HOW TO SETUP MICROSOFT 365 ADVANCED THREAT PROTECTION

A SIMPLE GUIDE BY DIAL A GEEK

Company reg no: 07550944
VAT: GB 110 5614 54

OVERVIEW

Working out how to set up Microsoft 365 Advanced Threat Protection is one of the most effective ways to protect your business from email-based cyber attacks.

This is vital. Because phishing is the most common type of cyber crime. Email impersonation and spoofing, CEO fraud, malware delivered through dodgy links and the like – all types of email-based cyber attacks – are also on the rise.

WHAT LICENCES DO I NEED TO ENABLE ATP?

To be able to activate Microsoft 365 Advanced Threat Protection, you need to have:

- Microsoft Defender for Office 365
- Microsoft 365 Business Premium
- Office 365 E5 or Microsoft 365 E5

If you don't have one of these, you will need to talk it over with your Managed Service Provider or internal IT department.

HOW TO - STEP BY STEP

I Sign in to your Threat Management Policy

1. Start a private or “incognito” browsing session
2. Go to https://protection.office.com/homepage
3. Use your global admin credentials to sign in
4. Navigate to Threat Management > Policy

II Turn on Microsoft 365 ATP Safe Attachments

1. Navigate to ATP Safe Attachments
2. Find the checkbox labelled Turn on ATP for SharePoint, OneDrive, and Microsoft Teams
3. Tick it to enable it
4. The create a new policy by clicking on the “+” symbol
5. On your settings, you should see a list of options with options of “off”, “monitor”, “block”, “replace”, and “dynamic delivery”

III Decide how restrictive your policy is going to be

1. Choose a restrictive policy – select ‘block’.

OR

1. Choose a less restrictive policy – select ‘replace’. Then click Enable redirect and enter the email address of the person you want to receive the ticket (usually your IT team).
2. Then, after you have chosen, find the checkbox labelled Apply the above selection if malware scanning for attachments times out or error occurs
3. Tick it to enable it
4. In the section that asks you to create a “recipient based rule”, choose If the recipient domain is
5. Click Save.
6. Wait for the changes to apply. This can be almost instant or take a few minutes.

IV Activate the Microsoft 365 ATP Safe Links feature

1. Navigate to ATP Safe Links
2. Double-click on Default
3. A pop-up window should open
4. You should then be able to spot a line of checkboxes labelled:

- Microsoft 365 Apps, Office for iOS and Android
- Do not track when users click safe links
- Do not let users click through safe links to original URL

Tick to enable all of those. Then click Save.

V Enable ATP Anti-phishing

Finally, let's enable some anti-phishing protection. This is quite a lot of actions, so buckle up!

1. Navigate to Anti-phishing > Default policy > Impersonation
2. Click Edit
3. Turn the button to On
4. Add all of your users. To do this, click Add user and enter the email address of an account you want to protect. You will need to do this individually for each user.
5. Click Save

Next up, domains and actions:

1. Navigate to Add domains to protect
2. Spot the buttons labelled Automatically include the domains I own and Include custom domains
3. Turn those both On
4. Click Actions
5. In the Actions section, spot the options labelled If email is sent by an impersonated user and If email is sent by an impersonated domain
6. Set both of those drop-down lists to Move message to the recipients' Junk Email folders
7. Below those, you should see a link that says Turn on impersonation safety tips
8. Click on it

9. Spot the three switches labelled Show tip for impersonated users, Show tip for impersonated domains, and Show tip for unusual characters
10. Turn all three of those On
11. Click Save

Phew! Now we're getting there. Just one thing still to do – Mailbox Intelligence:

1. Navigate to Mailbox Intelligence
2. Spot the buttons labelled Enable mailbox intelligence and Enable mailbox intelligence based impersonation protection
3. Turn those both On
4. Below that, you will see an option labelled If email is sent by an impersonated user
5. Choose Move message to the recipients' Junk Email folder in that drop-down list
6. There should be an option to Review your settings. Go ahead and do that.
7. If everything looks correct, click Save
8. Then click Close

We hope you found our guide helpful.

If you need any further help, get in touch!

help@dialageek.co.uk
0117 369 4335
www.dialageek.co.uk

DIAL A GEEK

DANIEL LEONARD
Carbometrics

Dial A Geek's dedication is evident in every interaction, making them not just a service provider but a partner in our technological growth.

Certified B Corporation
CYBER ESSENTIALS
IASME CYBER ASSURANCE LEVEL TWO
Company reg no: 07550944
VAT: GB 110 5614 54