



# How to Strengthen M365 Exchange Online Configurations



© Black Hills Information Security | @BHinfoSecurity



# Exchange Online



- [admin.exchange.microsoft.com](https://admin.exchange.microsoft.com)
- Some\* Security Considerations:
  - Mail flow/transport rules
  - Direct Send
  - Sending Directly



© Black Hills Information Security | @BHinfoSecurity



# Exchange Mail Flow Rules



- Where are we?

The screenshot displays the Exchange Admin Center (EAC) interface. On the left, the navigation pane shows the 'Mail flow' section highlighted with a red box. Below it, the 'Rules' link is also highlighted with a red box and a red arrow pointing to the 'Add a rule' button in the main content area. The main content area shows the 'Rules' page with a yellow warning banner at the top. Below the banner, the 'Rules' section title is followed by a description and a 'Learn more about' link. At the bottom, a list of rules is displayed, including 'Create a new rule', 'Apply Office 365 Message Encryption and rights protection to messages', 'Apply custom branding to OME messages', 'Apply disclaimers', 'Filter messages by size', 'Modify messages', 'Restrict managers and their direct reports', 'Restrict messages by sender or recipient', and 'Send messages to a moderator'.





- 

© Black Hills Information Security | @BHInfoSecurity

# Set rule conditions

**Required**

Name and set conditions for your transport rule

Name \*

Apply this rule if \*

Do the following \*

Except if

**Optional**

**Add more conditions**

The screenshot shows the 'Set rule conditions' window in Microsoft Exchange. It has a title bar and a main content area. The content area is divided into sections for naming the rule and setting conditions. The 'Name' field is required. The 'Apply this rule if' section has three conditions, each with a dropdown menu and a plus icon to add more conditions. The 'Do the following' section has a dropdown menu. The 'Except if' section has a dropdown menu. Red annotations highlight the 'Required' fields (Name, Apply this rule if, Do the following) and the 'Optional' fields (Except if). A red box labeled 'Add more conditions' points to the plus icons in the 'Apply this rule if' section.



# Rule Settings



## Test

Conditions Settings

Rule  
Name

Priority \*

0

Rule mode

- ☒ Enforce
- ☐ Test with Policy Tips
- ☐ Test without Policy Tips

Severity \*

Not specified

Conditions  
vs Settings

☐ Activate this rule on

7/27/2025



-

2:00 PM



☐ Deactivate this rule on

7/27/2025



-

2:00 PM



☒ Stop processing more rules



© Black Hills Information Security | @BHinfoSecurity



# Rule Flow



- Top starting at priority 0 through last rule
- Rules applied in order and additive
- One rule may bypass all remaining rules
  - Makes sense in certain cases, like a block.



Stop processing more rules



© Black Hills Information Security | @BHinfoSecurity



# Creating “Good” Rules



- Consider scope - be very specific
  - IP Address AND Domain name
  - IP Address AND x-header (Common for 3<sup>rd</sup> party phishing products)
- Don't be generic
  - Only email, only domain, only specific text
  - Don't reduce spam (SCL) level on only one point of identification
- Follow logic flow of rule - Apply/Do the following/Except if
  - Think of edge cases
  - Allow multiple admins/security personnel to review mail flow rule





# Rule Example - Conditions vs Description



## External Header

Name \*

External Header

Apply this rule if \*

The sender

is external/internal

The sender is located 'NotInOrganization'

Do the following \*

Prepend the subject of th...

specified prefix

Prepend the subject of the message with '[EXTERNAL]'

## Rule description

Apply this rule if

*Is received from 'Outside the organization'*

Do the following

*Prepend the subject with '[EXTERNAL]'*  
*and Stop processing more rules*



Black Hills Information Security, LLC. All rights reserved.



# Rule Function - Message Sent to Organization



Will you be at the webcast?

- Lily Sends:

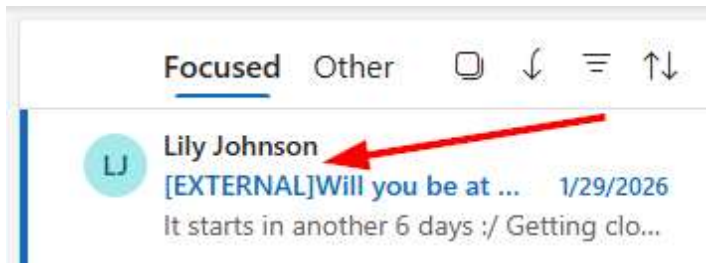
☰ Summarize this email



**Lily Johnson** <[REDACTED]@gmail.com>  
to AdeleV ▾

It starts in another 6 days :/ Getting close!

