vade

Microsoft 365

The Truth About Microsoft 365 Email Security

Microsoft 365 is the #1 business productivity suite in the world. This makes it a top target for hackers who want to access your sensitive company information stored in Microsoft 365. By breaching a single account via email, hackers can move freely throughout Outlook, SharePoint, OneDrive, and Teams. Hackers can copy, download, and share files, and conduct additional attacks within the system.

According to Ponemon Institute, 60 percent of SMBs experienced a cyberattack in 2020, and 48 percent reported being a victim of phishing/social engineering. As so many SMBs experienced in 2020, an ineffective solution can have major consequences on business:

48%
SMBs reported being a victim of phishing [1]

$5,600
Average ransomware payment [2]

$274,000
Average cost of downtime [3]

51%
SMBs reported malware evaded detection systems [4]

Phishing is an email scam that impersonates a brand both in an email and on a webpage. It tricks a user into visiting a fraudulent website and divulging their account credentials.

Spear Phishing is an email that impersonates a colleague or other acquaintance with the goal of tricking the recipient into scheduling a wire transfer, buying gift cards, or changing bank account information.

Malware is malicious software designed to compromise a computer or device, including corrupting or stealing data, damaging devices, and reproducing itself to infect other computers and/or devices.

Ransomware is malicious software that locks down a computer. It triggers an on-screen ransom demand instructing the victim to pay a specified amount of Bitcoin to regain access to their computer, or else face data destruction or leaks.

Microsoft 365 Email Attacks

Dynamic, highly targeted threats – In 2019 alone, hackers created more than 64,331 phishing webpages impersonating Microsoft login pages. Designed to steal account login credentials, phishing is just one type of email threat facing businesses that use Microsoft 365.

1 Ponemon Institute. "2020 Cybersecurity in the Remote Work Era: A Global Risk Report"
2 Datto. "Datto State of Ransomware Report 2020"
3 Ibid.
4 Ponemon Institute. "2020 Cybersecurity in the Remote Work Era: A Global Risk Report.".

Microsoft 365's Built-In Security (EOP)

Although Microsoft 365 comes equipped with Exchange Online Protection (EOP), Microsoft's built-in email security for Microsoft 365, it's known to have issues detecting sophisticated email attacks. During testing, EOP fared poorly in critical categories:

Protection Rating	Detection Rate	Total Accuracy Rating [5]
-17%	73%	29%

To identify phishing and malware, EOP scans an email for identifiable characteristics of a previously detected email threat.

- **IP addresses** known to send spam or phishing emails.
- **Domains** known to host malicious websites or pages.
- **Attachments** with known malware/ransomware code.

To identify spear phishing, EOP scans for exact domain spoofing — a replica email address of a legitimate company.

However, EOP is ineffective at recognizing other forms of email spoofing in spear phishing emails:

- **Close cousin email addresses** are similar but not identical to legitimate emails: microsoft.com.company
- **Display name spoofing** masks the sender's email address and shows their chosen display name, such as a variation on a brand's email address or name: microsoftsecurity.com

Vade for M365

Protecting Microsoft 365 requires additional email security. A solution that works with EOP gives you the built-in protection of EOP, along with an added layer of security to make up for its shortcomings. **Vade for M365 blocks advanced attacks** from the first email thanks to **machine learning** algorithms and heuristics that perform **real-time behavioral analysis** of the entire email, including any URLs and attachments.

Multi-faceted anti-phishing performs a real-time, multi-layered behavioral analysis of the email and URL.

Banner-based anti-spear phishing triggers a warning message if an email is suspected to be spear phishing.

Behavioral-based anti-malware looks beyond known threats and scans attachments and code for behavioral signs of malware/ransomware viruses.

Auto- and one-click remediation removes email threats that have been delivered to user inboxes, both automatically and via one-click remediation.

Ask me about Vade for M365

5 SE Labs. "Email Security Services Protection." December 2020.