Picture credit: AdobeStock

# TO SERVE AND PROTECT

**Richard Bourne** *explains why more is needed to protect government businesses*

**While there is now a multitude of options for organisations to connect online, email remains one of the most critical business tools for communication, collaboration, and information exchange in both the private and public sectors. Due to the ubiquitous, convenient nature of email it also makes for a prime target for cyber attacks.**

Government entities, entrusted with sensitive information and critical infrastructure, face heightened threats from malicious actors ranging from cyber criminals to nation-state adversaries. This article explores how email security has evolved, the gaps that persist, and what additional measures are necessary to protect government businesses.

Email threats have evolved dramatically over the past two decades. Initially, attackers relied on simple spam and phishing schemes to exploit vulnerabilities. Today the threat landscape is far more sophisticated, with multiple attack vectors. Phishing has morphed into Spear Phishing where highly targeted attacks use personalised information to trick recipients into revealing sensitive data or clicking on malicious links. Attackers impersonating trusted individuals to manipulate employees into transferring funds or divulging confidential information is known as Business Email Compromise (BEC). Malware within email messages deliver ransomware, spyware and other malicious software, sometimes laying dormant for months waiting for an opportune time to strike and quietly learning about the vulnerabilities of the infected network. There are also 'Zero-Day' exploits, using new or unknown vulnerabilities in email systems to infiltrate networks. Another strategy is to use Credential Harvesting to lure users to fake login pages, capturing usernames and passwords. The sophisticated and innovative ways that attackers look to compromise organisations continues to grow and evolve.

These threats are compounded by the increasing use of automation, artificial intelligence and machine learning by cyber criminals, enabling them to scale and refine their attacks with unprecedented precision.

In the past, poorly worded emails were a deliberate strategy used to weed out the smart users. Anyone actually responding to these types of email messages were far more likely to fall for the underlying scam. However, with the advent of artificial intelligence, attackers can now craft email messages that will tempt even the smart user.

In response to these escalating threats, email security has advanced significantly. While attackers may use artificial intelligence to craft emails, AI and machine learning on modern email security platforms is also used to detect and mitigate these threats. Machine learning algorithms analyse patterns and behaviours to identify anomalies indicative of phishing, malware or other malicious activities. Many modern email systems use Advanced Threat Protection (ATP) to provide a multi-layered defence. This includes sandboxing to analyse suspicious attachments and URLs, allowing them to detonate in a safe, controlled environment before they reach the end-user.

**Cyber security budgets in the public sector are not always adequate, hindering the adoption of state-of-the-art email security technologies**

There are now multiple email authentication protocols that are essential tools to help keep inboxes safe and ensure the email sender is trustworthy. Protocols such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting and Conformance) help prevent domain spoofing and phishing by validating the authenticity of senders. These protocols are like a security team working behind the scenes to protect email systems from scams and fraud, such as phishing and email spoofing.

Think of SPF as a guest list for your email. It allows the owner of a domain (like example.com) to specify which mail servers are authorised to send emails on their behalf. When someone receives an email claiming to be from example.com, their email server checks the SPF record to confirm that the email came from an authorised source. If it didn't, the email might be flagged as suspicious or sent to the spam folder.

DKIM works like a tamper-proof seal on emails. It uses cryptographic signatures to verify that the email content has not been altered during transit. When an email is sent, DKIM adds a unique digital signature. When the recipient's server gets the email, it verifies this signature against the sender's DKIM record. If the signature doesn't match, the email may be treated as unsafe.

DMARC ties SPF and DKIM together to provide a more comprehensive protection system. It lets domain owners specify how email servers should handle emails that fail SPF or DKIM checks – whether they should be rejected, quarantined or allowed through. DMARC also provides reports to domain owners, helping them to see if anyone is attempting to misuse their domain for fraudulent purposes.

In short, SPF, DKIM and DMARC work together to make email communication more secure and trustworthy by verifying the sender's identity and ensuring that the message hasn't been tampered. For businesses and individuals, setting up these protocols can significantly reduce the risk of cyber attacks and maintain trust in their communications.

**MANY BREACHES WERE CAUSED BY WEAKNESSES IN THE ORGANISATION'S SUPPLY CHAIN**

There is also end-to-end encryption, which ensures that email content remains secure and unaltered during transmission from the sender's device right through to the recipient's inbox, making it inaccessible to unauthorised parties.

