Security Awareness Safelisting in Microsoft 365

Question

How do I safelist Proofpoint Security Awareness Training within Office 365?

Answer

Follow the steps below to Safelist in Office 365:

Create a Transport Rule

Create a Transport Rule if the mock-phish has landed in your Junk or Spam folders. You may create a transport rule that sets the SCL (Spam Confidence Level) of the emails sent from Phishing to -1.

1. Login to the **Office 365 Admin** portal.
2. Select the **Admin Center i**con and then select **Exchange** from the menu to access the **Exchange Admin Center (EAC).**
3. Click **mail flow** and then **rules,** then click the **+** icon to **Create a new rule.**
4. Enter a **name** for the new rule.
5. Choose **More options . . .** This must be done to continue setting up the Rule.
6. Select the appropriate option below - **IP Address** or **Message Header**

For IP Address

a. From the drop-down menu, ***Apply this rule if …,** select **The sender**…, then select **IP Address is in any of these ranges or exactly matches.**
b. Enter Proofpoint Security Awareness Training's IP addresses into the dialog box. Click the **+** icon to add **multiple IPs.**

Note: The IPs for your server can be found in our Safelisting Guide on the Community

c. Click **OK**.
d. From the drop-down menu, ***Do the following …**, select **Modify the message properties**…, then select **set the spam confidence level (SCL)**
e. Select **Bypass spam filtering** and click **OK.** This sets the **SCL to -1.**
f. All other settings can be left with the default setting. Click **Save** at the lower right of the rule.

For information on Bypassing Microsoft ATP Safe Links and Safe Attachments, see Bypass ATP Attachment Processing and Bypass ATP Link Processing

For Message Header

a. From the drop-down menu, *Apply this rule if …, select **A message header**…, then select **includes any of these words** is in any of these ranges or exactly matches.

b. Enter the Searchable Header information for phishing emails and click **OK**.

c. Next to the header, select “**Enter words**… and input the value assigned with the header. Click **+** then **OK**.

d. From the drop-down menu, ***Do the following** …, select **Modify the message properties**…, then select **set the spam confidence level (SCL)**. Select **Bypass spam filtering** and click **OK**. This sets the **SCL to -1.**

e. Select **add action** and choose **Modify the message properties**… and **set a message header**.

f. Select **“Enter text**… to enter the following: **X-MS-Exchange-Organization-SkipSafeAttachmentProcessing**

g. Click **OK** and select **“Enter text**… to provide a value of **1**. Click **OK**.

h. All other settings can be left with the default setting. Click **Save** at the lower right of the rule.

i. Repeat steps under **For Message Header**, entering the following within **Step f: X-MS-Exchange-Organization-SkipSafeLinksProcessing**

Setting up a Connector

If you are seeing a significant delay between the time you send a Phish and the time it is received, it will be necessary to setup a Connector.

1. Login to the Office 365 Admin portal.
2. Select the **Admin Center** icon and then select **Exchange** from the menu to access the **Exchange Admin Center (EAC).**
3. Click **mail flow** and then **Connectors,** then click the

   icon to create a new rule.
4. Select your **Mail Flow Scenario** and set the **From** to **Partner Organization** and **To** to **Office 365** then click **Next.**
5. Select the **Name of the Connector** and a write an **optional description**. You will then want to make sure the box underneath **What do you want to do after connector is saved?** is checked and click **Next.**
6. Choose how Proofpoint Security Awareness Training should be identified. You will want to **Use the sender’s IP address**, then click **Next.**
7. Enter our IP addresses into the dialog box. Click the icon

   to add multiple IPs. Click **Next** when done.
8. Check the box - **Reject email messages if they aren't sent over TLS**, Click **Next** when done.
9. Click **Save**

Microsoft ATP

ATP provides limited abilities for safelisting or creating exceptions directly for Attachments or Safe Links. Mail Flow

Rules can be setup to insert Headers into the received emails that allow the system to bypass the ATP functions for those messages. This can be configured based on the sending IP addresses so that only those emails received from Proofpoint are subject to this behavior.

The following two rules will need to be created to set the following headers and values:

- X-MS-Exchange-Organization-SkipSafeAttachmentProcessing to a value of 1
- X-MS-Exchange-Organization-SkipSafeLinksProcessing to a value of 1

This will allow those emails to pass to the end users, without being subjected to the scanning that is creating false positive results.

After modifying Exchange, allow up to 12 hours for the configuration to propagate.

By applying the Actions within the transport rule, any messages coming from the Platform will bypass the ATP functions for those messages. This will allow those emails to pass to the end users, without being subjected to the scanning that is creating false positives