- Adele Sees:



- Adele Replies

**Adele Vance**

to me ▾

Yep! I plan to be there.

**From:** Lily Johnson <[REDACTED]@gmail.com>

**Sent:** Thursday, January 29, 2026 10:47 AM

**To:** Adele Vance <AdeleV@defendingazure.onmicrosoft.com>

**Subject:** [EXTERNAL]Will you be at the webcast?

...



© Black Hills Information Security | @BHinfoSecurity



# Reply to email chain and...



- Lily Replies:



**Lily Johnson**

to Adele ▼

What time does it start?

- Adele gets 2  
[EXTERNAL]  
Headers

[EXTERNAL]Re: [EXTERNAL]Will you be at the webcast?



**Lily Johnson** <lilyjohnson7689@gmail.com>

To: ☒ Adele Vance

What time does it start?

...

Not sure yet.

I am not sure yet.

Here is the schedule.





# Microsoft's Solution! (Sort of)



- <https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/disclaimers-signatures-footers-or-headers>
- **Except if:** To add an exception that prevents multiple disclaimers from being added in an email conversation, configure the following settings:
  - Select **The subject or body** and **Subject or body matches these text patterns**.
  - In the **Specify words or phrases** flyout that opens, enter the words or phrases in the disclaimer, select **Add**, and then select **Save**.

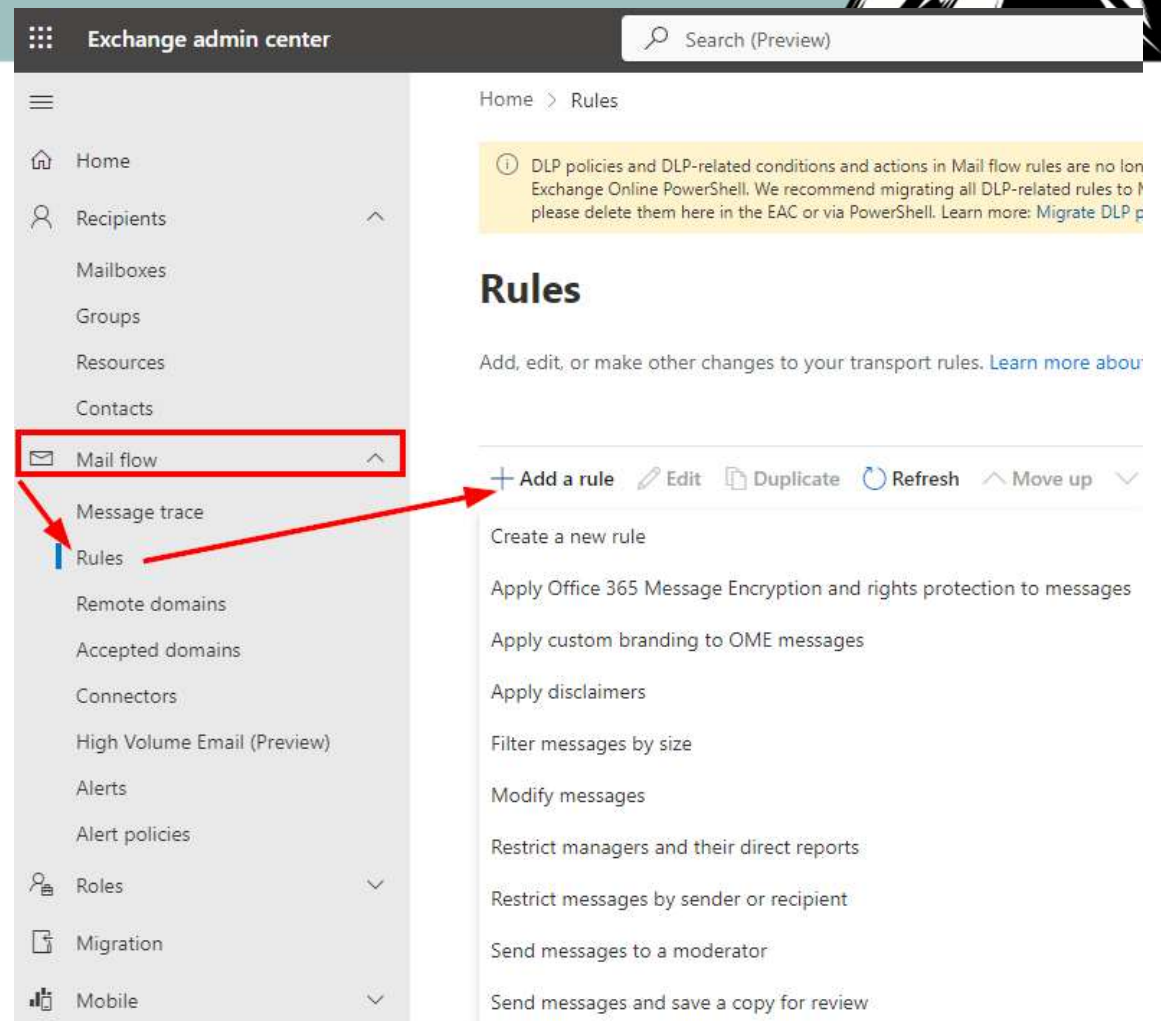
When you're finished, select **Next**.



