mimecast

3 Considerations When Deploying Microsoft 365

Don’t move to Microsoft 365 without enhancing your email security

94% OF CYBERATTACKS USE EMAIL

Yet, email remains one of the most critical business applications, making **email security** extremely important. Organizations count on buying a brand-name email application and then expect it to be secure. And while email applications can handle security somewhat well, they cannot handle attacks as effectively as required in today’s dynamic and **sophisticated threat environment**.

There are three important things that IT admins must consider when deploying Microsoft 365:

Security

Microsoft 365 provides basic anti-spam, malware, and spoofing protection. While these foundational protections do work, living in a security monoculture carries tremendous risk. Given the sophistication and relentlessness of cyberattacks, M365 email security is not enough.

Opportunistic attacks

Most cybercriminals look for low-hanging fruit, conducting social engineering attacks, combined with some pretexting, to easily discover whether their targets exhibit strong email security behaviors. Organizations with only “naked” Microsoft 365 security become opportunistic attacks.

Efficacy

Basic Microsoft 365 security stops a lot of spam, malware, ransomware, malicious links, and even impersonation attacks, but IT admins need to be concerned with the threats that are missed and allowed into their organization. Results typically show that far too many of these attacks still slip through Microsoft 365 security.

Microsoft 365, enhanced

Mimecast provides complementary security solutions to Microsoft 365 to help stop threats that are still getting through. IT admins facing pressure to reduce email-based attacks should take the time to read the **Conversational Geek Guide** on **Microsoft 365 Cyber Resilience** to learn how Mimecast can help.