

Phishing Campaign - Setting Up Microsoft o365

Why Whitelist in Office 365?

Whitelisting ensures the **CyTech - AQUILA Phishing Simulation(PS) Module** functions without issue and prevents PS emails from being automatically moved to the spam folder or notifying users about potential phishing emails. The Connection Filter Policy and Spam Filtering both required to be whitelisted.

Key Configurations:

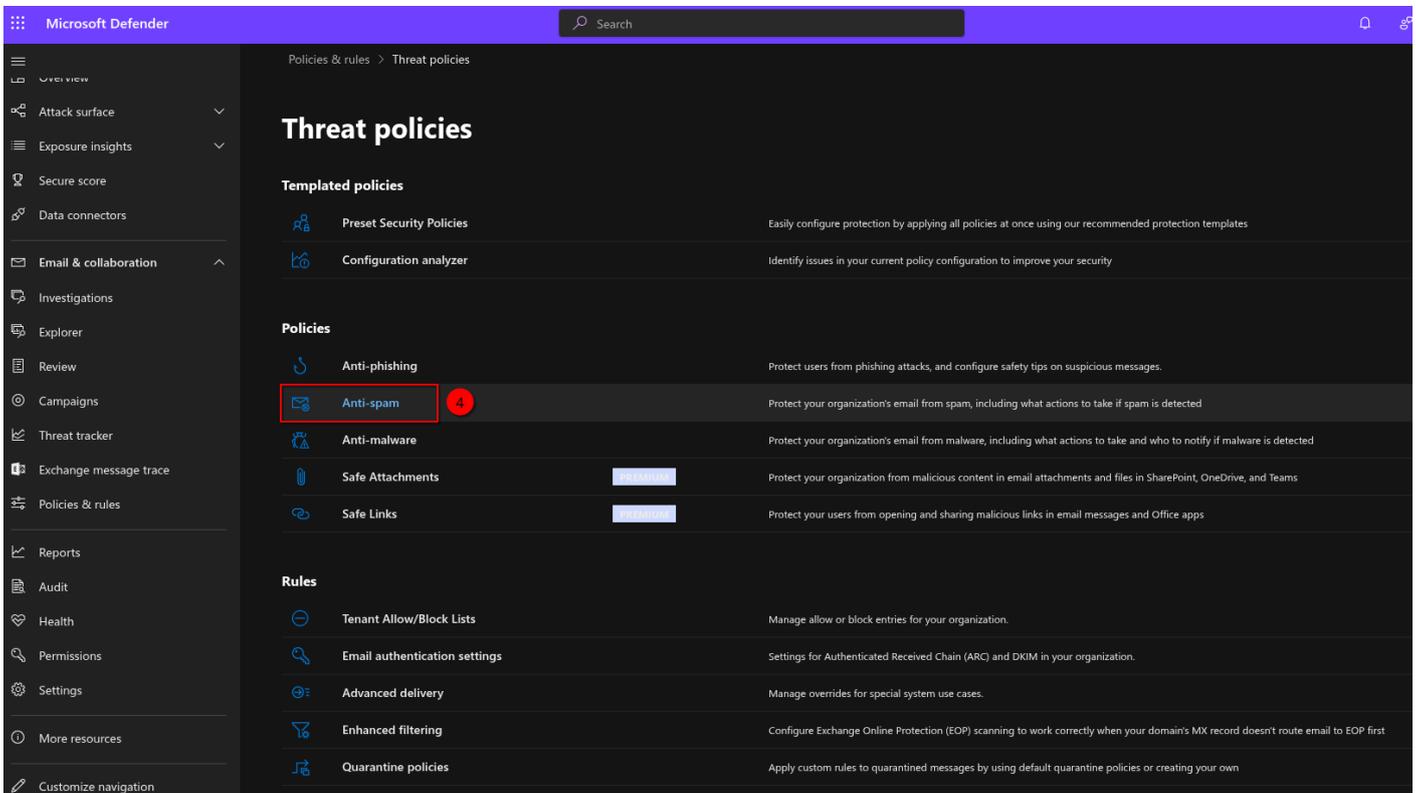
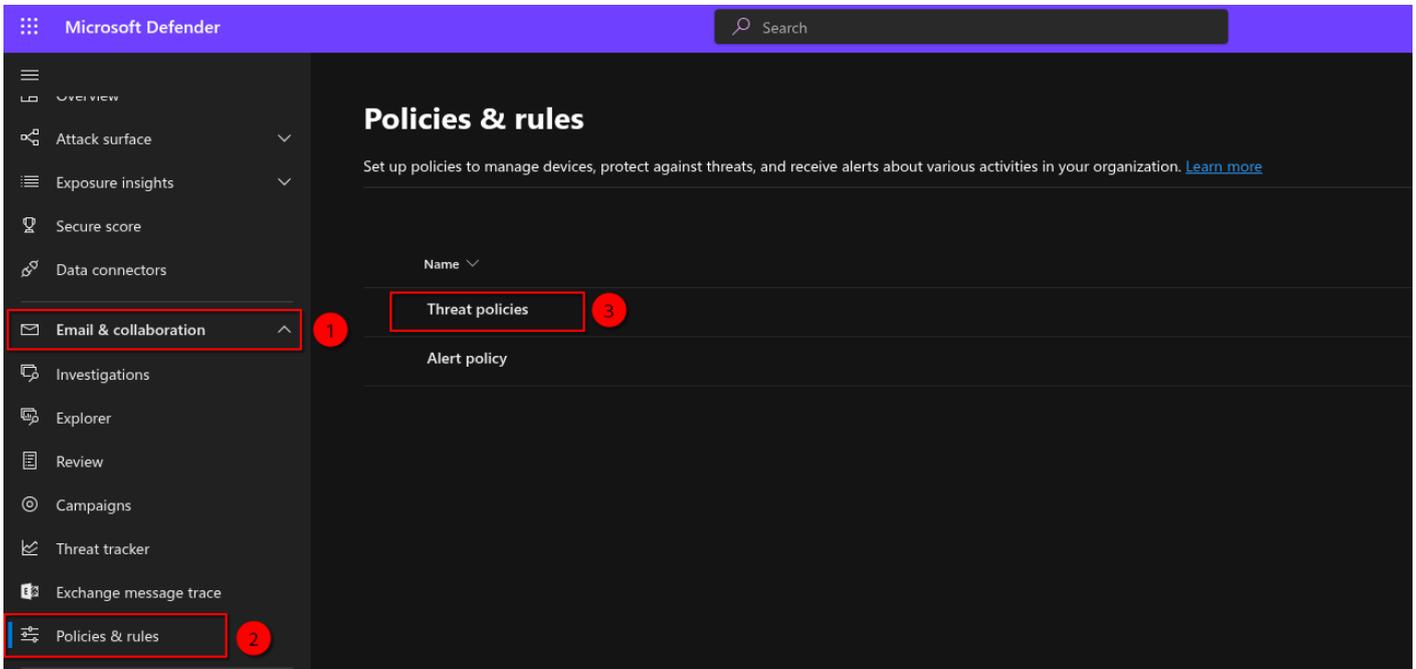
1. **Microsoft Defender**
 - Whitelist the Connection Filter Policy
 - Whitelist Using Advanced Delivery Policies
2. **Exchange Admin Center**
 - Whitelist Spam Filtering
 - Whitelist Advanced Threat Protection (ATP)

Whitelist Connection Filter Policy

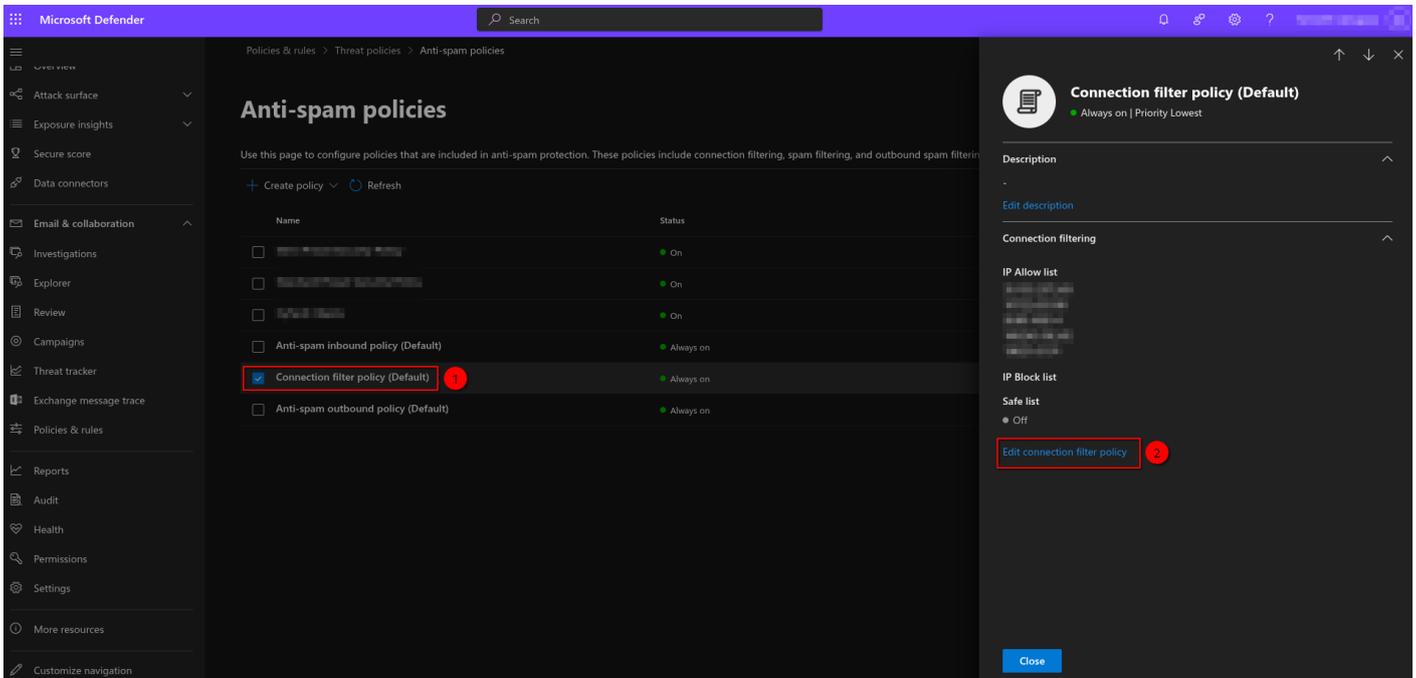
The Office 365 Exchange Connection Filter identifies good or bad source email servers by their IP addresses. The actions below will allow all emails from CyTech IP addresses to be received.

