mbc
MANAGED IT SERVICES

Advanced Threat Protection

WHAT IS IT?

Advanced Threat Protection (ATP)
Protects your email, files, and Office 365 applications against unknown and sophisticated attacks.

HOW CAN IT AFFECT YOUR BUSINESS?

Microsoft Office 365 Advanced Threat Protection (ATP) is a cloud-based email filtering service that helps protect your organization against unknown malware and viruses by providing robust zero-day protection. It includes features to safeguard your organization from harmful links in real time.
Traditional solutions like signature-based anti-virus might catch the known threats but cannot protect against unknown zero-day threats. This is where Advanced Threat Protection comes in to protect email.

Context is Key: Safe Attachments: Using Safe Attachments, Office 365 ATP protects against unsafe attachments and provides you with a malware-free, cleaner inbox.

Safe Links: Office 365 ATP blocks users from clicking on unsafe links. If a link they click on is unsafe, the user is either informed that the site's been blocked, or warned not to visit it. The protection remains every time they click the link, as malicious links are dynamically blocked while good links can be accessed.

Spoof intelligence: Spoof intelligence detects when a sender appears to be sending mail on behalf of one or more user accounts within one of your organization's domains. It enables you to review all senders who are spoofing your domain, and then choose to allow the sender to continue or block the sender. Spoof intelligence is available in the Security & Compliance Center on the Anti-spam settings page.

Always verify and validate: Spoof intelligence detects when a sender appears to be sending mail on behalf of one or more user accounts within one of your organization's domains. It enables you to review all senders who are spoofing your domain, and then choose to allow the sender to continue or block the sender. Spoof intelligence is available in the Security & Compliance Center on the Anti-spam settings page.

Quarantine: Messages identified by the Office 365 service as spam, bulk mail, phishing mail, containing malware, or because they matched a mail flow rule can be sent to quarantine. By default, Office 365 sends phishing messages and messages containing malware directly to quarantine. Authorized users can review, delete, or manage email messages sent to quarantine.

Ask you MBC account representative to make sure that the feature is active in your engagement.