Preventative Measures: Marking External Emails

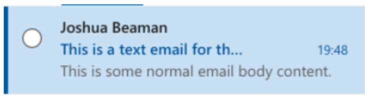
Blue Team Level 1 Certification (Standard) > PA6) Taking Defensive Actions > Preventative Mea... IN PROGRESS

Employees must understand the risk of external emails. Although they could be legitimate from entities such as customers, employee personal email addresses, vendors, suppliers, and potential clients – the majority of phishing emails will come from external addresses. In platforms such as Microsoft Exchange or Office365 there is the ability to alter the subject line or body text of an email address that is coming into the organization as to alert the recipient that this email isn't an internal communication, and could potentially be malicious. This simple warning can make employees think twice about interacting with an external email, such as opening an attachment or clicking on a hyperlink.

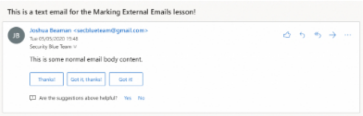
A good idea is to apply a rule where any email coming from an external sender into the organization has the subject line appended with a very short message, such as "[EXTERNAL]" or "[EXT]".

EXAMPLE WALKTHROUGH

To quickly show you what email marking looks like, this example will show us setting up a rule on our Security Blue Team email addresses within Office 365. Here's what an email looks like coming from an external source **without** any rules being used.



Joshua Beaman
This is a text email for th... 19:48
This is some normal email body content.

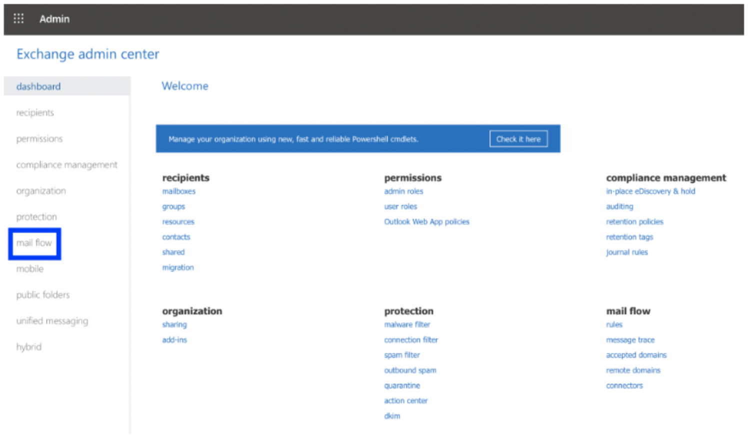


This is a text email for the Marking External Emails lesson!

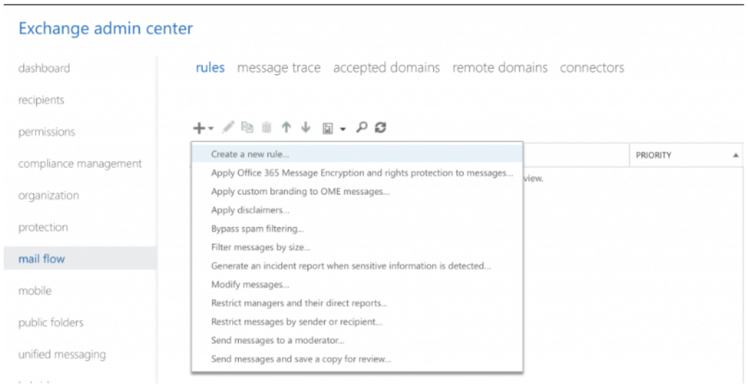
Joshua Beaman <secblueteam@gmail.com>
Tue 05/05/2020 19:48
Security Blue Team

This is some normal email body content.

To implement a rule, we'll head over to the Exchange admin center and click on mail flow on the left-hand menu.



From here we're able to create email rules. We will click the "+" icon, and select "Create a new rule...".