Whitelist the Connection Filter Policy

1. Login to Microsoft Defender, click here - [Microsoft Defender](#).
2. Navigate through **Email & Collaboration>Policies & Rules>Threat Policies>Anti-spam**.

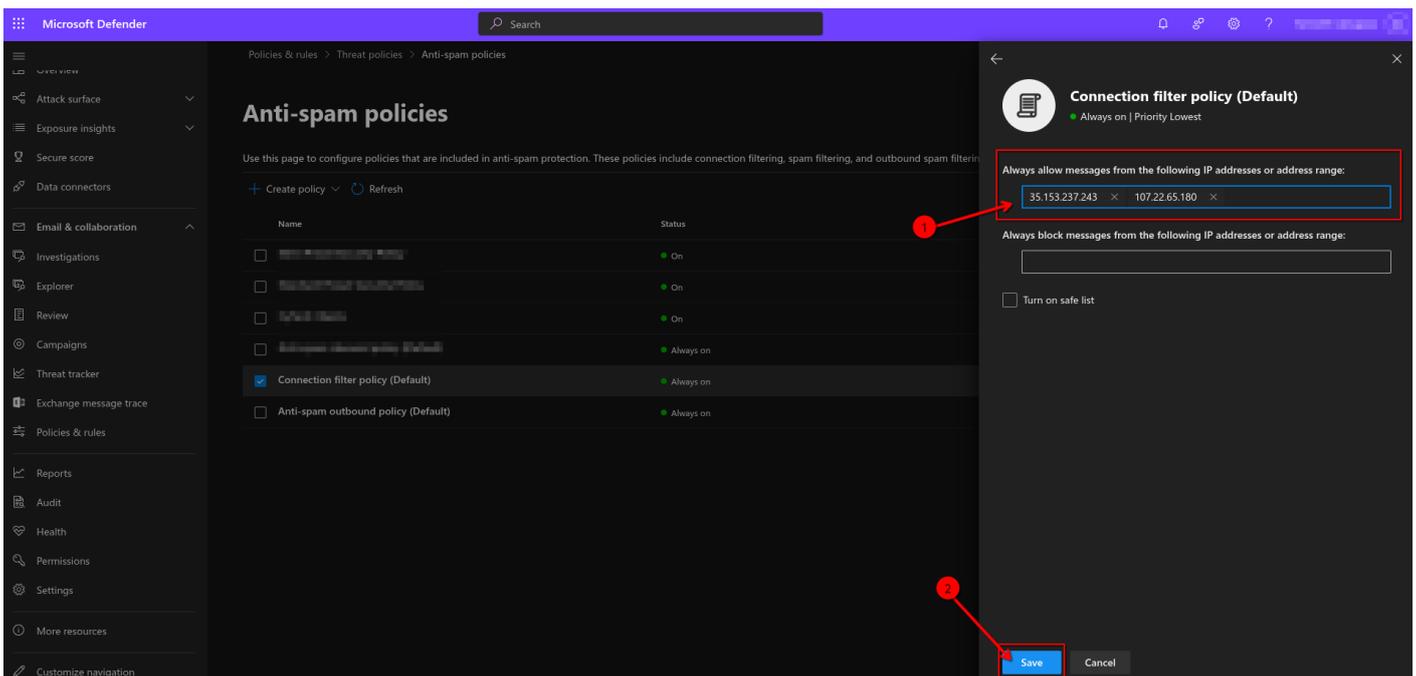


3. Click on "**Connection filter policy**". Then click on "**Edit connection filter policy**".



4. Add the **IP's** to the "Always allow messages from the following IP addresses or address range:". Then click the **"Save"** button.

Allow IP's: 35.153.237.243(Mail Server), **107.22.65.180**(Landing Page)

