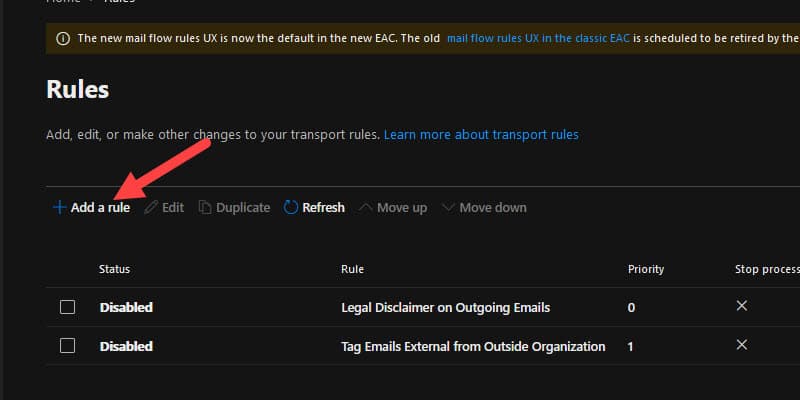
**Report on Implementation of Disclaimer Banner for External Emails**

**Introduction:** The following report outlines the process and steps involved in implementing a disclaimer banner for external emails in our company's email system. The purpose of this implementation is to alert users to potential risks associated with external emails and encourage caution when interacting with their contents.

**Background:** Email remains one of the most common vectors for cyber threats, including phishing attacks and malware distribution. As part of our ongoing efforts to enhance cybersecurity measures, we have implemented a disclaimer banner for external emails. This banner serves as a visual indicator to users that the email originates from an external source and may pose a higher risk.

**Implementation Steps:**

1. **Access Email Defender Administration Console:**
   * Log in to the Exchange Admin Center at [https://admin.exchange.microsoft.com](https://admin.exchange.microsoft.com/).
2. **Navigate to Email Policy Settings:**
   * In the Exchange Admin Center, go to the Mail Flow section and select Rules.
   * Click on "Add a Rule" and then choose "Create a new rule."

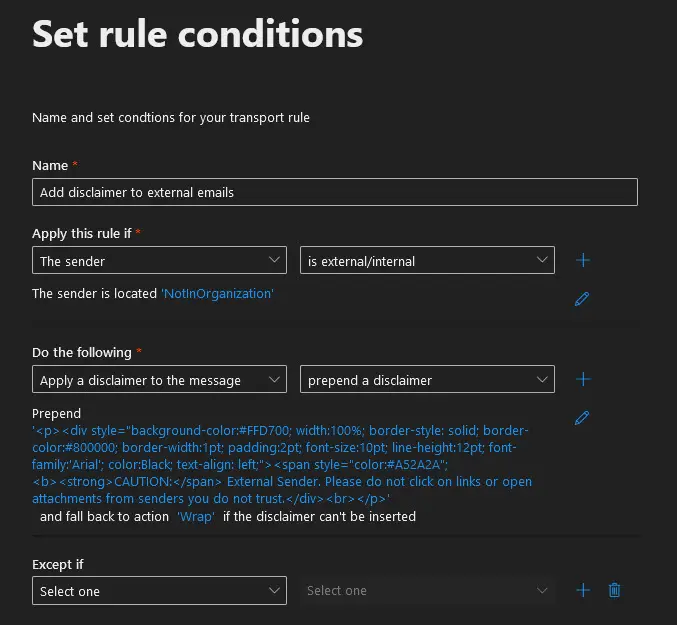


1. **Create New Policy Rule for External Emails:**
   * Give the rule a descriptive name, such as "Add disclaimer to external emails."
   * Set the condition to apply the rule if the sender is external, located outside the organization.
2. **Define Conditions for External Emails:**
   * Specify conditions for external emails, ensuring the rule applies only to messages originating from outside the organization.
   * Choose the condition based on the sender's location. Select "The Sender" and specify "is external/internal," then choose "Outside the organization." The sender's location will display as "NotInOrganization."
3. **Add Action to Insert Disclaimer Banner:**
   * Choose to apply a disclaimer to the message and select "prepend a disclaimer."
   * Entered the below HTML code for the disclaimer banner, which includes a caution message and instructions for users.