Exchange admin center

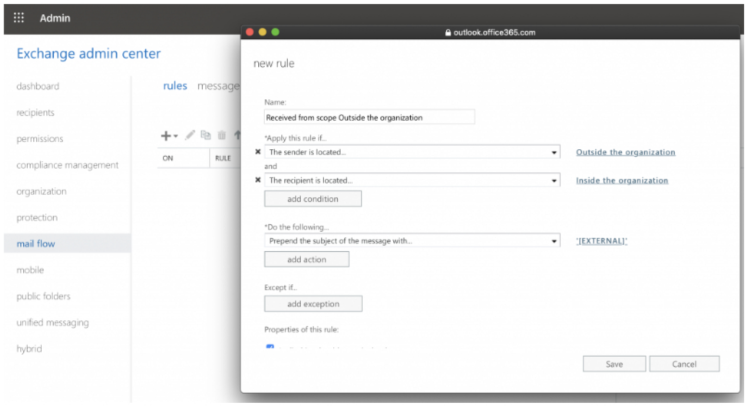
dashboard
recipients
permissions
compliance management
organization
protection
mail flow
mobile
public folders
unified messaging
rules
message trace
accepted domains
remote domains
connectors
PRIORITY
view.
Create a new rule...
Apply Office 365 Message Encryption and rights protection to messages...
Apply custom branding to OME messages...
Apply disclaimers...
Bypass spam filtering...
Filter messages by size...
Generate an incident report when sensitive information is detected...
Modify messages...
Restrict managers and their direct reports...
Restrict messages by sender or recipient...
Send messages to a moderator...
Send messages and save a copy for review...

In the below screenshot, we have named our rule "Received from scope Outside the organization". The rule is applied if:

- The sender is outside the organization (securityblue.team domain)
- AND the recipient is inside the organisation

If these two conditions are met (which will always occur when an external email is delivered to a @securityblue.team mailbox) the following action will be taken:

- Prepend the subject of the message with "[EXTERNAL]"



Name:
Received from scope Outside the organization

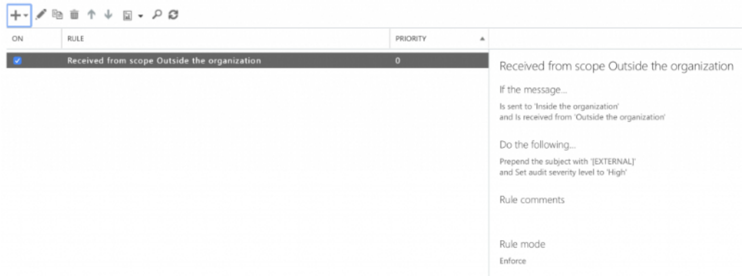
*Apply this rule if...
✖ The sender is located... Outside the organization
and
✖ The recipient is located... Inside the organization

*Do the following...
Prepend the subject of the message with... '[EXTERNAL]'

Except if...

Properties of this rule:

You can see the completed rule below on the right-hand side.



ON	RULE	PRIORITY
☑	Received from scope Outside the organization	0

Received from scope Outside the organization

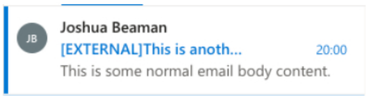
If the message...
Is sent to 'Inside the organization'
and Is received from 'Outside the organization'

Do the following...
Prepend the subject with '[EXTERNAL]'
and Set audit severity level to 'High'

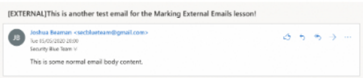
Rule comments

Rule mode
Enforce

So now if we send another email to our @securityblue.team mailbox from our Gmail address, we can see that the email is now being marked!



Joshua Beaman
[EXTERNAL]This is anoth... 20:00
This is some normal email body content.



[EXTERNAL]This is another test email for the Marking External Emails lesson!
Joshua Beaman <secblueteam@gmail.com>
Tue 05/05/2020 20:00
Security Blue Team ✓
This is some normal email body content.

The same method can be applied to automatically add warning messages to the start of the body content instead of (or as well as) appending the subject line, and styling can be applied such as making the text red so it stands out more, and means the employee is more likely to read it and proceed with caution.

10 Topics | 2 Quizzes

BTL1 EXAM

○ Exam Preparation

○ Using RDP and SSH

○ How to Start Your Exam

Previous Topic

Mark Complete ✓

Next Topic

Back to Lesson