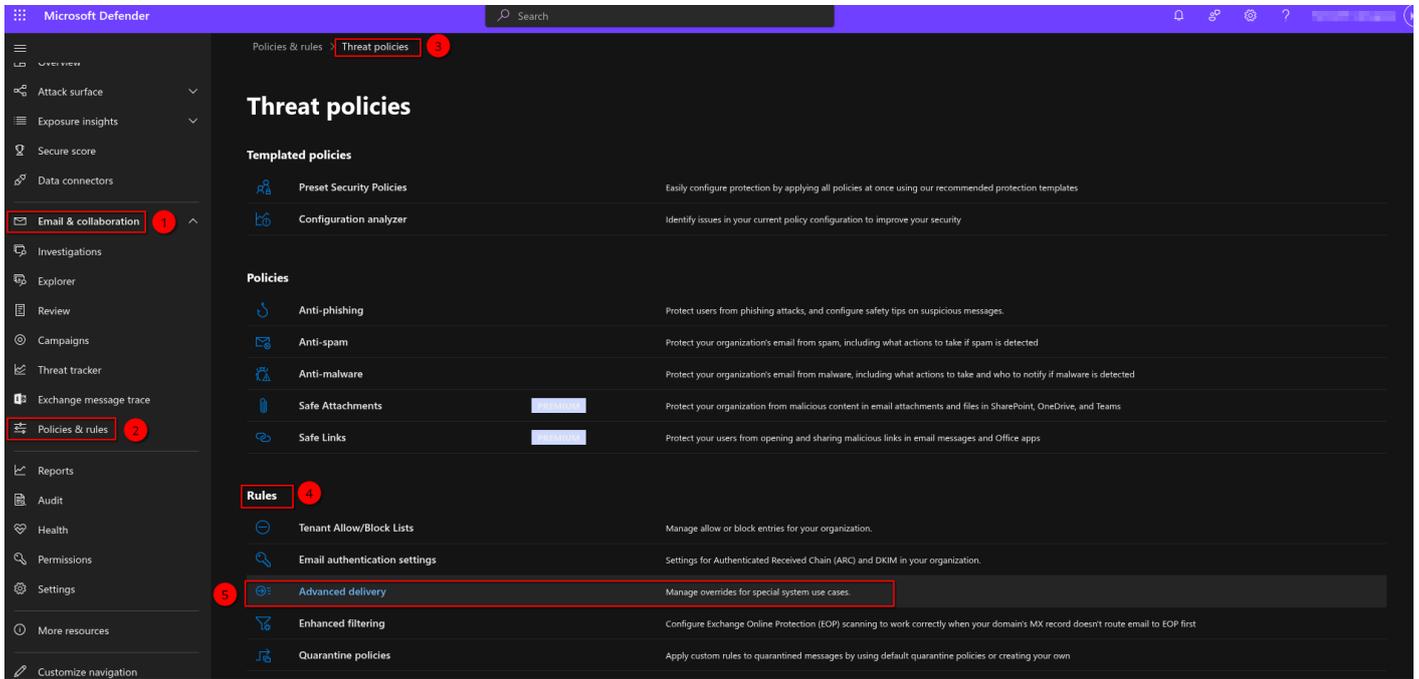


Whitelist Using Advanced Delivery Policies in Microsoft Defender for Office 365

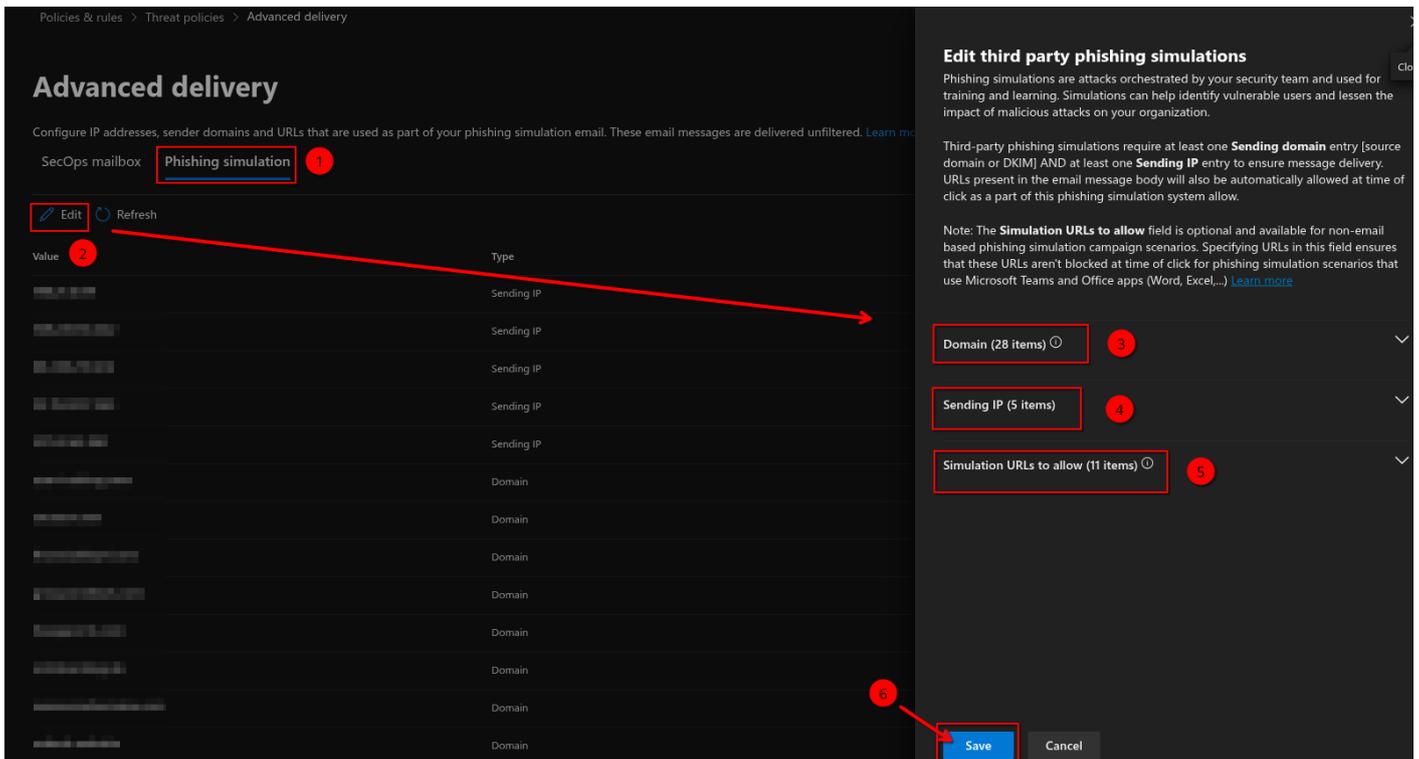
Phishing simulations are attacks orchestrated by your security team and used for training and learning. Simulations can help identify vulnerable users and lessen the impact of malicious attacks on your organization.

Third-party phishing simulations require at least one Sending domain entry [source domain or DKIM] AND at least one Sending IP entry. Simulations URLs to allow entries are optional, and prevent the simulated phishing URLs from being blocked at time of click.

1. Go to **Email & Collaboration > Policies & Rules > Threat policies > Advanced delivery in the Rules section.**



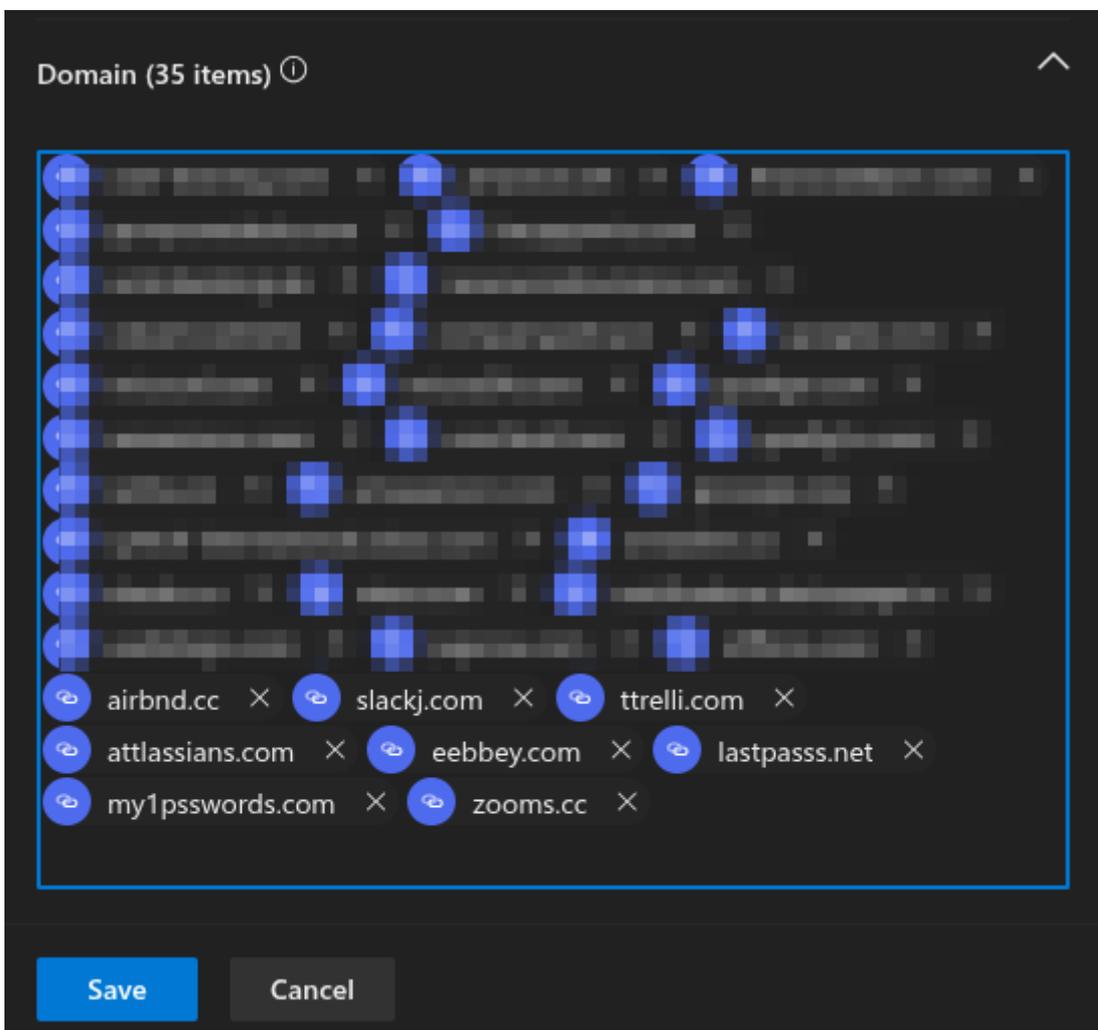
2. In the Advanced delivery menu, navigate to the Phishing simulation tab and press Edit to either add new or configure existing values (refer to the screenshot below). After editing all the needed Domain, Sending IP and Simulation URLs to allow. Click **"Save"**.



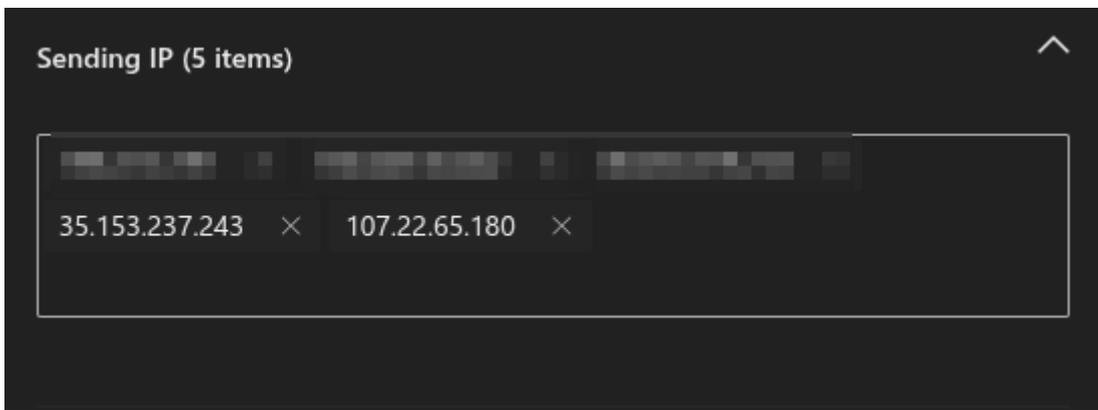
3. On the Edit third-party phishing simulation menu that opens, configure the following settings:

Domain: Expand this setting and enter at least one sending domain specific for campaign by clicking in the box, entering a value, and then pressing Enter or selecting the domains displayed below. Repeat this step as many times as necessary. You can add up to 20 entries.

- slackj.com
- ttrelli.com
- airbnd.cc
- atlassians.com
- eebbey.com
- lastpass.net
- my1psswords.com
- zooms.cc



Sending IP: Expand this setting and enter at least one valid IPv4 address by clicking in the box, entering a value, and then pressing Enter or selecting the value that's displayed below the box. Repeat this step as many times as necessary. You can add up to 10 entries.



Simulation URLs to allow: Expand this setting and optionally enter specific URLs that are part of your phishing simulation campaign that should not be blocked or detonated by clicking in the box, entering a value, and then pressing Enter or selecting the value that's displayed below the box.

