CPA
Practice Advisor

your CPA firm's reputation and integrity, security is paramount.

Apr. 09, 2024

By Oren Koren

Tax season is underway, which means cyber criminals are hard at work. With the plethora of highly sensitive personal and financial data being shared between firms and clients, it’s the perfect time for bad actors to strike, especially as the April 15th

What tactics are ‘hot’ this season

Phishing continues to be one of the main vectors for tax-related scams this year with malicious actors impersonating legitimate entities to trick CPA professionals into divulging sensitive information or downloading malicious software. These attacks often leverage social engineering techniques to appear authentic, making them difficult to detect.

Another significant concern is the emergence of malware strains like AsyncRAT, which we’ve seen a rise of this year, as they grant attackers remote access to compromised systems. This type of malware poses a severe risk to CPA firms, often starting as a dripping leak but becoming a gushing waterfall, as it can enable unauthorized access to sensitive client data, including tax returns, financial statements, and personal information.

While AsyncRAT is just one example, a common thread among the multitude of other threats is the attacker’s simple usage of file sharing platforms like Google & MediaFire which start the chain of infection.

Non-negotiable Cyber Strategies for CPA Firms

To effectively protect your CPA firm and clients from cyber threats during tax season, consider implementing the following principles and strategies:

1. Be Vigilant & Skeptical: Unfortunately, we live in a world where you can never truly let your security guard down. If an email or message seems suspicious, even if it appears to be from a known contact, approach it with caution. Be sure to verify the sender’s identity before opening any attachments or clicking on any links.

- Foster A Culture of Cyber Awareness: Conduct regular training sessions to educate

- Update Your Endpoint Security Tools: While you may think you've checked the box by simply installing endpoint security measures like antivirus software, firewalls, and intrusion detection systems – you must not overlook the importance of *maintaining* and *regularly updating* these systems. These updates often include patches for security vulnerabilities.

- Leverage Security Control Assessments: By leveraging tools that automate the analysis of security tools, you can identify and neutralize threats well before they infiltrate the network. Better yet, you'll save time and money, reduce the risk of human error and allow for the safe remediation of threats.

Shift Your Mindset: Tax Season, Year-round.

You're well aware of the pressure that mounts each year in advance of the filing deadline – so why add extra stress to an already overwhelming time of year? Cyber security should be weaved into your firm's ethos all year round – not just a few months each year when there's an uptick in threats.

The key to securing and maintaining clients will always be trust. In order to safeguard your CPA firm's reputation and integrity, security is paramount. It's time to enable an always-on security approach that flips the script and shows hackers who the real security-savvy one is.

Oren Koren is the Co-founder and Chief Product Officer at Veriti. Prior to founding Veriti, he was the senior product manager at Check Point Software Technologies, where he led AI-based innovations and advanced data analytics projects redefining threat hunting and SIEM applications. Oren also served for 14 years at the prestigious 8200 unit and was responsible for different cyber security activities and research.

Firm Management • Security • Taxes