



MICROSOFT DEFENDER SET UP QUICK GUIDE



SYSTEMAGIC
DOING IT DIFFERENTLY

Purchase Microsoft Defender for Office 365 **(Plan 1)** for Standard/basic or exchange licences



Configure the following after logging into as 365 admin:

- Anti-Phishing - <https://protection.office.com/antiphishing>
- Create new Policy
- Apply to Recipient domain



SYSTEMAGIC
DOING IT DIFFERENTLY



Once policy created **edit** the following options:

Antiphish Policy

↑ Increase Priority ↓ Decrease Priority

Delete policy

Priority	0	
Status	On	
Last modified	7 September 2020	

Policy setting	Policy name	Antiphish Policy
	Description	
	Applied to	If the recipient domain is: bathspadentistry.com

Impersonation	Users to protect	On - 6 User(s) specified
	Protect all domains I own	On
	Protect specific domains	Off
	Action > User impersonation	Move message to the recipients' Junk Email folders
	Action > Domain impersonation	Move message to the recipients' Junk Email folders
	Safety tips > User impersonation	On
	Safety tips > Domain impersonation	On
	Safety tips > Unusual characters	On
	Mailbox intelligence	On
	Mailbox intelligence > Protection	On
	Mailbox intelligence > Action	Move message to the recipients' Junk Email folders

Spoof	Enable Spoof Intelligence	On
	Enable Unauthenticated Sender Feature	On
	Action	Move message to the recipients' Junk Email folders

Advanced settings	Advanced phishing thresholds	1 - Standard
-------------------	------------------------------	--------------



SYSTEMAGIC
DOING IT DIFFERENTLY

3.

Safe Attachments - <https://protection.office.com/safeattachment>

- Turn on ATP for SharePoint, OneDrive, and Microsoft Teams
- Create New Policy
- Set to Block any emails with detected malware
- Apply to Recipient domain

Safe Links -

<https://protection.office.com/safelinksv2>

- Create a new policy
- Give it a name
- Select the domains to protect