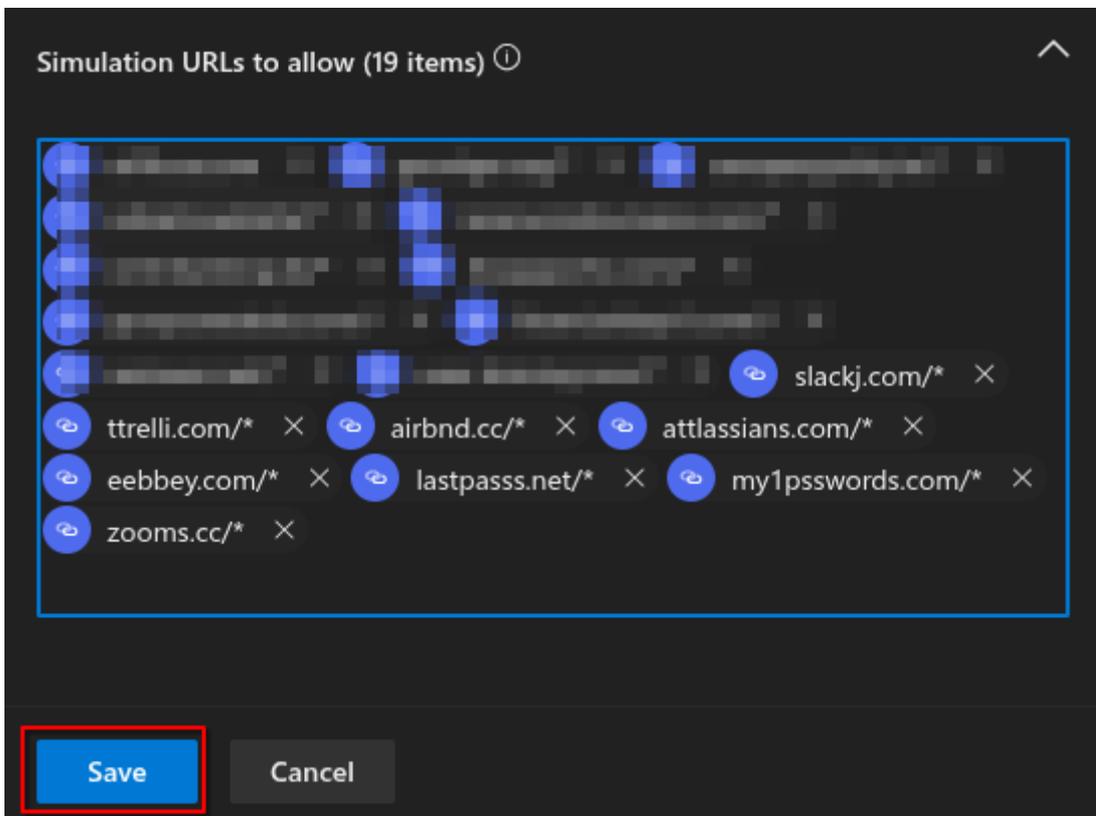
For the URL syntax format, see [URL syntax for the Tenant Allow/Block List](#) (opens in a new tab). These URLs are wrapped at the time of the click, but they aren't blocked.

When you're finished, you can click Add, and click close afterward if this was a first-time addition, or if you were editing existing values click Save and then click Close.

- Manage allows and blocks in the Tenant Allow/Block List

Refer to these simulation URLs to allow in your campaign:

- slackj.com/*
- ttrelli.com/*
- airbnd.cc/*
- atlassian.com/*
- eebbey.com/*
- lastpass.net/*
- my1psswords.com/*
- zooms.cc/*

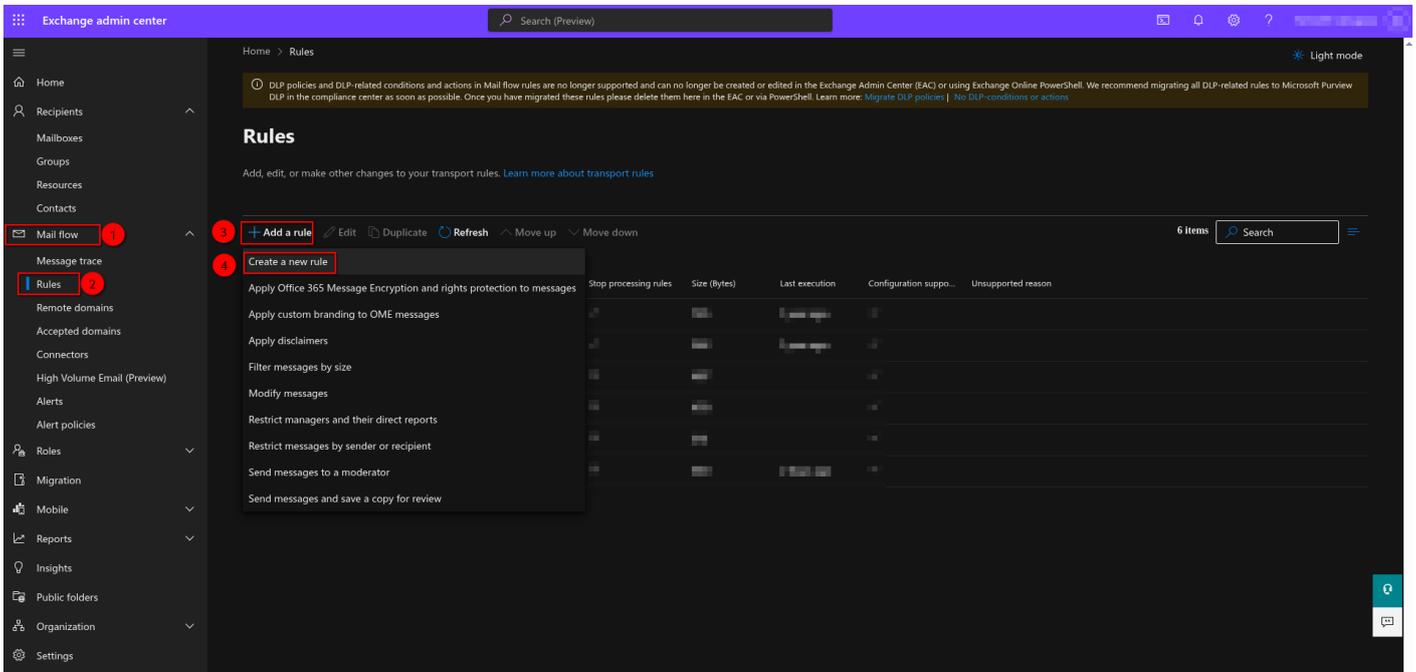


Whitelist Spam Filtering

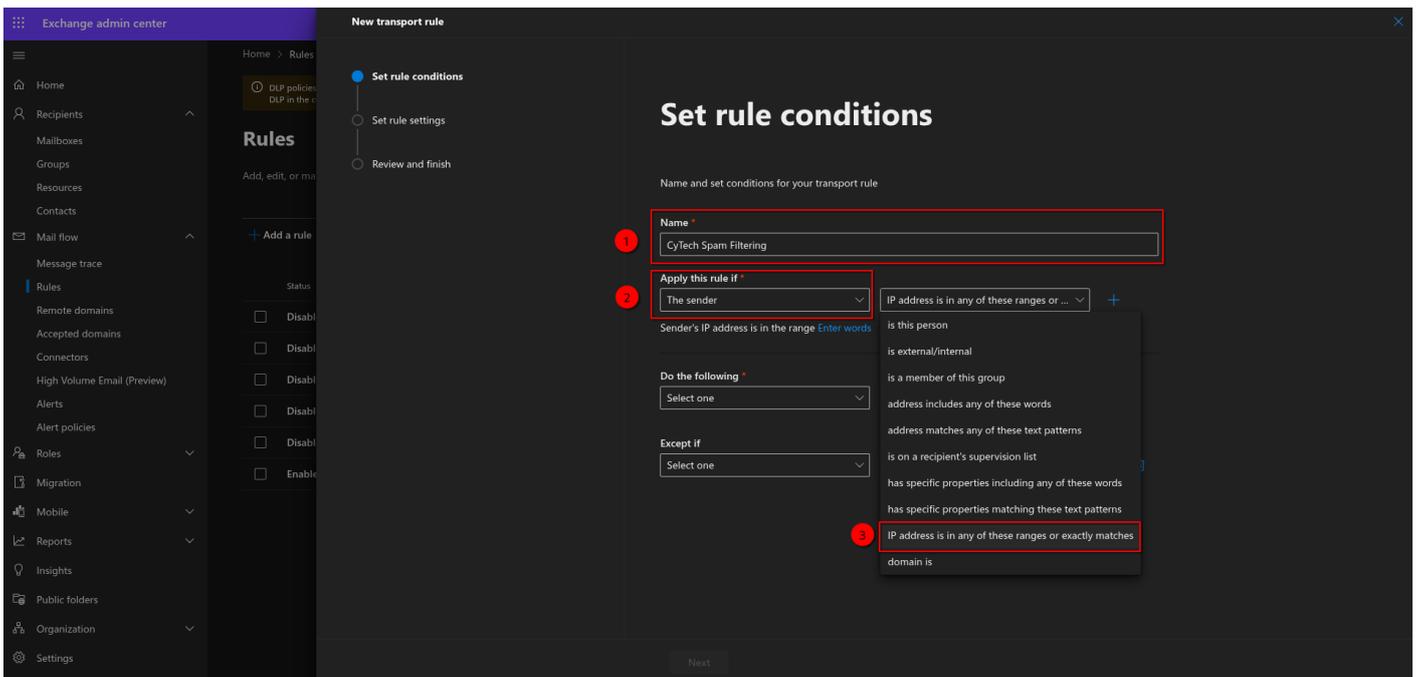
All mail systems have spam filtering. As the CyTech PS emails are "phishing: by definition, the Microsoft spam filter must be whitelisted. The steps below outline how to disable all spam checks for CyTech PS emails, so you won't experience issues with 100% clicked and 100% opened emails, even if the users don't click on them.

