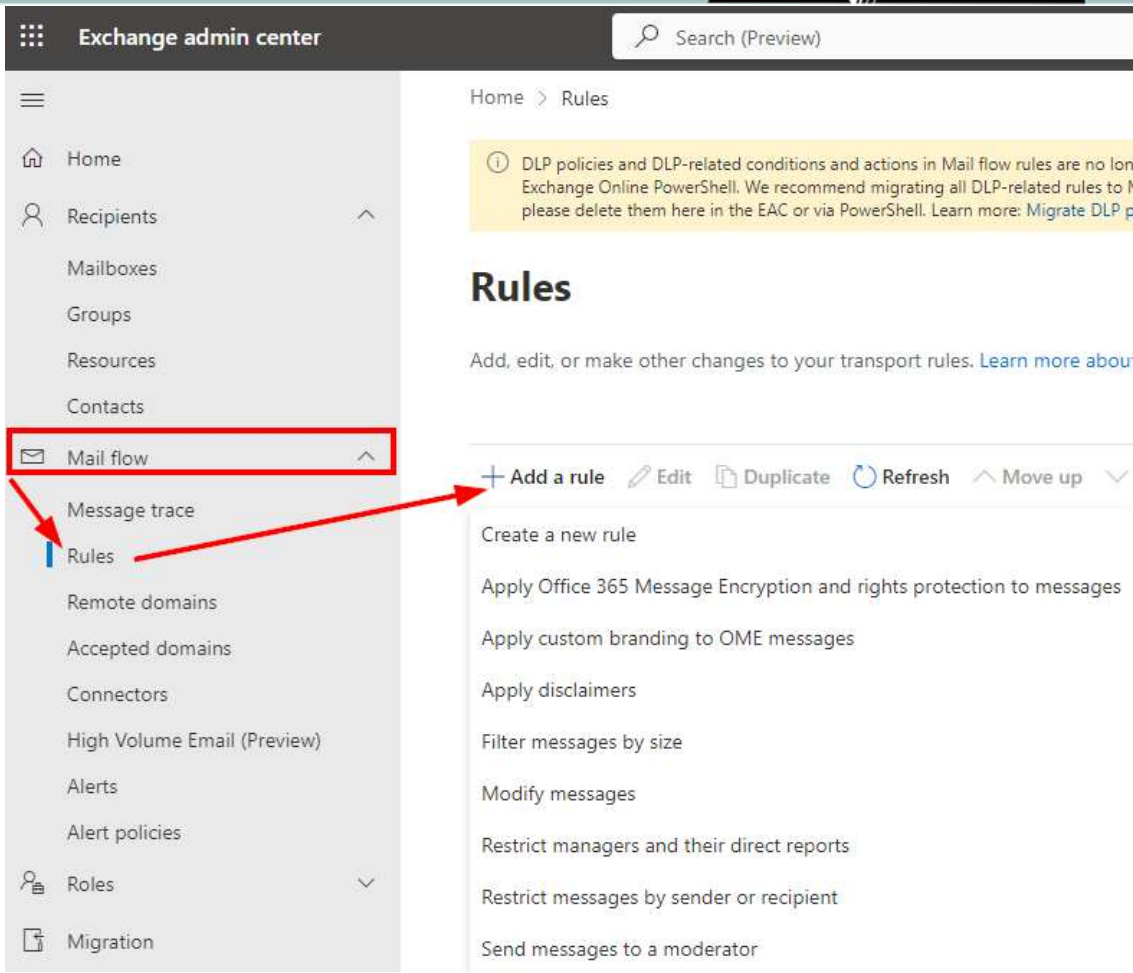
How to Strengthen M365 Exchange Online Configurations

Exchange Online

- admin.exchange.microsoft.com
- Some* Security Considerations:
  - Mail flow/transport rules
  - Direct Send
  - Sending Directly

