What is Microsoft Defender / Advanced Threat Protection?

What is Microsoft Defender / Advanced Threat Protection?

Dynamic Computing has implemented Microsoft's Advanced Threat Protection (ATP) service as part of our ongoing cyber security initiative to protect your network, infrastructure, and clients from malware and unsafe links, such as those that have appeared in recent phishing scam emails. ATP analyzes incoming email and blocks malware and unsafe links.

How does Defender/ATP work?

ATP provides two-part protection: Safe Links and Safe Attachments.

- **Safe Links:** This feature proactively protects against malicious hyperlinks in an email message. A banner appears across the top of the email stating that the email is likely to be Junk or contain phishing content. When a malicious link is clicked the protection dynamically blocks the content, while good links can be accessed. If a link is found to lead to a malicious web site, a warning will be displayed instead of the website. This service does not guarantee that all links which are scanned are safe but does guard against many known unsafe sites and is continually updated with new information about malicious sites.
- **Safe Attachments:** This feature checks email message attachments for malware and viruses. If an attachment is found to contain malicious content, the email is not delivered, and the sender is notified.

If you receive an email with possible malicious content, you would see a banner across the top of the message. Links within emails will be re-written and will look like this when hovering over them with your mouse: https://...safelinks.protection.outlook.com.../ .

All email attachments are scanned upon delivery before being accessible by the user. You may sometimes see an "ATP scan in progress" file as a placeholder for the actual attachment. After a few minutes, the email will automatically populate with the file if it passes security checks.

Cyber attacks are becoming more and more sophisticated and ATP will reduce the likelihood that employees will become the victims of phishing scams or malware/virus infestations. Office 365 is a cloud-based platform that Microsoft continues to improve, and they will continually update the detection functions within ATP, which will help to protect users from future threats. As with all malicious content detection systems, while greatly reducing attacks, there is the possibility for newer attacks to come through the system and not be flagged. Continue to be diligent when opening attachments or entering passwords or sensitive information on the Internet.

Please contact Dynamic Computing if you suspect that ATP may be blocking

legitimate links or attachments.

The Support Team
Dynamic Computing, Inc.

1011 Western Avenue, Suite 920 | Seattle, Washington 98104
Main: (206) 284·6200 | Toll Free: (855) 284·6200
service@dyncomputing.com

Custom Fields

- **Article Status:** Specialist Reviewed