Steps to Whitelist the Spam Filtering

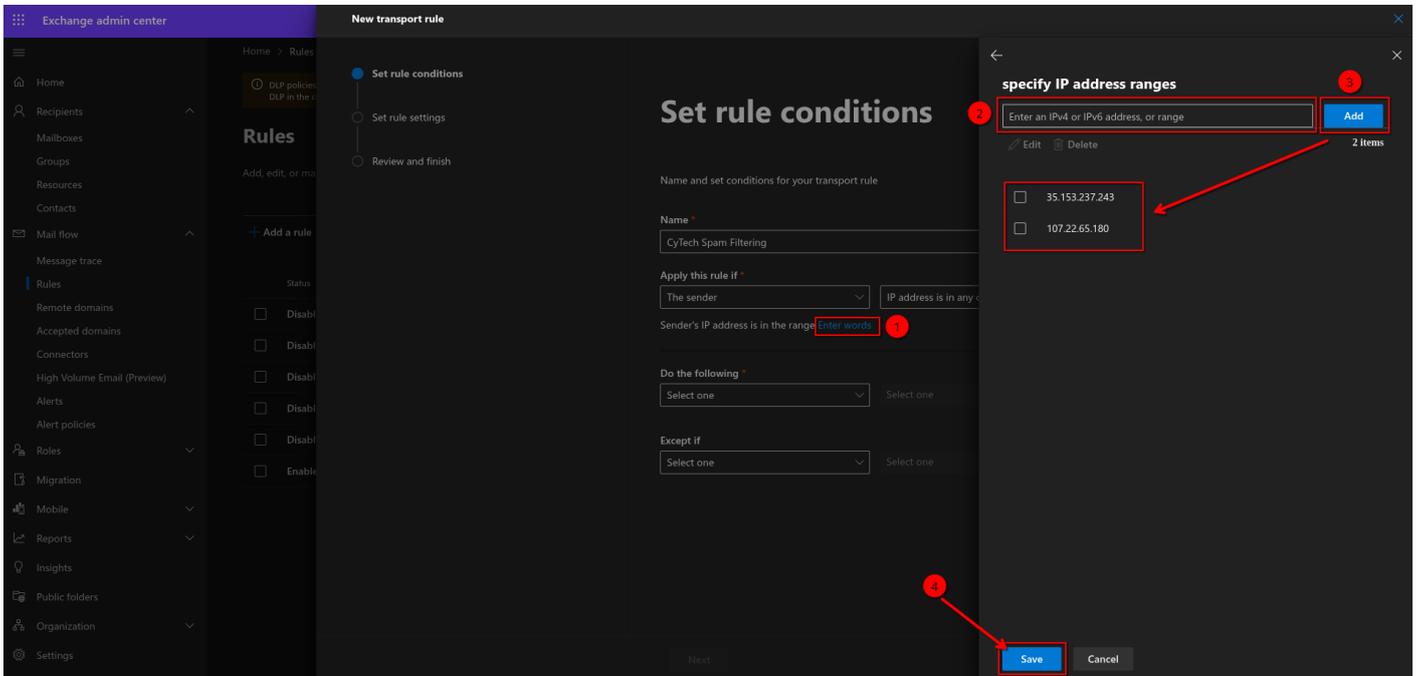
1. Login to Exchange Admin Center, click here - [Exchange Admin Center](#).
2. Navigate through **Mail flow>Rules>+Add a rule>"Create a new rule"**.



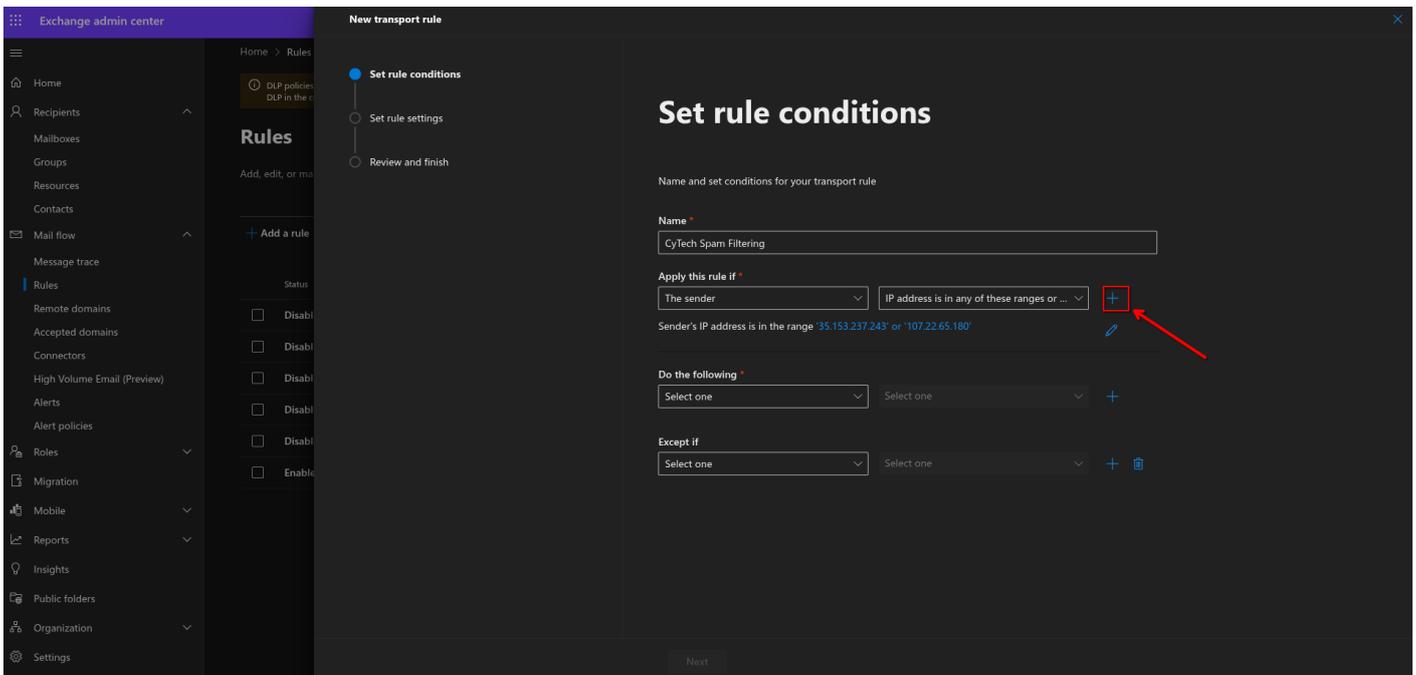
3. Give the rule a name, such as **"CyTech Spam Filtering"**. Click on **"Apply this rule if"** → **"The sender"** → **"IP address is in any of these ranges or exactly matches"**.



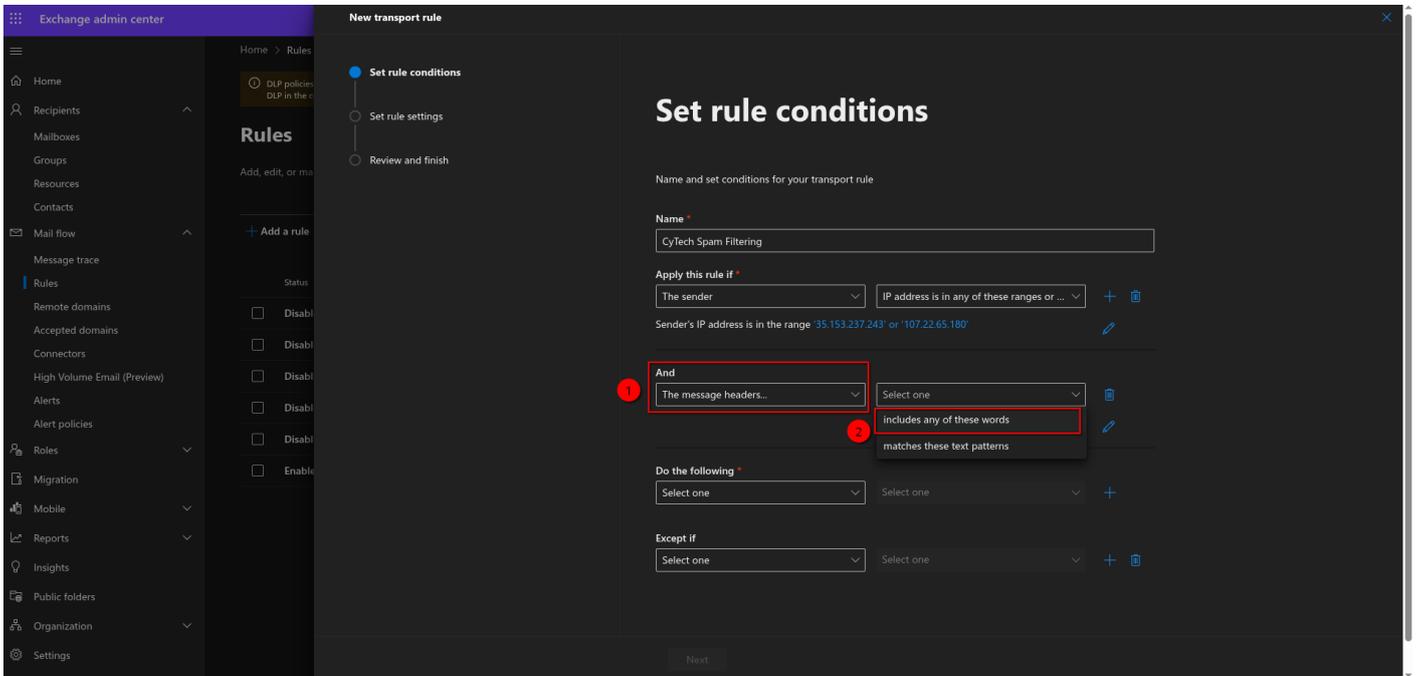
4. Specify the IP addresses in the field IP's: **35.153.237.243**(Mail Server), **107.22.65.180**(Landing Page). Please do not forget to click on **"Save"**.