Real-Time Threat Intelligence systems now integrate with global threat intelligence networks to identify and respond to emerging threats in real-time. Services like PhishTank or the NZ Government Phishing Protection Service have lists of known active malware/phishing campaigns and nefarious URL links. Email gateways consuming these services can match emails against these lists and delete them.

Of course, the most significant vulnerability is human error. Almost all compromising has been caused by a user clicking on a link or opening an attachment with a malicious payload. Organisations that invest in regular user training and awareness programmes for their employees will go a long way to helping users identify phishing attempts and other email-based threats.

Despite these advances in technologies and protocols, significant challenges still remain, particularly for government businesses. Some of the key issues that exist for government (and other organisations) include: legacy systems, budget challenges, insider threats, supply chain risks and regulatory compliance limitations.

Government organisations will often rely on outdated email platforms that lack modern security features, making them susceptible to advanced attacks. Upgrading or replacing systems can be complex and expensive, particularly if other support systems need to also be upgraded to work with the new modern email system.

Cyber security budgets in the public sector are not always adequate, hindering the adoption of state-of-the-art email security technologies or where budgets are spread too thinly across all attack vectors.

Malicious insiders or negligent/disgruntled employees pose potentially one of the greatest risks. Even the most secure systems are vulnerable if internal actors inadvertently or intentionally compromise email accounts.

Government organisations need to work with third-party vendors who may have weaker email security measures, creating a potential entry point for attackers. Many well-known publicly reported breaches were caused by vulnerabilities in the organisation's supply chain.

USING AI ATTACKERS CAN NOW CRAFT EMAIL MESSAGES THAT WILL TEMPT EVEN SMART USERS

Government organisations must navigate complex regulatory requirements related to data privacy and security. The breadth of services provided by government and the multiple touch points required to service citizens makes for a potentially vast attack surface, this can delay the implementation of necessary security measures. On top of all this, government organisations are attractive to sophisticated attackers backed by nation-states which have the resources to bypass conventional defences, posing a unique and real threat to government email systems. To address these challenges and ensure robust protection for government email systems, there is a need for enhanced measures. A multifaceted approach is essential.

This includes the adoption of Zero-Trust principles that assume no user or device is inherently trustworthy. With strict identity verification, continuous monitoring and limiting of access to a need-to-know basis. Investing in next-generation email security, prioritising the adoption of advanced email security solutions that integrate AI, threat intelligence and real-time analytics to proactively detect and block threats.

A comprehensive employee training programme, evolving beyond basic phishing awareness training should include simulated attacks, real-world scenarios and regular updates on emerging threats. The upgrade of legacy systems to replace outdated email platforms with modern, cloud-based solutions can enhance security while improving scalability and reliability.

Government organisations must enforce stringent email security requirements for third-parties and conduct regular audits to ensure compliance. Understanding that supply chain vulnerability is one of the most likely avenues for compromise.

Developing robust incident response plans and conducting regular drills can minimise the impact of email-based attacks. Collaboration with cyber security agencies and threat intelligence networks is also crucial.

Mandatory use of email authentication protocols such as SPF, DMARC, DKIM and MTA-STS can significantly reduce the risk of phishing and spoofing, as well as provide communication encryption.

Governments must allocate sufficient resources to implement and maintain advanced email security measures. Public-private partnerships can help to bridge funding gaps and provide access to cutting-edge technologies.

In conclusion, email security is an ongoing challenge, especially for government businesses tasked with safeguarding sensitive information and critical infrastructure. While significant progress has been made, evolving threats and persistent vulnerabilities underscore the need for continuous improvement.

By adopting a proactive, multi-layered approach to email security, governments can enhance their resilience against cyber attacks. This includes embracing Zero Trust principles, investing in next-generation technologies and fostering a culture of cyber security awareness. In a world where the stakes are higher than ever, robust email security is not just a necessity, it is a cornerstone of national security ●

**RICHARD BOURNE** is CEO at Liverton Security

**Machine learning algorithms analyse patterns and behaviours to identify anomalies indicative of phishing, malware or other malicious activities**

Picture credit: AdobeStock