**Improving Security in Exchange Online Organizations**

Who can make these changes?

If you are in an organization that utilizes PIM (highly recommended), Exchange Admin is required. If not, this will need to be completed by a global administrator.

All Below tasks are handled with the following steps to start:

There are 3 example mail flow rules listed below.

* The first is creating a banner that marks when an email is external to help the recipient recognize if an external party may be falsely representing themselves as a member of your organization.
* The second is creating a banner that looks for words that have a higher likelihood of being a phishing attempt, a useful alert during periods of high volume attacks – like the current ‘voicemail retrieval’ example reflected below.
* The last is for creating rules that block spoofing of executives, a frequent and high volume attack technique for hackers.

Note: Testing Mailflow rules

1. While creating a rule, add something that only will apply to the person testing the rule.
2. For example, Click “apply this rule if” and then, “the recipient is…” only selecting your account.
3. Try to recreate something that would simulate the rule. For example, in the external email banner, I would try emailing my work account from my personal email. I would then verify that the banner looks as expected. I would also try emailing my work account from my work account. This would ensure that the banner is only appearing when needed.
4. When full functionality has been verified, you may go back into the saved rule and click the x next to “apply this rule if the sender is…” To apply the rule across the organization.

**Creating a Banner for External emails**

1. Go to portal.office.com
2. Click the 9 dots in the top left-hand corner of the screen
3. Click admin
4. Click “exchange” you may need to select “more” for this option to present itself
5. Go to Mail flow
6. Go to rules
7. Click the plus sign to create a new rule
8. Click “create a new rule” (See testing a rule for information on how to safely test mailflow rules.”
9. Name the rule appropriately.
10. On “Apply this rule if…” Select “the sender is located…” and then, “outside the organization”. Click ok.
11. On “Do the following” select “append the disclaimer”. In the specify disclaimer text box, enter in the format you would like the bar to appear, in HTML format. Below is an example. Highlighted are the fields that can be changed to suite your organizations preferences.

**<div style="background-color:#D5EAFF">**

**<span style="font-size:11pt; font-family: 'Cambria','times new roman','garamond',serif; color:#ff0000;">EXTERNAL EMAIL - </span>**

**Please use caution with email links or attachments.</div>**

**<br>**

**Appearance:**



1. **On the fall back action selection, choose wrap.**
2. **Click “more options”**
3. **Click “add action”**
4. **Select “prepend the subject with” and add a term to designate an external email. In our example, we say “[EXTERNAL]”**
5. **Add necessary exceptions. Recommended exceptions are listed below but will vary from organization to organization.**
	1. **Calendar invitations**
	2. **Ip addresses of systems used by organization**
	3. **Domains of systems used by organization**
	4. **Exclude emails that contain the designation in step 9. Ours says “Includes these words in the message subject: ‘[EXTERNAL]’. This step is critical as it will remove redundancy.**
6. **Check the box next to “audit this rule”**
7. **Select enforce**
8. **Select save**

**Creating a Banner for Suspected Phishing emails**

This banner was created as we noticed an uptick of voicemail phishing scams recently. We also have a banner that checks for Covid-19 phishing. The banner is used to warn users that emails could have a higher chance of being a phishing email, and to use extra caution when clicking links.

* Go to portal.office.com
* Click the 9 dots in the top left-hand corner of the screen
* Click admin
* Click “exchange” you may need to select “more” for this option to present itself
* Go to Mail flow
* Go to rules
* Click the plus sign to create a new rule
* Click “create a new rule” (See testing a rule for information on how to safely test mailflow rules.”
* Name the rule appropriately.
* On “Apply this rule if…” Select “the sender is located…” and then, “outside the organization”. Click ok.
* On “Apply this rule if…” Select “the subject or body includes these patterns” and input the different terms you’d like.



* On “Do the following” select “append the disclaimer”. In the specify disclaimer text box, enter in the format you would like the bar to appear, in HTML format. Below is an example. Highlighted are the fields that can be changed to suite your organizations preferences.
* **<div style="background-color:#FFFF00"> <span style="font-size:11pt; font-family: 'Cambria','times new roman','garamond',serif; color:#000000;">POTENTIAL PHISH - </span> Suspicious 'voicemail' attachment identified</div> <br>**

**Appearance:** 

* **Select “prepend the subject with” and add a term to designate an external email. In our example, we say “[POTENTIAL PHISH]”**
* **Add necessary exceptions. For examples, please view the external email banner documentation.**
* **Check the box next to “audit this rule”**
* **Select enforce**
* **Select save**

**Blocking Executive Spoofing**

* Go to portal.office.com
* Click the 9 dots in the top left-hand corner of the screen
* Click admin
* Click “exchange” you may need to select “more” for this option to present itself
* Go to Mail flow
* Go to rules
* Click the plus sign to create a new rule
* Click “create a new rule” (See testing a rule for information on how to safely test mailflow rules.”
* Name the rule appropriately.
* Click more options (this will populate all possible fields in the next step.)
* On “Apply this rule if…” select “the sender is…” and “has specific properties matching these text patterns”
* On the page that appears, you will be asked to select a property for each sender. Select display name for each, and then the first name/ last name of each executive.
	+ 
* **Press “OK”**
* **Select Add condition**
* On “Apply this rule if…” select “a message header…” and “matches these text patterns”
* **In “enter text” type** “Received-SPF”
* **In “matches” type “none”**
* **On “do the following” Choose an action. We recommend selecting “Redirect the message to” and sending to an IT security monitored inbox. This allows IT insight into potential spoofing attempts. If you choose to not go this route, we recommend setting the message to a high spam confidence score so it will be filtered as such.**
* **List exceptions. This will include ips and domains that are allowed to spoof these people. Examples would be personal emails, and 3rd party resources that are approved to spoof.**
* **Select audit**
* **Click enforce**
* **Click Save**