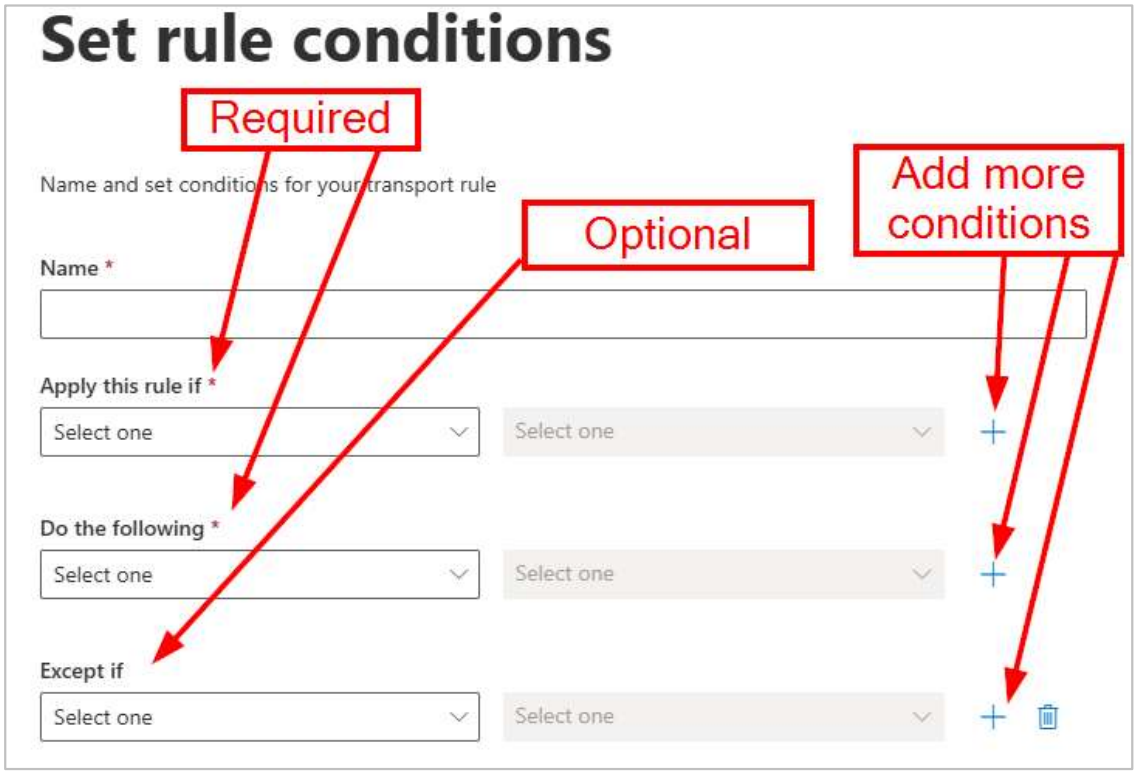
Exchange Mail Flow Rules

- Where are we?



Rule Requirements - Conditions

- Apply this rule if (Required): One or more condition(s)
- Do the following (Required): One or more: Bypass, append header, prepend header, etc
- Except if (Optional): One or more condition(s)



Rule Settings

Test

Rule Name

Conditions | Settings

Conditions vs Settings

Priority *

0

Rule mode

- (•) Enforce
- ( ) Test with Policy Tips
- ( ) Test without Policy Tips

Severity *

Not specified

[ ] Activate this rule on

7/27/2025 - 2:00 PM

[ ] Deactivate this rule on

7/27/2025 - 2:00 PM

[x] Stop processing more rules

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.

Creating “Good” Rules

- Consider scope - be very specific
  - IP Address AND Domain name
  - IP Address AND x-header (Common for 3rd 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

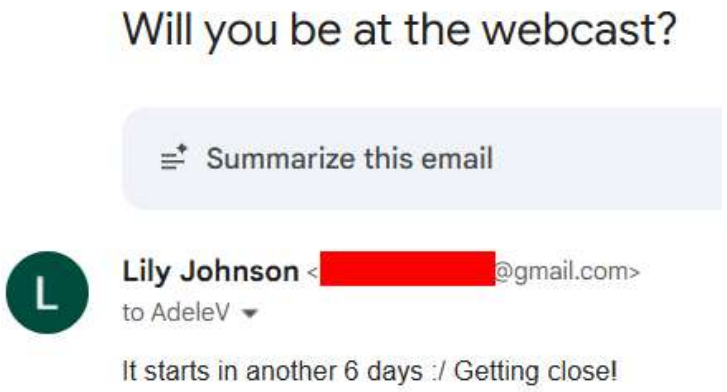
Is received from 'Outside the organization'