© Black Hills Information Security | @BHinfoSecurity



# Mail Rule vs Disclaimer



Exchange admin center

Search (Preview)

Home > Rules

DLP policies and DLP-related conditions and actions in Mail flow rules are no longer supported in Exchange Online PowerShell. We recommend migrating all DLP-related rules to Exchange Online PowerShell. Learn more: [Migrate DLP policies](#)

## Rules

Add, edit, or make other changes to your transport rules. [Learn more about rules](#)

[+ Add a rule](#) [Edit](#) [Duplicate](#) [Refresh](#) [Move up](#)

Create a new rule

- Apply Office 365 Message Encryption and rights protection to messages
- Apply custom branding to OME messages
- Apply disclaimers
- Filter messages by size
- 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





# Modify Original Rule



- Added “Except if”
  - Subject OR body includes.

## External Header

Apply this rule if ^

The sender

is external/internal



The sender is located 'NotInOrganization'



Do the following \*

Prepend the subject of th...

specified prefix



Prepend the subject of the message with '[EXTERNAL]'



Except if

The subject or body

subject or body includes ...



The subject or body includes any of these words '[EXTERNAL]'



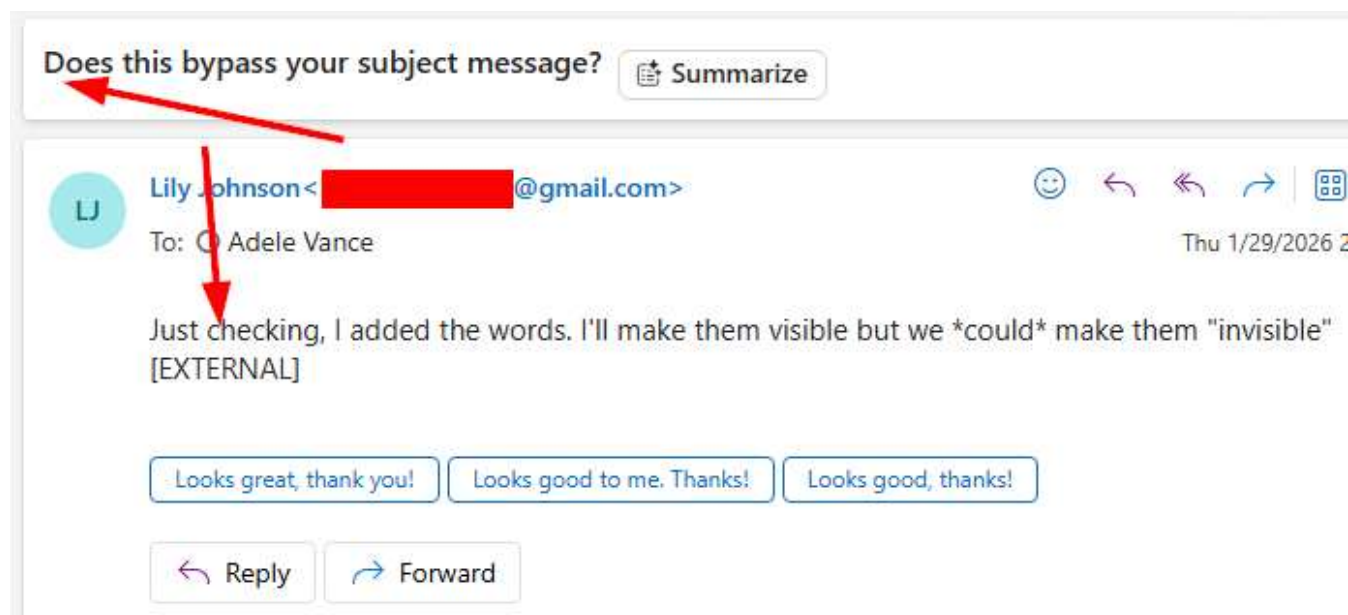
© Black Hills Information Security | @BHinfoSecurity



