The Top Cyber Security Threats Facing Accountants, CPAs, and Bookkeepers In 2021

March 20, 2022

With 72% of tax-filing adults in the US expressing some level of concern over their personal data being compromised when they file taxes, accounting professionals need to carefully consider threats connected to software, hardware, and communications channels.

It's difficult to quantify the impact of a cyberattack, but any attack must be considered a dangerous data breach. Accountancies are attractive targets as even the smallest firms possess valuable sensitive client data that cybercriminals can use to steal identities, create fraudulent tax returns, or drain life savings.

In this post we'll review cybersecurity in accounting and show how cloud hosting is a straightforward way to eliminate threats.

What Are the Biggest Threats to Accountants?

The most common threat to accountants is malicious software, or malware. Around 91% of all cyberattacks start with a phishing email that entices you to open a link or attachment containing malware, according to the IRS. Once you download malware the attacker can steal passwords, track keystrokes, or gain access to sensitive client data in your computer systems.

Viruses

A type of malware that inserts itself in legitimate programs and self-replicates into other programs on the host system.

Ransomware

Malware that restricts access to software or client files until a ransom is paid. Ransomware is

increasingly pernicious since attackers can hire a service to perform the ransomware attack, then demand payment in the form of cryptocurrency to keep their identity hidden. An Albany, New York-based accounting firm was hit with one such attack in December 2019. The attackers breached the firm's computer network for three days before the firm noticed. They exposed confidential data of some of the accountancy's healthcare clients, including names and dates of patients, and blocked access to the firm's files.

Phishing

A type of cyber attack where an attacker masquerades as a legitimate organization or individual to dupe victims into opening a link or attachment that contains ransomware. In early 2021, the IRS warned tax professionals of one such email phishing scam that claims to be from "IRS Tax E-Filing." The email asks tax professionals to reply with a copy of their driver's license and Electronic Filing Identification Number (EFIN). The thieves could use this information to file fraudulent tax returns. The IRS also warns of a phishing scheme where cybercriminals pose as a potential client then send an email with an attachment they claim is their tax information, but in fact is malware.

How Does Malware Enter Your System?

Office technology and staff behavior can present potential gateways for hackers and their malware. Proactive steps must be taken to close vulnerability gaps.

Vulnerable technology

Computers, laptops, smartphones, and wireless networks present exposure risk for accountancies. Client data stored on devices could be jeopardized if attackers gain access to the device by infecting it with malware. Using public WiFi networks to share work files also leaves them open to attackers, as public WiFi is notoriously vulnerable to hackers.

SMS

SMS texts lack end-to-end encryption, so if hackers attack the network used to send your messages, they can read the contents and steal sensitive data. Cell phone services including Verizon, T-Mobile, and US Cellular store the contents of texts for a period of time, presenting another layer of vulnerability. This means SMS is not a secure way to share sensitive client information.

Weak security at the email recipient's end

Many email programs, including Gmail, automatically encrypt messages stored on their server. However, if your recipient's email provider does not support encryption, your message could be exposed as it travels to their computer. Robust email security requires end-to-end encryption.

Weak passwords

Password reuse and weak passwords remain one of the most common cybersecurity vulnerabilities. Password manager NordPass found that the two most common passwords of 2020 were “123456” and “123456789.” Each of these passwords can be cracked in under a second using easily available password cracking software. Another danger is using the same password across websites. If a hacker cracks the password on one site, they may gain access to other accounts where you use the password.

Poor staff training

With the rise of remote work, cybersecurity training gains an extra level of complexity and importance. Employees often use the same devices for work and their personal lives, which creates potential security risks. They may use public wifi, which potentially exposes their devices to hackers. And they may not be aware of the basics of accounting cybersecurity.

Cloud-Hosted Accounting Software Resolves Common Security Issues

It’s critical, even mandatory, to develop a comprehensive security plan for your organization. But you’re not a cybersecurity expert — you’d rather devote your time to growing your business and solving problems for your customers.

A cloud-hosted accounting platform can counteract these threats. Sharing client data in a secure cloud environment is more secure than sending files through email. It helps keep data out of smartphone and laptop storage where it’s more susceptible to attack. A seasoned cloud hosting provider supports your move to a digital workplace while freeing you from the headaches associated with maintaining your IT stack.

To read more about how Swizznet’s secure, enterprise-grade hosting helps you serve clients virtually while protecting their data, read our Tech Matters data sheet.

For a deeper look at top security threats accountants are facing and what you can do about it, download our ebook here.

Wes Stillman, Chief Executive Officer, RightSize Solutions

“Really understanding the industry you serve is the only way to fully leverage technology.”

After 30+ years of managing technology in high-level positions, Wes began RightSize Solutions in 2002 because wealth management firms needed a technology partner who really understood their needs. More than 13 years later, he remains committed to understanding

every nuance of his clients' businesses.

Prior to founding RightSize Solutions, Wes' clients included major airlines, broker dealers, trust companies, health care providers, community banks and other financial institutions. He has held high-level positions at National Advisors Trust Company, FSB, Comdisco, Midwest Consulting Group (Senior Consultant and Yellow Technology Services (Director of Technology).

A technology pioneer in every sense, Wes is regularly quoted as a subject matter expert in industry publications and also speaks to small and large groups on topics such as cybersecurity, cloud-based environments and leveraging technology.

About RightSize Solution

A sister company in the Swizznet family, RightSize Solutions is headquartered in Lenexa, KS. Our company roots date back to 2002 and our focus is exclusively in the wealth management community. As a leading provider of IT Management and Cybersecurity, RightSize Solutions helps firms navigate the promise of technology to gain greater flexibility, lower costs and increase productivity. A hybrid of customized technology, proactive management and unrivaled service, we keep your systems securely running and your business soaring.Your blog post content here…