Do the following

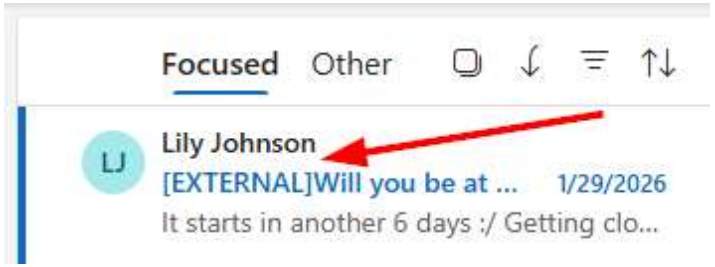
Prepend the subject with '[EXTERNAL]' and Stop processing more rules

Rule Function - Message Sent to Organization

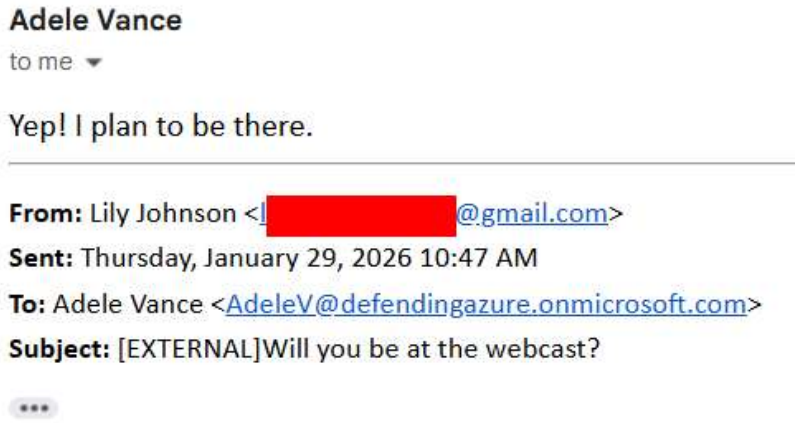
- Lily Sends:



- Adele Sees:



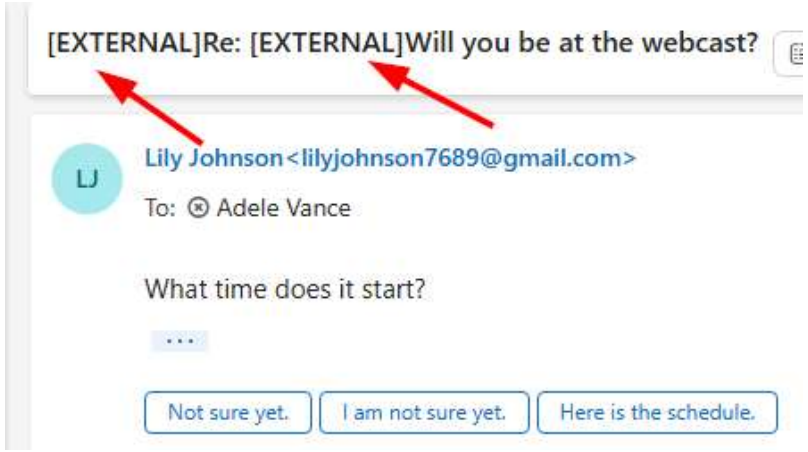
- Adele Replies



Reply to email chain and...

- Llily Replies:

- Adele gets 2 [EXTERNAL] Headers



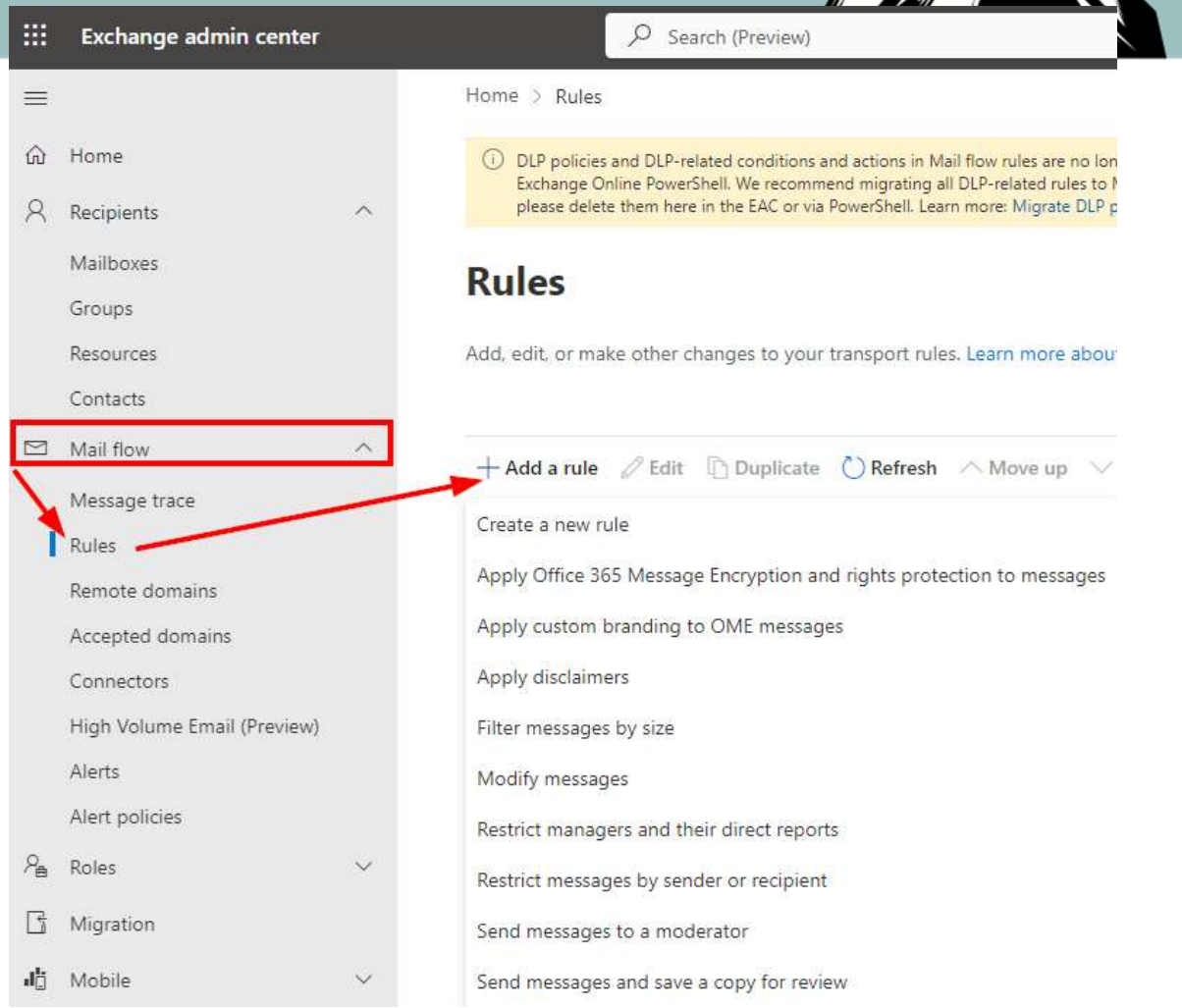
Microsoft's Solution! (Sort of)

- 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**.

