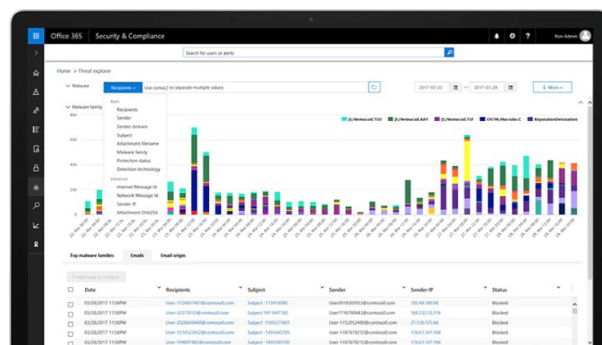


Microsoft Defender for 365

Microsoft Defender for 365 is an enhancement to the standard email filtering and security that comes with Microsoft 365. It gives much greater protection against malicious attacks and the latest threats that can be delivered via email or collaboration tools.

Defender for Microsoft 365 reduces the risk of attacks that use malicious links intended to collect usernames and passwords, to direct you to sites hosting malware, or that have attached documents actually containing malware.

Microsoft Defender for 365 will scan both incoming and outgoing emails as well as emails already in a users mailbox. The system will also scan existing and new cloud stored files in SharePoint, Teams and OneDrive to ensure they are safe. Where an email is identified as being 'malicious' the message will be moved to Quarantine. Users will receive a daily email to review these messages so they can review/release/block the emails as appropriate. Any files that are found to be containing malicious content will also be blocked from opening or downloading. Providing peace of mind that users are protected from malicious email content.



Economic impact study of Defender for Microsoft 365 capabilities (by Forrester Research)

- 528** Security events eliminated annually by organisations surveyed
- 60%** Reduced likelihood of a security breach
- 186%** Return on investment

Configuration, protection, and detection capabilities



Safe attachments



Safe links



ATP for Teams,
OneDrive, and
SharePoint



Anti-phishing



Safe attachments

Safe attachments gives an extra layer of protection for email attachments, in addition to being scanned by anti-malware protection in Exchange Online, Defender uses a virtual environment to open and check attachments in email messages before they're delivered to recipients to find any potential threats hidden inside, (this process is referred to as detonation.) Giving peace of mind to users that email attachments have been double checked to ensure they are not malicious.



Safe links

Safe links analyses links in emails and office documents by redirecting the link to a secure server in the Microsoft 365 environment, the server then checks the link against a list of known malicious web sites, if the server identifies the link as malicious the user is blocked from accessing the site and is shown a warning page to let them know. If the site is 'safe' the users is taken to the original link destination.

Both safe links and safe attachments apply to internal and external emails in real-time.



ATP for Teams, OneDrive, and SharePoint

With Microsoft Defender for 365 you are also protected within SharePoint, OneDrive, and Microsoft Teams. ATP (Advanced Threat Protection) for SharePoint, OneDrive, and Teams helps detect and block existing files that are identified as malicious in team sites and document libraries by locking them and preventing users from accessing them.



Anti-phishing

Microsoft Defender for 365 helps prevent phishing attacks by utilising 'spoof protection' and 'mailbox intelligence' for all recipients. It protects against phishing emails by preventing internal or external email addresses from being impersonated. Spoof protection ensures that senders are who they say they are by checking the displayed 'From' address actually matches the domain the email came from. Mailbox Intelligence uses artificial intelligence (AI) to learn who a user frequently communicates with via email, and creates a map of common communication, to allow Defender to determine the risk an email poses before applying quarantine actions.

Find out more

ramsac can assist organisations with deploying Microsoft Defender for 365. For more information, speak to your relationship manager:

Call: **01483 412 040**

Email: **info@ramsac.com**

Visit: **www.ramsac.com**