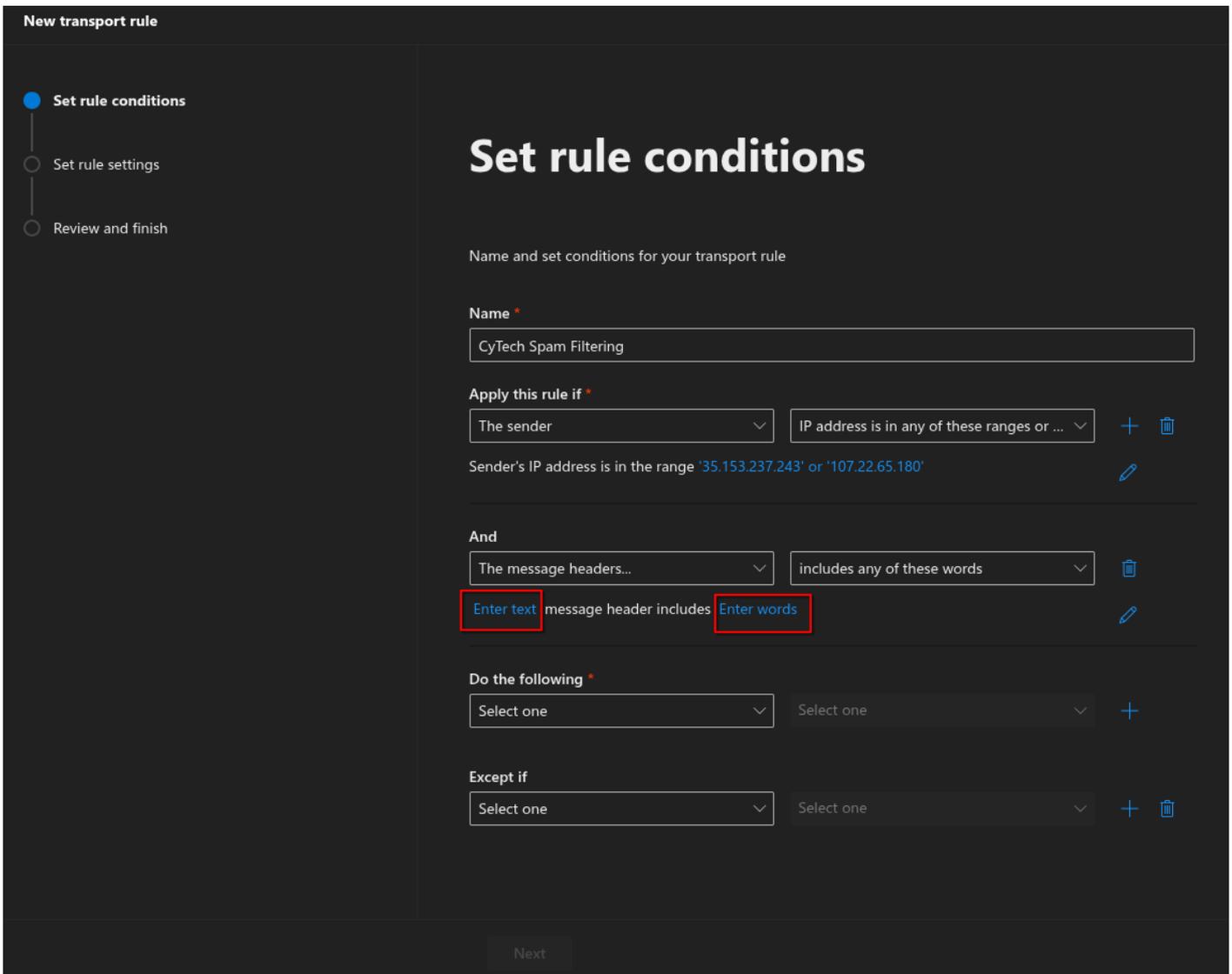
5. Click the "+" to add another rule condition for the message headers.



6. Click on "The message headers...." → "includes any of these words".



7. Click → **Enter text.**



8. Specify header name → **X-PHISHTEST** and specify words or phrases → **CYTECH**.

New transport rule

- Set rule conditions
- Set rule settings
- Review and finish

Set rule conditions

Name and set conditions for your transport rule

Name *

CyTech Spam Filtering

Apply this rule if *

The sender IP address is in any of these ranges or ...

Sender's IP address is in the range '35.153.237.243' or '107.22.65.180'

And

The message headers... includes any of these words

'X-PHISHTEST' message header includes 'CYTECH'