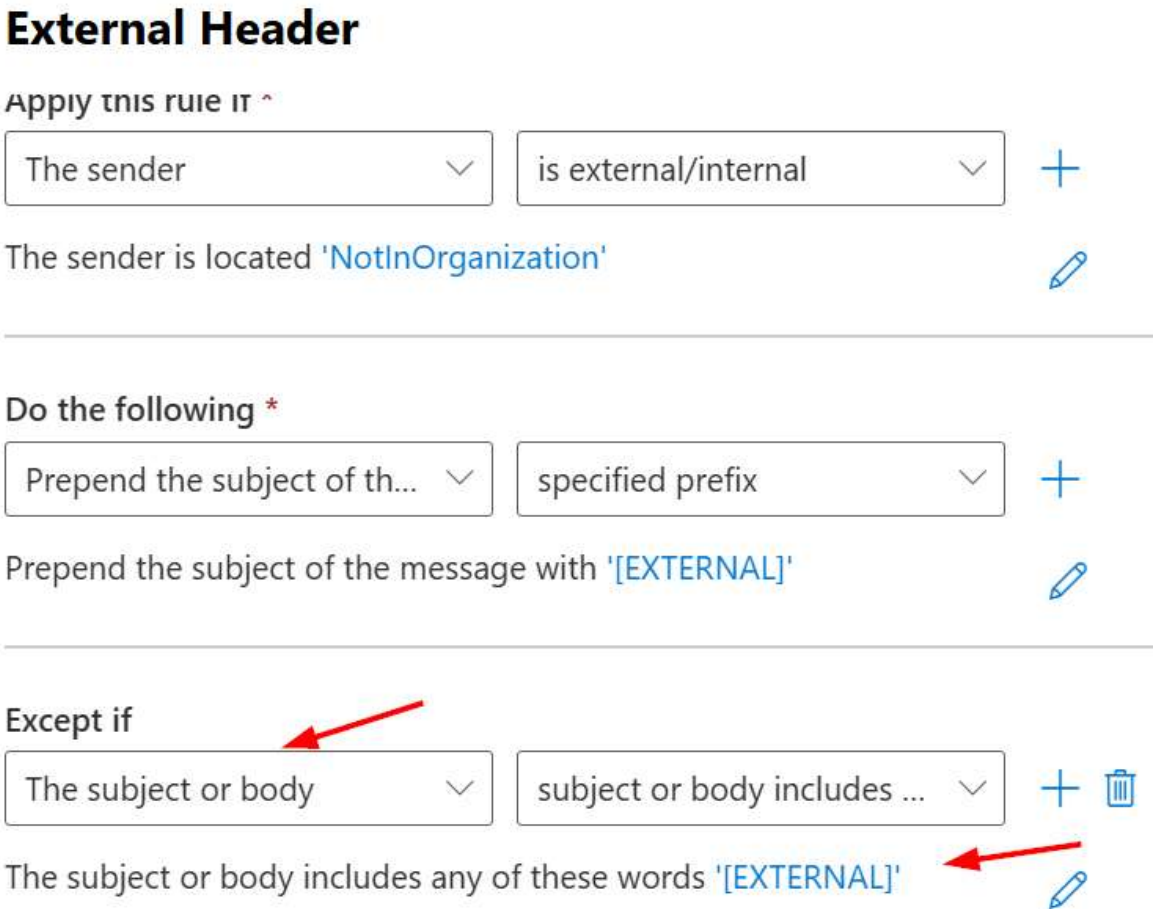
When you're finished, select **Next**.

