Tax Filing Season and Cybersecurity Threats

The U.S. tax filing season, running from January to April, presents a prime opportunity for cybercriminals to exploit vulnerabilities in organizations, as millions of individuals file their taxes electronically. With over 90% of tax returns processed digitally, cybercriminals take advantage of the increased online activity by impersonating trusted entities like the IRS and financial institutions. This period sees a rise in phishing, smishing, and other social engineering tactics, designed to trick individuals into disclosing sensitive information. The surge in online filing services and tax-related communications further expands the attack surface, making it challenging for both individuals and organizations to distinguish legitimate services from malicious threats.

Cybercriminals often lure victims with promises of unusually high refunds, expedited processes, or significantly reduced filing fees, enticing individuals to provide their personal and financial details. For organizations, these scams pose an even greater risk, as compromised personal data can grant attackers unauthorized access to corporate networks. The handling of sensitive information during tax season is a significant risk, especially for financial institutions and businesses that rely on electronic filing. Malicious actors exploit this increased urgency and financial information flow, potentially causing long-term damage to the institution's reputation and regulatory standing.

Understanding the techniques cybercriminals use during tax season – not limited to phishing, smishing, malvertising – helps organizations better prepare to defend against these sophisticated and evolving threats. This article will also explore the broader impact on organizational security, emphasizing the critical need for proactive threat detection, continuous monitoring, and robust security awareness training to protect sensitive financial data during and beyond the tax filing season.

This report contains valuable insights for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email info@criticalstart.com.

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.