Cybersecurity Tips for Accounting Data in 2021

July 25, 2022

October may be over, but cybersecurity awareness and the National Cyber Security Alliance's (NCSA) theme of "Do Your Part. #BeCyberSmart" applies year round. At Swizznet, we're happy to join in and continue the theme throughout the year. This isn't the first time we've shared tips to help firms improve accounting data security.

Let's explore why it's important for tech-powered accounting firms to #BeCyberSmart, then take a look at some common threats to accounting data security. We'll wrap up with a few up-to-date steps accountants can take to protect their firms and their clients.

Why It's Important to #BeCyberSmart

Ransomware attackers have hit major companies like Colonial Pipeline and JBS, the largest beef supplier in the world. The world's largest organizations are spending billions of dollars on cyber security and insurance. With the media focus on these large-scale attacks, small- and medium-sized accounting firms may think they're not attractive targets, but even the smallest firms have access to customer financial and organizational data that hackers find valuable.

One growing mode of attack against small or medium-sized accounting practices is ransomware. A cybercriminal who gains access to accounting data could threaten to delete or expose that data if a ransom is not paid.

Swizznet has seen this firsthand in a state-based construction company client. Swizznet's AI-enabled technology powered by CrowdStrike® noticed an unusual log in and behavior from one of the firm's employees. Our experts monitored the situation and realized the intruder had hacked the employee's credentials and was attempting to gain full access to the client's server, a sign they were setting the client up for a ransomware attack. We were able to halt the attack in this case.

Remote work creates new vulnerabilities, as accountants, employees, and clients share data through personal devices and out-of-office networks. Altogether, accounting firms of all sizes should assume they are in hackers' crosshairs and prepare security plans with that in mind.

By the Numbers:

- 43% of ransomware attacks hit small businesses, and 40% of ransomware victims chose to pay the ransom, which cost an average of $8,100 in 2020 (PurpleSec).
- The FBI's Internet Crime Complaint Center fielded 2,084 ransomware incident reports from January to July 31, 2021, with over $16.8M in losses (CISA).

- One in 15 US-based organizations experienced a ransomware attack or breach that blocked access to systems or data from July 2020 – July 2021 (IDC).

The Most Common Threats to Accounting Data Security

The thought of securing an accounting firm's entire online presence may seem overwhelming. Accountants, after all, are in the business of accounting, not IT.

Fortunately there is a consistent pattern to how bad actors attempt to breach networks and data. Verizon reports that email is the most common medium attackers use for distributing malware and phishing.

Email-based attacks work because email provides a direct way to reach employees and gain access to your systems and data. It's difficult to prevent users from following malicious links in emails, and hackers use a variety of tactics to trick recipients into clicking through.

Verizon found a median click-through rate of 3% in simulated phishing emails, but some of the simulated phishing emails had over 50% click-through rate, illustrating why attackers increasingly use this method.

Keep An Eye Out for These Phishing Tactics:

- Emails from a known contact but with the wrong email address.
- Grammar or other mistakes in emails
- Landing pages missing images or with misspelled URL
- Unexpected emails, like an email from Amazon stating your laptop couldn't be delivered when you didn't order a laptop (CPA Practice Advisor)

Building a Human Firewall

Since human error is behind most data breaches, it's critical to train both employees and clients so they can help prevent cyber attacks. Systems security is no longer the sole responsibility of IT departments. While cyber security experts are necessary to identify and halt breaches, it's much less expensive and stressful to prevent attacks in the first place.

A key part of training is teaching employees about malware, which commonly enters systems through phishing emails. These emails masquerade as trustworthy sources, such as banks or the IRS, and invite users to click on a malicious link or ask users to transmit sensitive information, such as credit card numbers or passwords.

For more about the types of information you should include in employee training (and our advice about how to plan a training day), check out our post, Are Your Work-from-Home Accounting Setups Secure? Cybersecurity Tips.

The Importance of Technology

Cybersecurity often brings to mind antivirus software or other technology-based ways of securing your systems. While the human side of cybersecurity is critical, new technology makes your systems much more secure against data breaches, even in the event an employee or client downloads malware.

Swizznet’s new SwizzStack suite of services is an accessible yet powerful way to protect your firm’s data. In addition to security compliance and managed IT services, SwizzStack delivers continuous system monitoring, device management, and private cloud platforms that are flexible and scalable. SwizzStack backs all that up with Swizznet’s Obsessive Support®, so you can focus on your business without worrying about security.

To learn more about how SwizzStack can help boost your accounting data security, contact us.