Office 365 Microsoft

Organization:

We’re extending coverage of enhanced anti-spoofing protection to all Exchange Online organizations

Major update: General Availability rollout started

Applied to: All customers

We’re excited to announce that we’re extending enhanced anti-spoofing capabilities to all Exchange Online Protection (EOP) organizations. Previously, this feature was only available to E5 and Advanced Threat Protection (ATP) add-on organizations.

If you are an existing E5/ATP customer, then this feature was previously enabled for you. We continue to add additional updates to improve this filter, including a new spoof intelligence insight that is being rolled out to provide better visibility and review experience.

If you have previously disabled enhanced anti-spoofing in your anti-phishing policy or via customer support, you will not be impacted.

This message is associated with Office 365 Roadmap ID: 32820.

[How does this affect me?]
After this change takes place, your organization will have access to enhanced anti-spoofing functionality that utilizes cloud intelligence, sender reputation and patterns to identify potentially malicious domain spoofing attempts. The new functionality works in conjunction with existing standards based email authentication checks (DMARC/DKIM/SPF). Once this feature is enabled, messages that fail our extended implicit authentication checks will be automatically sent to the junk mail folder. You can use policies to customize these actions and turn this functionality on and off.

We are also updating the Get/Set-PhishFilterPolicy cmdlet to allow you to block/allow domains that are allowed to send spoofed mails, as well as the Get/Set-AntiphishPolicy cmdlet to let you modify the policies applied to spoofed messages. After the cmdlet changes, we will also roll out policy options in Security and Compliance center

If you have domain ‘allow’ or ‘safe’ sender policies or transport rules in place, they will not be impacted.

Policy options for these changes will be available after September 1. We’ll begin rolling this out and will be enforcing changes after September 21, 2018. We anticipate rollout completion in the following weeks.

[What do I need to do to prepare for this change?]
If you wish to disable enhanced anti-spoofing functionality, you will need to set polices before September 21, 2018. After September 21, we will begin rolling this feature out worldwide, and will enforce the available settings.

To access settings and make changes you’ll need to use Get/set-Antiphishpolicy PowerShell cmdlets (after September 1). The same will also be possible via the Security and Compliance Center (under Threat Management->Policy->Anti-Phishing) once those changes are rolled out for EOP.

Please click Additional Information to learn more about how anti-spoofing functionality can benefit your organization and to learn how to access settings to enable and disable this feature.

Sign in to the Office 365 Admin center to use the links below:

View this message in the Office 365 message center