Mail Rule vs Disclaimer



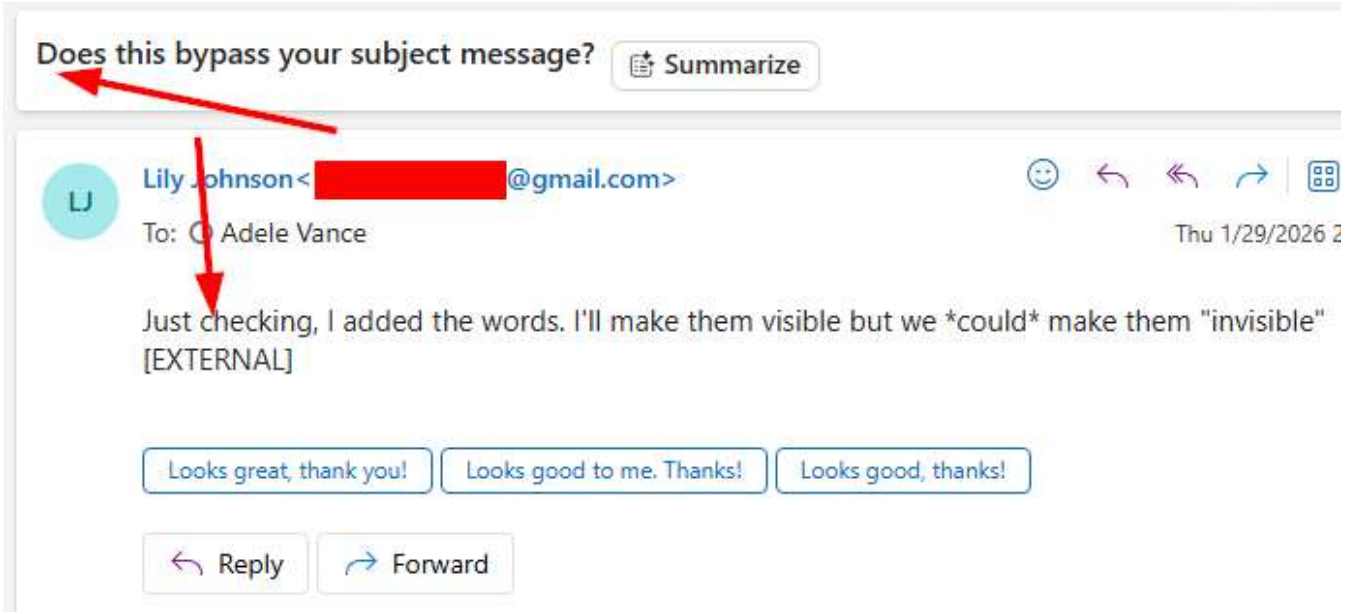
Modify Original Rule

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



New message “Bypassing” Subject Rule

- Can be done with body warning messages too!
-
- [EXTERNAL]
-



Common Rule Issues

- Bypasses (Spam/Attachment/Scanner)
  - TO user (Specific user X)
  - FROM user
    - **Example**:
      - helpdesk@companyname.tld
      - support@companyname.tld
      - noreply@companyname.tld
      - no-reply@companyname.tld
      - noreply@email.teams.microsoft.com
      - support@companyname.Atlassian.net
      - notification@slack.com
      - -Known 3rd party phishing company sites
        - Example follows
  - FROM Domain
    - subsidiary, trusted 3rd 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.magnetonics.com,
Socialmedia-insights.bloemlight.com,
Messaging-security.comano.us,

exch01-corp.com
facbook-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
instagrarn.net
internalitsupport.com
investmentsecureportal.com
itnues.net
lesportsacxx53.com

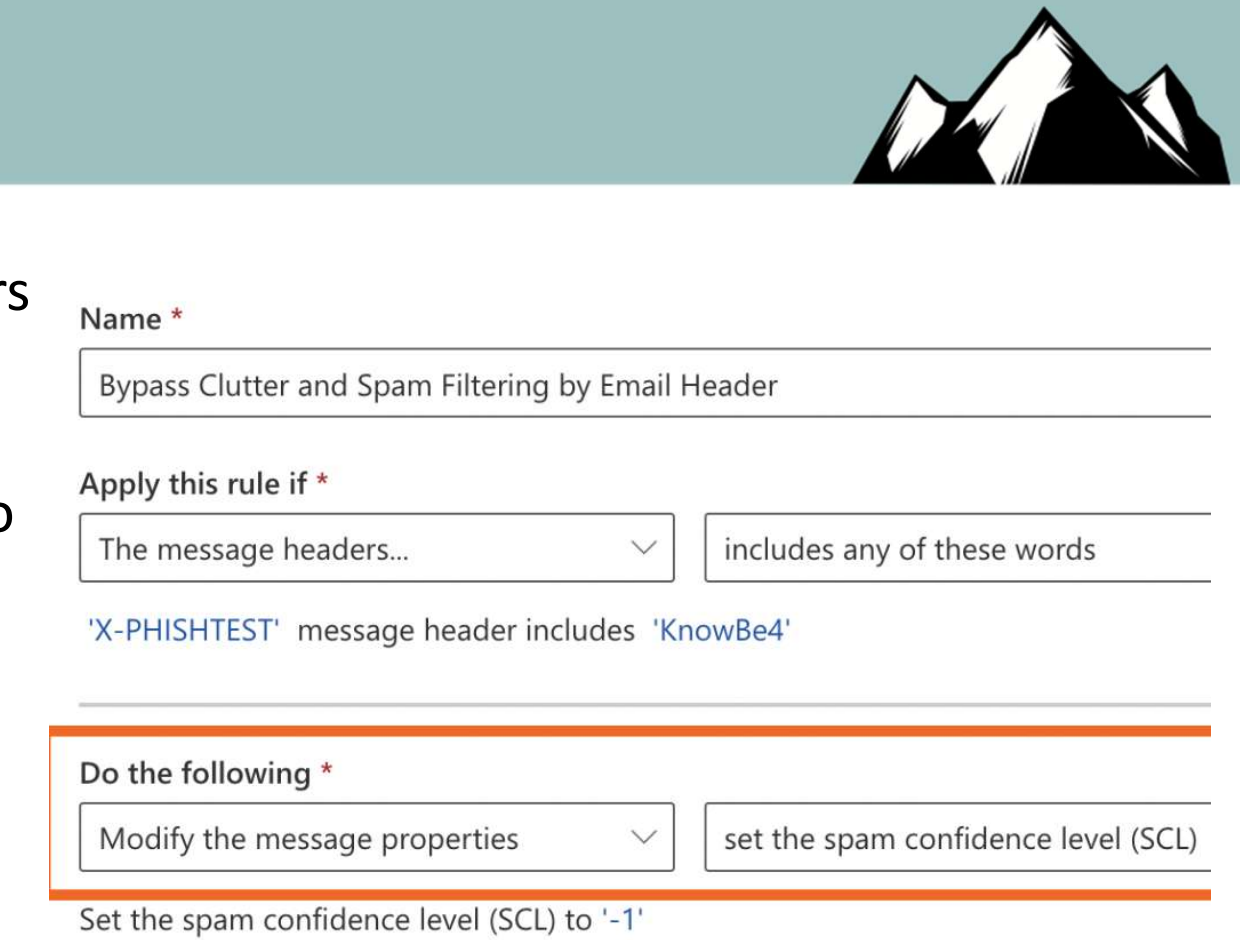
pharmamedsonline.com
pharmlink.in
phishingtraining.com
pipelinenews.net
postcardfast.com
prnewsnet.us
publicemailservice.com
qqoffi55.cc
qqoffi55.com
qquio.com
ransomware.site
register-now.world
rwebfix.com
saleslinkforce.com
salesteamlink.com
scandeviceservices.com
sec-10k.com
securebankingsevices.com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