Do the following *

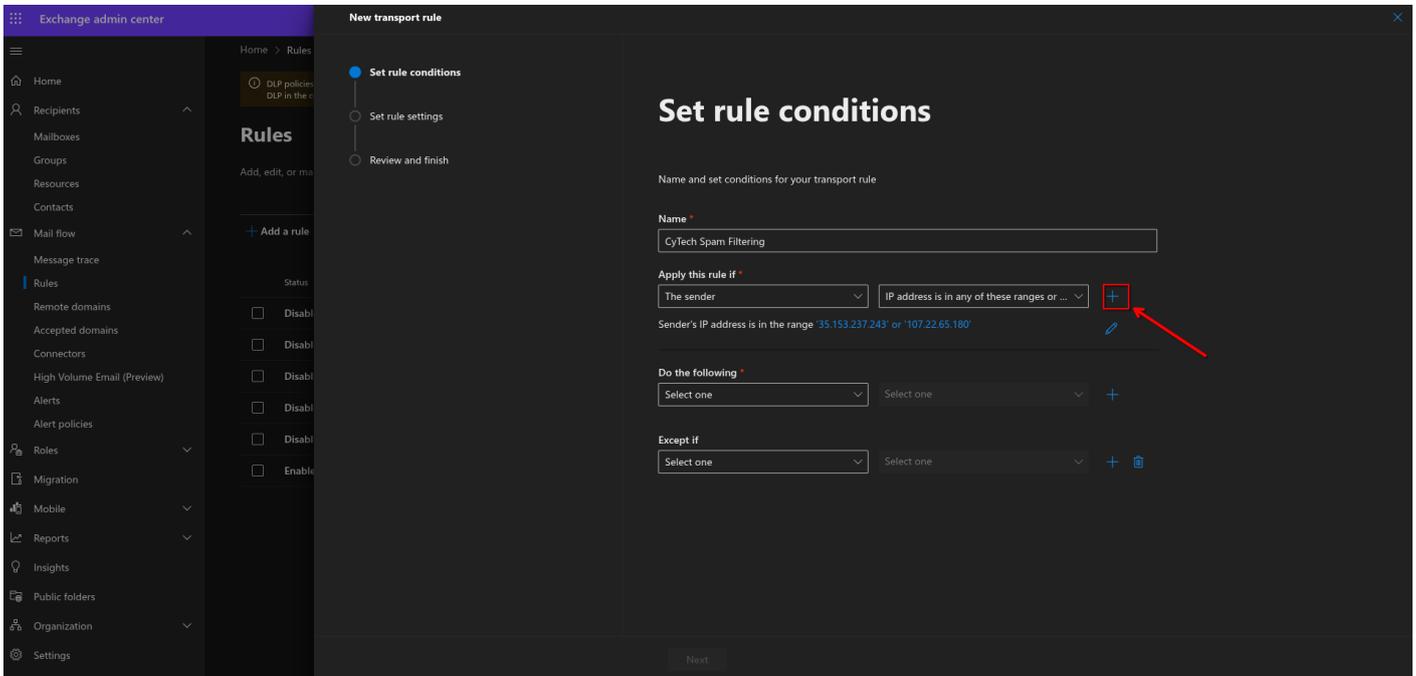
Select one Select one

Except if

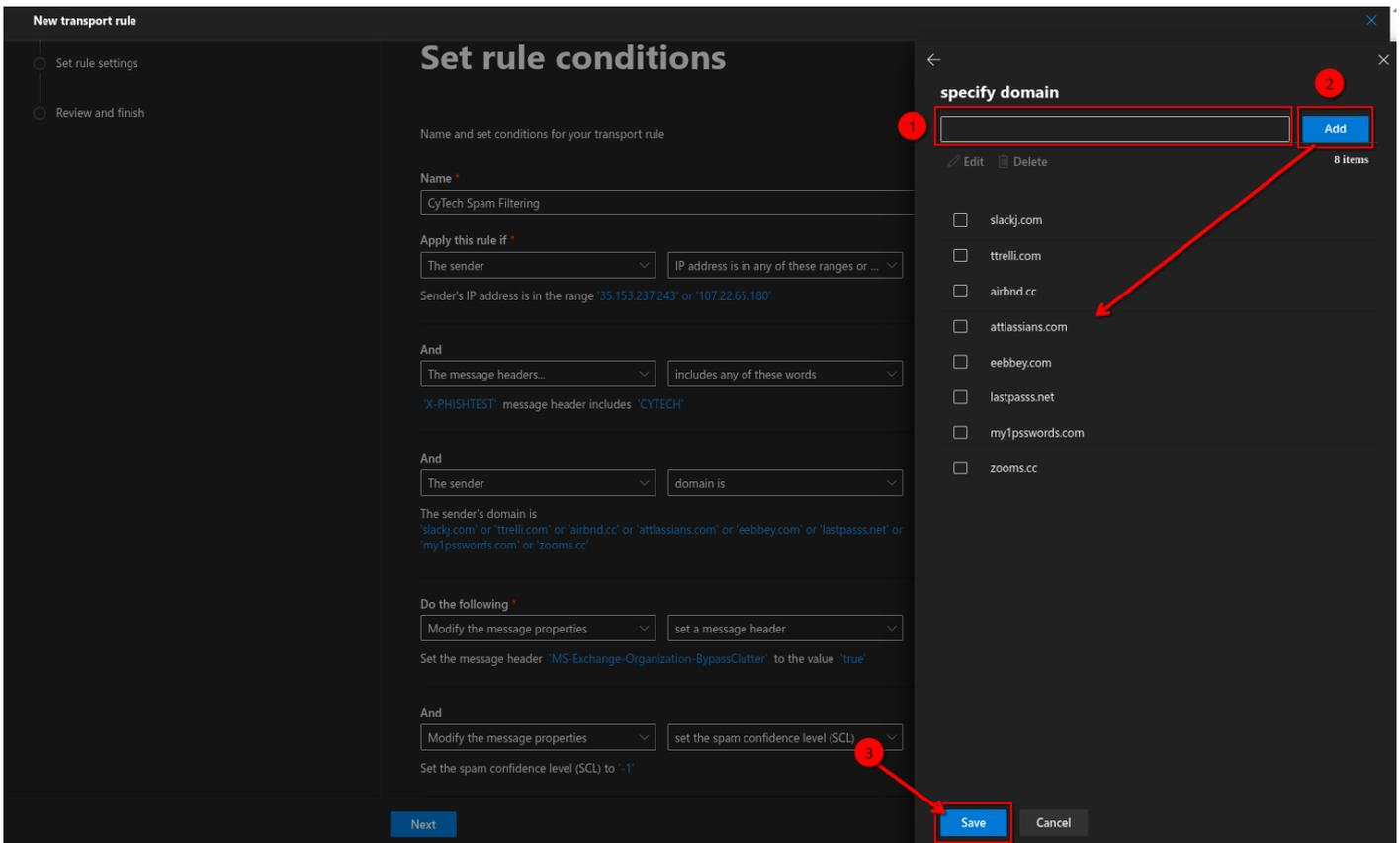
Select one Select one

Next

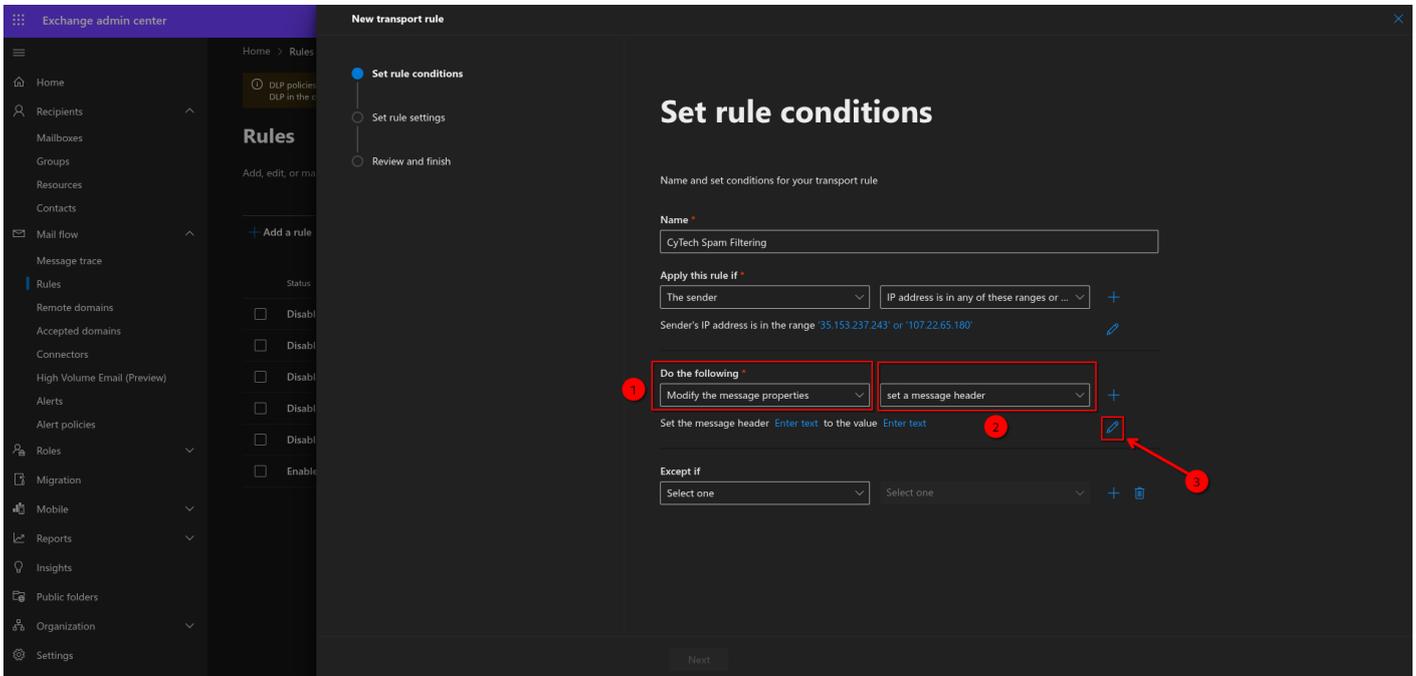
9. Click the "+" to add another rule condition for the The sender.



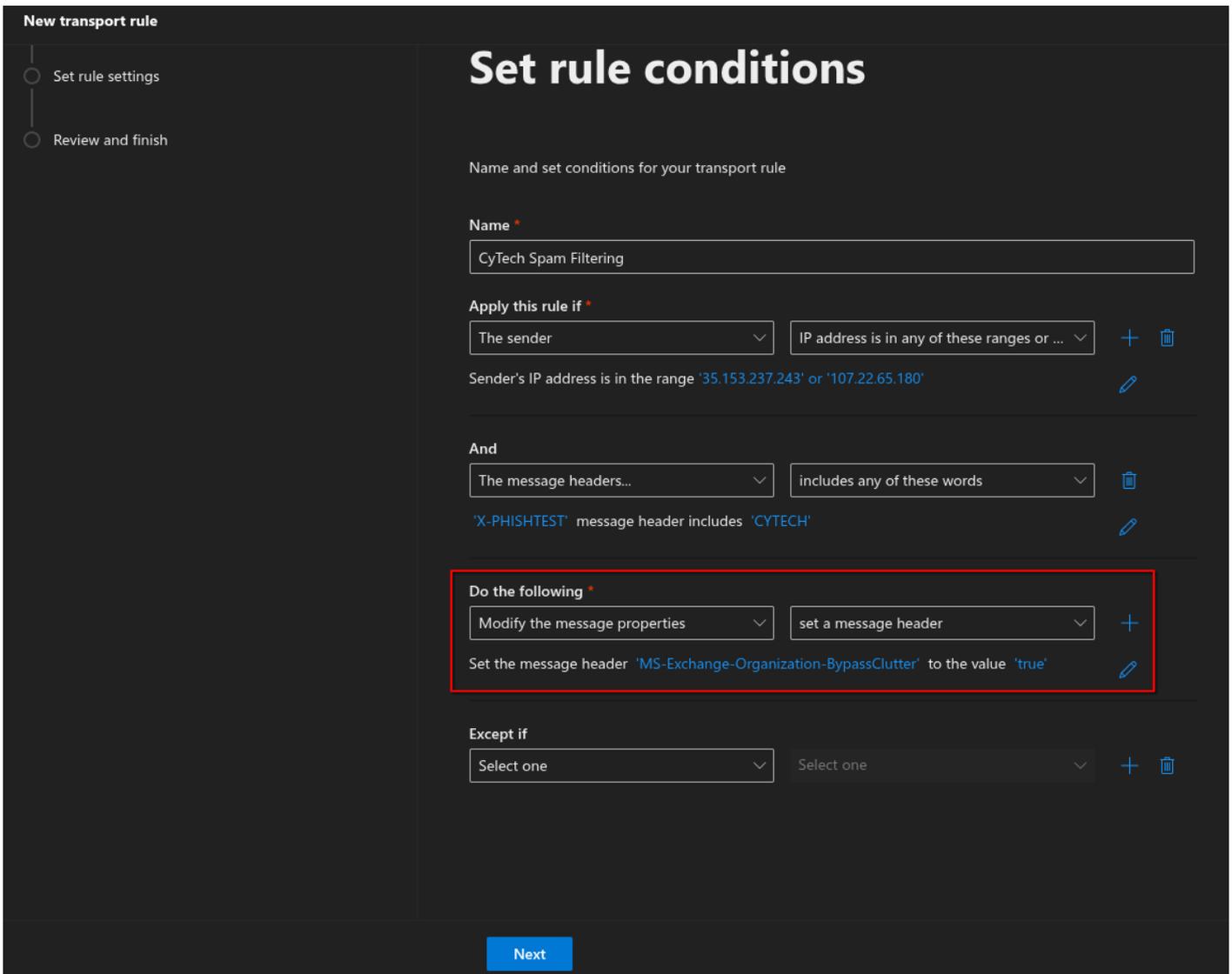
10. Click on "The sender...." → "domains is". Specify the domain in your case. Then click "Save".