# New message “Bypassing” Subject Rule



- Can be done with body warning messages too!
- `<div style="color: white; background-color: white; padding: 10px; font-weight: bold; font-family: Arial, sans-serif;">`
- [EXTERNAL]
- `</div>`





# Common Rule Issues



- Bypasses (Spam/Attachment/Scanner)

- TO user (Specific user X)

- FROM user

- **Example:**

- [helpdesk@companyname.tld](mailto:helpdesk@companyname.tld)
      - [support@companyname.tld](mailto:support@companyname.tld)
      - [noreply@companyname.tld](mailto:noreply@companyname.tld)
      - [no-reply@companyname.tld](mailto:no-reply@companyname.tld)
      - [noreply@email.teams.microsoft.com](mailto:noreply@email.teams.microsoft.com)
      - [support@companyname.atlassian.net](mailto:support@companyname.atlassian.net)
      - [notification@slack.com](mailto:notification@slack.com)
      - -Known 3<sup>rd</sup> party phishing company sites
        - Example follows

- FROM Domain

- subsidiary, trusted 3<sup>rd</sup> parties, etc

- X-HEADER-VALUE

- Examples Follow

- Warning Banner / Disclaimers

- Previous Example

- Additional Example:

- Subject contains "Jira"
      - Body contains company body email header and/or footer





# Phishing Products



- Potential ProofPoint Examples:
- \*Most (all?) products request you allow by IP now.
- KnowBe4 Examples:

Online-banking.kb4.io,  
En-us.secureconnection.moneytransaction.kb4.io,  
Mail.kb4.io,  
Breakingnews.comano.us,  
Secure-mail.web.magnetronics.com,  
Socialmedia-insights.bloemlight.com,  
Messaging-security.comano.us,

© Black Hills Information Security | @BHinfoSecurity



exch01-corp.com  
facebook-login.com  
firstfedtrust.com  
flightstatalert.com  
freeenergypress.com  
fundingsource.services  
goggl.cc  
gotwebinar.online  
gov-online.net  
gov-services.com  
greetingsweb.com  
grnail.world  
hpdocument.com  
informedvoterleague.com  
info-week.net  
info-week.us  
instagramn.net  
internalitsupport.com  
investmentsecureportal.com  
itnues.net  
lesportsacxx53.com

paypal-rogm.com  
pharmamedsonline.com  
pharmlink.in  
phishingtraining.com  
pipelinenews.net  
postcardfast.com  
prnewsnet.us  
publicemailservice.com  
qqoffi55.cc  
qqoffi55.com  
qquio.com  
ransomware.site  
register-now.world  
rwebfix.com  
saleslinkforce.com  
salesteamlink.com  
scandeviceservices.com  
sec-10k.com  
securebankingsevices.com  
securelogin-wallet.com  
securityeducation.com  
self-care.co



# X-Header Bypass Examples



- X-PHISHTEST = KnowBe4
- x-salesforce\_custom\_header = true
- X-MS-Exchange-Organization-SkipSafeLinksProcessing = 1
- x-psat\_header = true
- X-MS-Exchange-MeetingForward-Message = Forward
- X-Mimecast-Spam-Score \*Contains\* - or 0 or 1 or 2





## X-Header Example - 2



- You should set custom headers for Phishing products
- If the header is not changed - can use the default headers to bypass mail rules
- Code to use example:  
`$email.Headers.Add("X-PHISHTEST", "KnowBe4")`

Name \*

Bypass Clutter and Spam Filtering by Email Header

Apply this rule if \*

The message headers...



