns you've filed.

Your clients received a tax transcript that they didn't request or a message that someone created an online IRS account for them.

Clients contact you about or respond to emails or other requests that you didn't send.

Your clients tell you the IRS sent them authentication letters or a refund even though you haven't filed their tax return yet.

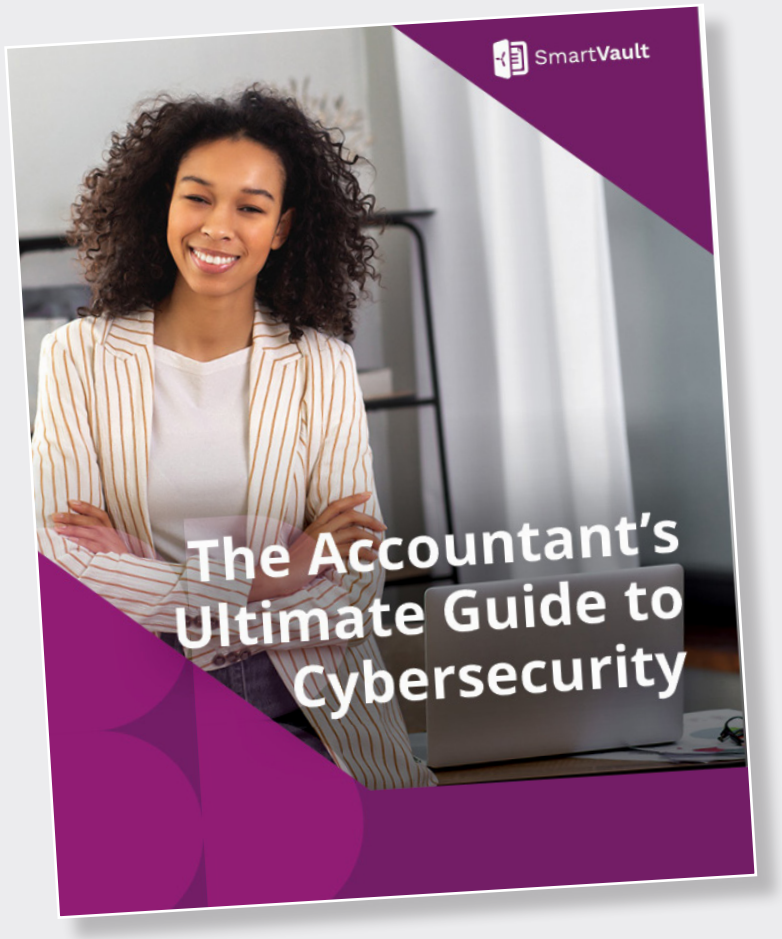
Your computer starts acting slow, unresponsive, or strange, including software taking longer to load, the cursor moving without you touching the mouse, and/or it locks you out of your computer or network.

Your clients receive a message that someone has accessed their online account or that the IRS disabled their online account.

The IRS rejects your client's e-filed return because they've already received another return with their Social Security Number.

Keep Your Data Safe: Complete a Risk Assessment and Build a Robust Cybersecurity Program

Don’t risk your business. Download The Accountant’s Ultimate Guide to Cybersecurity to learn actions you can implement to proactively protect your data and meet compliance obligations.



Here’s a breakdown of the free guide:

- Chapter 1: See why cybersecurity has to be a top priority for your firm, including the possible legal and financial ramifications you may face if you don’t have a plan.
- Chapter 2: Learn about tax scams, common ways cybercriminals access data, and how to conduct a risk assessment to see where you’re firm is at risk.
- Chapter 3: Learn how to develop a strong cybersecurity program to lower your vulnerability and meet legal requirements.
- Chapter 4: Learn how to stay updated on the cybersecurity threats of tomorrow without having to become an IT expert.
- Chapter 5: See how a document management system will enhance your cybersecurity, as well as how to find the right vendor and integrate the solution into your tech stack.

Download Your Free Guide