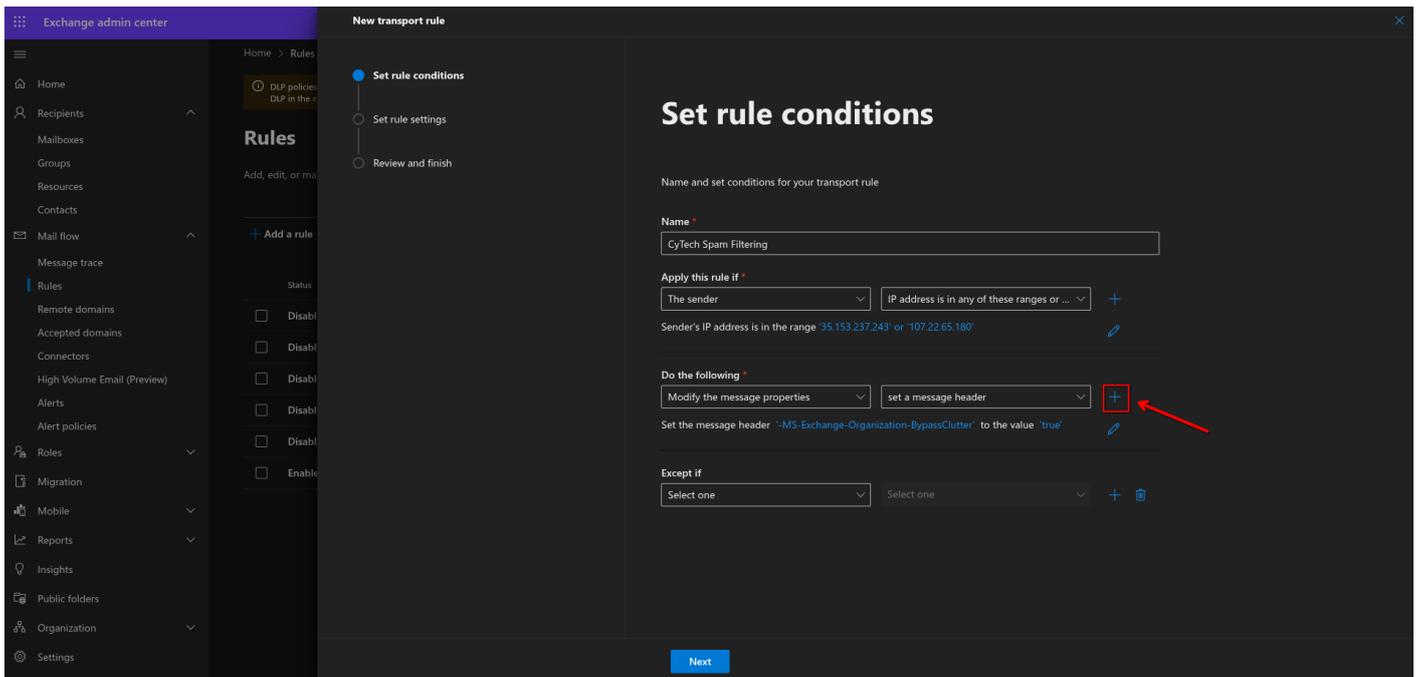
11. Click on "Do the following → Modify the message properties → Set a Message Header"



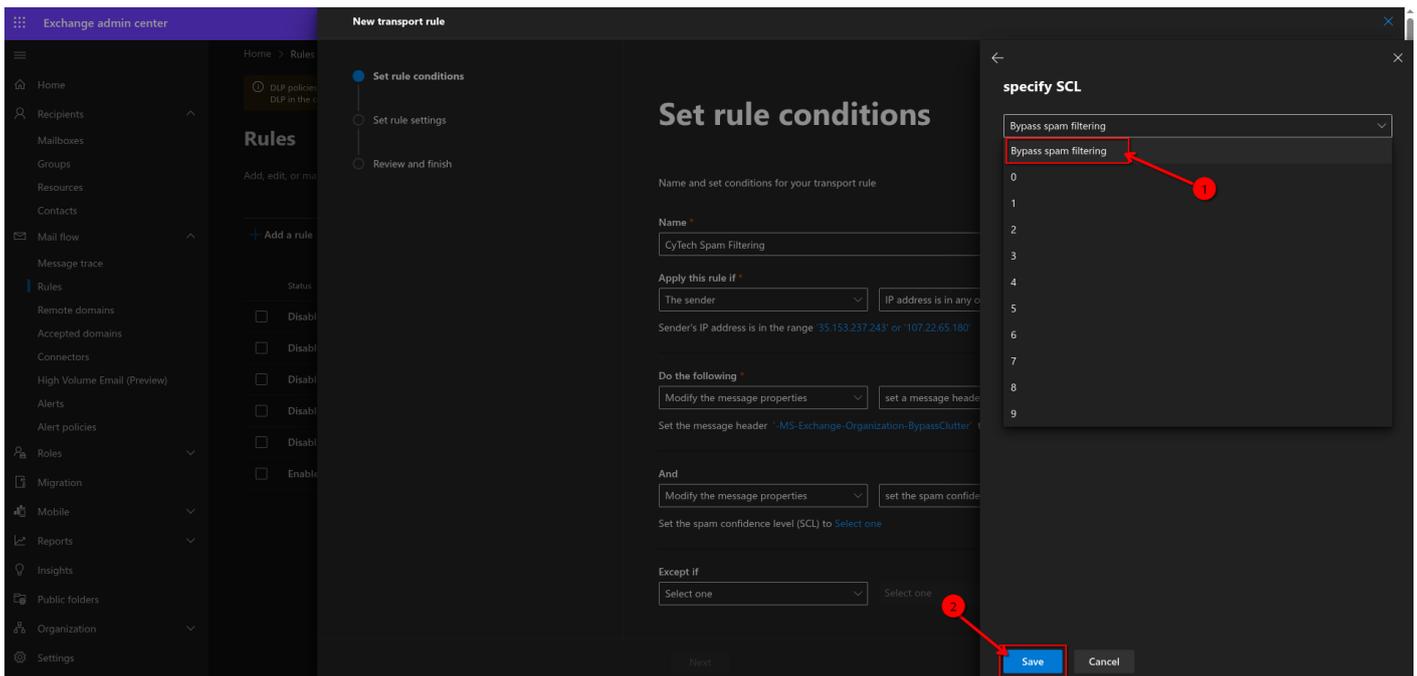
12. Click the "Enter text" buttons by the right side of the "Do the following" field and enter these values: "MS-Exchange-Organization-BypassClutter" and "true".



13. Click on the "+" sign, to add another rule condition.



14. Choose "Modify the message properties → Set the spam confidence level (SCL)" and select "Bypass Spam Filtering", this will set the value of SCL to -1. Then click "Save" button.



15. Make sure you have the same output as shown in the image below before proceeding on clicking the "Next" button.

Name *

CyTech Spam Filtering

Apply this rule if *

The sender IP address is in any of these ranges or ...

Sender's IP address is in the range '35.153.237.243' or '107.22.65.180'

And

The message headers... includes any of these words

'X-PHISHTEST' message header includes 'CYTECH'

And

The sender domain is

'slackj.com' or 'ttrelli.com' or 'airbnd.cc' or 'atlassians.com' or 'eebbey.com' or 'lastpass.net' or 'my1psswords.com' or 'zooms.cc'

Do the following *

Modify the message properties set a message header

Set the message header 'MS-Exchange-Organization-BypassClutter' to the value 'true'

And

Modify the message properties set the spam confidence level (SCL)

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

Next

16. Leave the Set Rule settings as is and proceed to the Review and finish window and save the rule.

New transport rule

○ Review and finish

Set settings for your transport rule

Rule mode

Enforce

Test with Policy Tips

Test without Policy Tips

Severity *

Not specified ▾

Activate this rule on

5/19/2025 - 6:30 PM ▾

Deactivate this rule on

5/19/2025 - 6:30 PM ▾

Stop processing more rules

Defer the message if rule processing doesn't complete

Match sender address in message *

Header ▾

Comments

Back **Next**

17. Please make sure the rule is **Enabled**, and priority is **set to "0"**. Your final Completed Mail Flow Rule screen should look as below:

CyTech Spam Filtering

 Edit rule conditions  Edit rule settings

Status: Enabled **1**

Enable or disable rule
 Enabled

Rule settings

Rule name CyTech Spam Filtering	Mode Enforce 2
Severity Not specified	Set date range Specific date range is not set
Senders address Matching Header 3	Priority 0 4

For rule processing errors
Ignore

Rule description

Apply this rule if **5**

*sender ip addresses belong to one of these ranges: '35.153.237.243' or '107.22.65.180'
and 'X-PHISHTEST' header contains "CYTECH"
and sender's address domain portion belongs to any of these domains: 'slackj.com' or 'ttrelli.com' or 'airbnd.cc' or 'atlassians.com' or 'eebbey.com' or 'lastpass.net' or 'my1psswords.com' or 'zooms.cc'*

Do the following **6**

*Set the spam confidence level (SCL) to '-1'
and set message header 'MS-Exchange-Organization-BypassClutter' with the value 'true'*

Rule comments

If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.

Revision #5

Created 19 May 2025 05:53:43 by Richmond Abella

Updated 29 May 2025 10:08:01 by Richmond Abella