includes any of these words

'X-PHISHTEST' message header includes 'KnowBe4'

Do the following \*

Modify the message properties



set the spam confidence level (SCL)

Set the spam confidence level (SCL) to '-1'

- <https://support.knowbe4.com/hc/en-us/articles/212723707-Whitelist-by-Email-Headers-in-Microsoft-365-Microsoft-Exchange-2016-and-Microsoft-Exchange-2019>



© Black Hills Information Security | @BHinfoSecurity



# Direct Send



- Used by IoT and multi-function devices like printers
- Send-MailMessage -SmtpServer somedomain-tld.mail.protection.outlook.com -To someuser@somedomain.com -From ITSupport@somedomain.com -Subject “are you vulnerable” -Body “Do you see this text...” -BodyAsHTML
- <https://www.blackhillsinfosec.com/spoofing-microsoft-365-like-its-1995/>
- <https://www.blackhillsinfosec.com/spamming-microsoft-365-like-its-1995/>

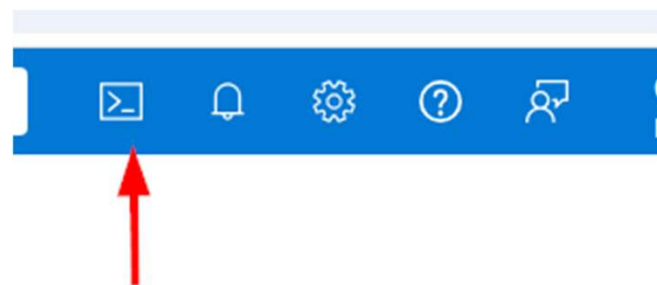




# Direct Send



- Easy to self-test
- I typically use a Cloud Shell to send these messages (Shown Left)
- Sometimes blocked due to previous cloudshell users (Spam) - Example Below



**<br>Error: 550 5.7.501 Service unavailable, Client host blocked using Spamhaus. To request removal from this list see <http://www.spamhaus.org/lookup.lasso>**





# Direct Send



- Helps to spoof several common rule issue conditions like:
  - FROM user X (Bypass rule)
  - Known 3<sup>rd</sup> party phishing sites
  - FROM Domain
- Direct send NOT required for these conditions:
  - TO user (Specific user X)
  - X-HEADER-VALUE
  - Warning Banners / Footers/ Subjects / Body Contains





# Direct Send - Transport Rules



- Exchange Online > Mail Flow > Connectors
- Configuring connector rules
  - Force all incoming mail to the organization proxies
- Vendors may forget to set this up!

## How to identify your partner organization

Identify the partner organization by verifying that messages are coming from these domains: \*

[Edit sent email identity](#)

## Security restrictions

Reject messages if they don't come from within these IP address ranges:

```
Send-MailMessage: Mailbox unavailable. The server response was: 5.7.51 TenantInbound Attribution; There is a partner connector configured that matched the message's recipient domain. The connector had either the RestrictDomainsToIPAddresses or RestrictDomainsToIPAddresses
```





# Disable Direct Send\*\*



- Set-OrganizationConfig -RejectDirectSend \$true
- 30 minute deploy
- Does not seem to completely block direct send but better than nothing.

By default, the new opt-in RejectDirectSend setting is set to **False**. To enable the Reject Direct Send feature, Exchange Online administrators can run the following PowerShell cmdlet:

```
Set-OrganizationConfig -RejectDirectSend $true
```

The change should propagate out to our entire service within 30 minutes. With the feature enabled, any received Direct Send messages will see the following message:

```
550 5.7.68 TenantInboundAttribution; Direct Send not allowed for this organization from unauthorized sources
```

Unless Direct Send is re-enabled again, any messages that hit this error will need a partner connector created to authenticate their source as an approved sender.

<https://techcommunity.microsoft.com/blog/exchange/introducing-more-control-over-direct-send-in-exchange-online/4408790>

© Black Hills Information Security | @BHinfoSecurity





# DMARC



- Proper configuration of DMARC appears to properly reject messages sent via Direct Send.
- This does not apply to other mail rule issues
  - TO user (Specific user X)
  - X-HEADER-VALUE
  - Warning Banners / Footers/ Subjects / Body Contains





# Securing Exchange Online



- Rules review / considerations
  - Most time spent here, regular/repeated
- Disable Direct Send
- DMARC



© Black Hills Information Security | @BHinfoSecurity