78% of Organizations Susceptible to Tax-Related Phishing Attacks

Valimail's analysis focused on the presence and validity of Domain-based Message Authentication, Reporting and Conformance (DMARC) and Sender Policy Framework (SPF) records. Across all domains analyzed, 78% of the organizations either lack DMARC ...

Mar. 30, 2020

Most organizations, including businesses of all sizes, don't have adequate protocols to help protect them from tax-related phishing scams, according to a new report. The

2020 Tax Scam Report is from Valimail, a provider of identity-based anti-phishing solutions.

Valimail analyzed the public DNS records for 200 domains likely to be impersonated for tax fraud, including the 2019 Fortune 100 (some of the largest U.S. employers), U.S. states' departments of revenue, federal tax agencies and well-known tax preparation services. Valimail found the majority of these organizations lack adequate protection against email-based scams including phishing, BEC and W-2/personal information scams.

Valimail's analysis focused on the presence and validity of Domain-based Message Authentication, Reporting and Conformance (DMARC) and Sender Policy Framework (SPF) records. Across all domains analyzed, 78% of the organizations either lack DMARC records or their DMARC policy is not enforced. However, 91% of the domains have SPF records, which indicates a willingness to implement email authentication — although SPF does not protect domains from phishers spoofing the "From:" field. Without DMARC at enforcement, attackers are able to spoof these organizations' domains and initiate convincing tax-related phishing attacks.

"Threat actors have historically used major events to enhance their phishing attacks, and tax season is no exception," said Alexander García-Tobar, CEO and co-founder, Valimail. "However, we are in a unique position today: Not only is it tax season, but the COVID-19 pandemic has forced U.S. legislators to take aggressive actions to limit social interactions, and as a result many recently out-of-work individuals are facing lost wages. These individuals may be counting on a quick tax return, or they may be confused about the recently changed tax filing deadline. This makes people all the more susceptible to convincing tax scams, and cybercriminals are always willing to take advantage of uncertainty. Unfortunately, organizations that do not have DMARC records at enforcement are an easy target for criminals who use spoofing to launch highly convincing tax-related scams aimed at consumers or these companies' own employees."

Additional key findings from Valimail's Tax Scam Report include:

- State tax agencies are the most vulnerable to domain spoofing: 49 of the 55 agencies analyzed are either missing DMARC records or do not have DMARC policies at enforcement.

- 5 of the 6 federal agencies analyzed are protected with DMARC at enforcement, underscoring the effectiveness of practices outlined in the 2018 Homeland Security

Binding Operational Directive 18-01.

- Of the 16 tax preparation services analyzed, just 7 (44%) were protected with DMARC at enforcement.

- 77 of the 2019 Fortune 100 are not protected with DMARC at enforcement.

The low overall rate of DMARC enforcement indicates that there is much work to be done to eliminate tax-related fraud and identity theft caused by domain spoofing and phishing. To download the full report, please visit: https://www.valimail.com/resources/tax-season-vulnerabilities/

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.