Business Email Security Updates Critical to Keep Pace with Emerging Threats

Cyber criminals love email. Everyone uses it. Businesses depend on it. And threat actors successfully use email as an attack vector over and over again. In fact, over 90 percent of malware arrives via email. Hackers have upped their cyber attack strategies, but business email security often lags behind. Organizations must modernize their security practices.

Business Email Security Predictions for 2024

To build an effective defense, security teams need to know the nature of the dangers they face. Experts have identified several key email threats for 2024, including the following:

- More sophisticated phishing attacks – Phishing attacks continue to evolve. Now, with AI, threat actors can make the attacks extremely convincing. Additionally, even hackers with limited skill can purchase phishing kits that contain everything they need to deploy an advanced threat. This includes sophisticated anti-detection tools.
- QR code phishing (quishing) – In addition to malicious hyperlinks and attachments, threat actors send malicious QR codes from seemingly legitimate sources. When victims scan the QR code, it sends them to a spoofed login page or a site that downloads malware.

- New spear phishing techniques – Hackers constantly hone their spear phishing tactics. For instance, in one new technique hackers forward a fake email thread to the target. The email thread appears to include a legitimate conversation between the target's trusted colleague and a representative of another company.
- Malicious use of AI – In addition to creating convincing content, AI also enables threat actors to easily and quickly design and orchestrate attacks. Using machine learning, they can test attacks, almost immediately learning ways through the target organization's defenses.
- Fileless attacks – Instead of downloading a malicious file, emails may contain deceptive links or attachments that trigger an exploit. The attack initiates actions in legitimate programs such as the Windows registry, without downloading any files. Consequently, they bypass traditional antivirus scans and leave no discernable trace.

Strengthen Authentication Methods

Because threat actors use email overwhelmingly as an attack vector, protecting email accounts from compromise plays a critical role in business email security. Begin by automatically enforcing strong passwords.

According to NIST password guidelines, organizations should check user passwords against breached password lists. They should also require a mix of uppercase and lowercase and special characters and prevent the use of repetitive or sequential passwords (for instance '12345678'). Finally, long passwords or passphrases greatly improve password strength.

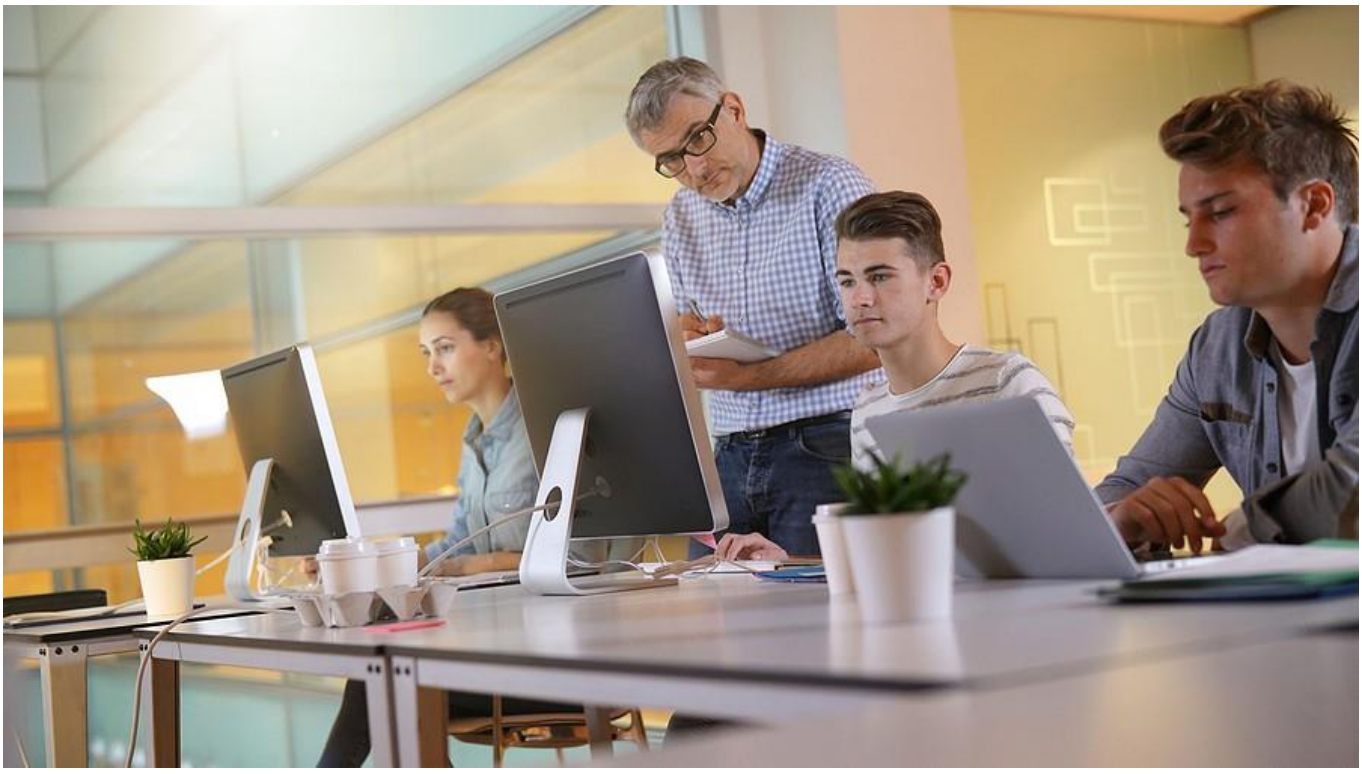
However, even strong passwords will not provide sufficient protection. Organizations should implement multi-factor authentication (MFA) to provide additional verification beyond simply a password.

Prioritize Security Awareness Training for Employees

Cyber criminals use phishing attacks for two reasons. First, they are cheap and require very little manpower to deploy. Second, phishing involves human targets, and humans can be fooled. Thus, security awareness training will always play a key role in email security. But organizations must update their training programs.

Training programs should teach end users to question QR codes, links, and attachments, even from seemingly legitimate senders. They should train users how to verify the legitimacy of the senders, especially if the sender requests money or credentials or if the email contains links or QR codes. In addition to recognizing suspicious emails, users need to know how to report them.

Most importantly, companies should personalize security awareness training to specific teams and individual roles. And they should include immersive experiences such as phishing simulations to engage users and test their understanding.



Update Email Filtering and Enable Authentication Protocols

Email filters detect and block a variety of email-based threats before they reach the end user, from spam to viruses and phishing attacks, including emerging threats. Defense systems should also filter file types commonly used in attacks, as well as URLs and QR codes that lead to potentially malicious websites.

Additionally, organizations should deploy DMARC, DKIM, and SPF. These essential email authentication methods play a key role in preventing email spoofing. And they help to prevent tampering and ensure email integrity.

Upgrade Business Email Security with Expert Help

Email threats grow more persistent and more sophisticated every year. Organizations cannot afford to relax their security stance or depend on last year's security measures to protect against this year's threats.

None of the security measures above will provide sufficient protection on its own. Security teams should build a multi-layered defense that includes automated defenses and also addresses the human factor. AI-powered security tools can strengthen those defenses.

By enlisting the help of email security experts, businesses gain the expertise and the tools they need to mount a modern defense against increasingly complicated threats. The email experts at Messaging Architects work with companies to build defense strategies tailored to business needs and resources.