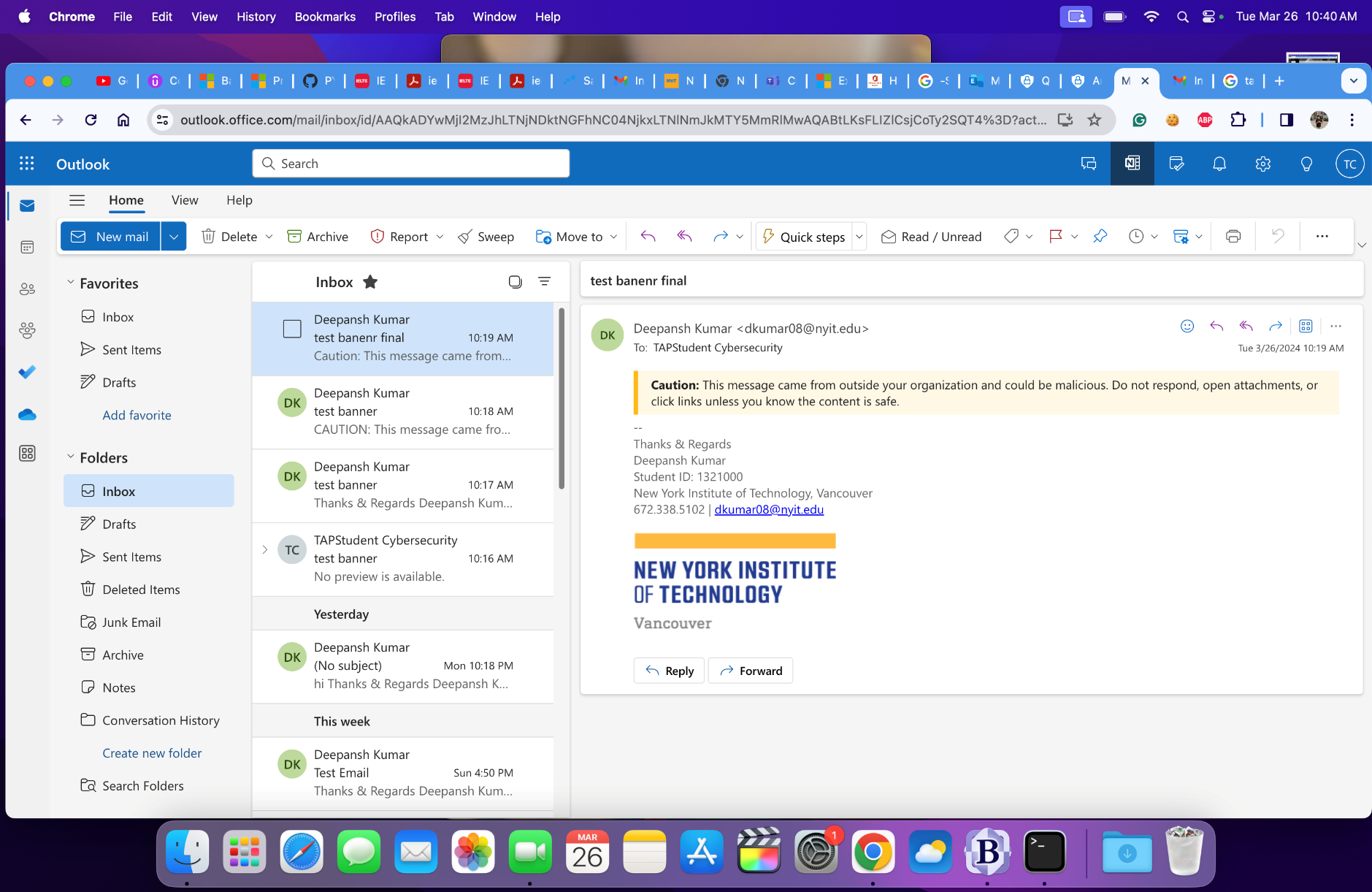
*<!-- Red Banner -->  
<table border=0 cellspacing=0 cellpadding=0 align="left" width="100%">  
<tr>  
<td style="background:#ff0000;padding:5pt 2pt 5pt 2pt"></td>*

*<td width="100%" cellpadding="7px 6px 7px 15px" style="background:#ff000;padding:5pt 4pt 5pt 12pt;word-wrap:break-word">  
<div style="color:#000000;">  
<span style="color:#000000; font-weight:bold;">Caution:</span>  
        This is an external email and may be malicious. Please take care when clicking links or opening attachments.  
</div>  
</td>  
</tr>  
</table>*  
<br />

1. **Customize Disclaimer Banner:**
   * Customize the disclaimer banner text as needed to align with company policies and guidelines.
2. **Save and Apply Policy Rule:**
   * Review the rule settings, set the priority, and ensure the rule mode is set to "Enforce."
   * Your rule should look like the below picture:



1. **Test Configuration:**
   * Send a test email from an external source to verify that the disclaimer banner is inserted correctly at the top of the email.
   * It should look something like below image.



1. **Monitor and Adjust as Needed:**
   * Regularly monitor the effectiveness of the disclaimer banner feature and make adjustments to the text or rule settings as necessary.
2. **Train Users on Significance of Disclaimer Banner:**
   * Conduct user awareness training sessions to educate employees about the presence and significance of the disclaimer banner.
   * Emphasize the importance of exercising caution when interacting with external emails and following company guidelines.

**Conclusion:** The implementation of a disclaimer banner for external emails represents a proactive step in strengthening the company's cybersecurity defenses. By alerting users to potential risks associated with external emails, we aim to reduce the likelihood of falling victim to phishing attacks or other malicious activities. Continued monitoring and user education will be key to ensuring the ongoing effectiveness of this security measure.