Mimecast State of Email Security 2020 Report Reveals 60% of Organizations Expect to Suffer from an Email-borne Attack

June 9, 2020

Fourth Annual Report Finds Greatest New Concern is Email and Web Spoofing

LEXINGTON, Mass., June 09, 2020 (GLOBE NEWSWIRE) -- Mimecast (NASDAQ: MIME), a leading email and data security company, today unveiled its fourth-annual State of Email Security 2020 report. This report summarizes details from 1,025 global IT decision makers on the current state of cybersecurity. Providing year-over-year comparisons, along with Mimecast's analysis from the first 100-day period of the coronavirus public health crisis, the report is designed to both offer valuable insights into recent attack trends organizations are challenged with and to serve as a guide to drive continuous improvement to any organization's cyber resilience strategy.

The findings in this year's State of Email Security report demonstrate that despite high levels of confidence in respondents' cyber resilience strategies, there is a clear need for improvement. The large majority (77%) of respondents say they have or are actively rolling out a cyber resilience strategy, yet an astounding 60% of respondents believe it is inevitable or likely they will suffer from an email-borne attack in the coming year. Respondents cite data loss (31%), a decrease in employee productivity (31%) and business downtime (29%) due to a lack of cyber resilience preparedness.

"We're seeing the same threats that organizations have faced for years playing out with tactics matched to world events to evade detection. The increases in remote working due to the global pandemic have only amplified the risks businesses face from these threats, making the need for effective cyber resilience essential," said Joshua Douglas, vice president of threat intelligence. "It's likely that cyber resilience strategies are lacking key elements, or don't have any at all, depending on the organization's maturity in cybersecurity. Security leaders need to invest in a strategy that builds resilience moving at the same pace as digital transformation. This means organizations must apply a layered approach to email security, one that consists of attack prevention, security awareness training, roaming web security tied to email efficacy, brand exploitation protection, threat remediation and business continuity."

Times are Changing: The Threats You Can't See Impacting your Brand

This latest research comes at a time when organizations across the globe have been forced to adopt remote work policies for employees in response to the coronavirus pandemic. Threat actors have seized this opportunity and evolved the ways they are targeting their victims. Domain-spoofing and email-spoofing have become mainstream attack vectors, according to the report.

Nearly half of organizations (49%) surveyed report anticipating an increase in web or email spoofing and brand exploitation in the next 12 months, and it is a rising concern. In fact, 84% of respondents feel concerned about an email domain, web domain, brand exploitation, or site spoofing attack.

It is critical for organizations to look beyond their email perimeters to determine how cyber threat actors may be using and damaging their brands online.

Yesterday's Threats Are Unwavering Year over Year

Similar to years past, impersonation attacks, phishing attempts and ransomware continue to be a major problem, according to the research. Seventy-two percent of report participants said phishing attacks remained flat or increased in the last 12 months and 74% report the same of impersonation attacks. This indicates that phishing is potentially becoming more difficult to stop or prevent due to more advanced tactics like spear-phishing.

Ransomware also continues to wreak havoc, as just over half of respondents (51%) said ransomware attacks impacted their organization, citing data loss, downtime, financial loss and loss of reputation or trust among customers.

The Need for a Strong Human Defense

The State of Email Security 2020 report also shines a light on the urgent need for a more cyber aware workforce. Encouragingly, 97% of the respondents' organizations offer security awareness training at varying frequencies and formats. However, 60% of those surveyed reported having been hit by malicious activity spread from employee to employee, pointing to the fact that the format or frequency of these trainings could be the problem.

With frequent, consistent, engaging content that humanizes security, security awareness training is an effective way to reduce risk inside the network and organization.

Download the full State of Email Security 2020 report.

About Mimecast:

Mimecast (NASDAQ: MIME) was born in 2003 with a focus on delivering relentless protection. Each day, we take on cyber disruption for our tens of thousands of customers around the globe; always putting them first, and never giving up on tackling their biggest security challenges together. We are the company that built an intentional and scalable design ideology that solves the number one cyberattack vector – email. We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error and technology failure; and to lead the movement toward building a more resilient world. www.mimecast.com

Mimecast Resources

- Download the full report: State of Email Security 2020
- Read past reports on the State of Email Security Hub

Mimecast Social Media Resources

LinkedIn: **Mimecast**
Facebook: **Mimecast**
Twitter: **@Mimecast**
Blog: **Cyber Resilience Insights**

Press Contact

Alison Raymond Walsh
Press@Mimecast.com
617-393-7126

Investor Contact

Robert Sanders
Investors@Mimecast.com
617-393-7074

Source: Mimecast Limited