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")



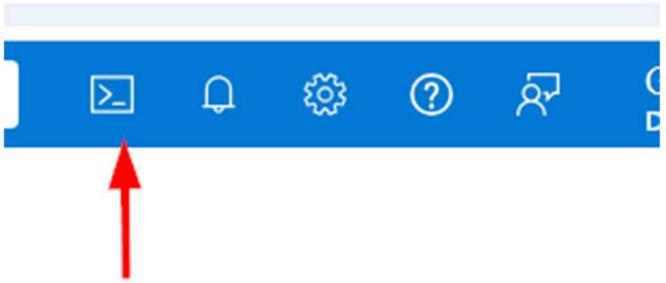
- https://support.knowbe4.com/hc/en-us/articles/212723707-Whitelist-by-Email-Headers-in-Microsoft-365-Microsoft-Exchange-2016-and-Microsoft-Exchange-2019

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

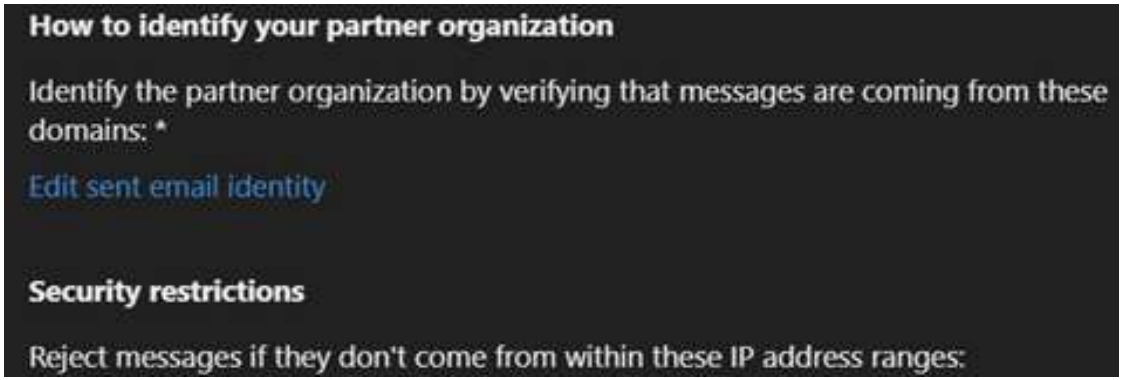
Error: 550 5.7.501 Service unavailable, Client host blocked using Spamhaus. To request removal from this list see http://www.spamhaus.org/lookup.lasso

Direct Send

- Helps to spoof several common rule issue conditions like:
  - FROM user X (Bypass rule)
  - Known 3rd 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!




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

Disable Direct Send**

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

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

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.

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