**Report: Enhancing Microsoft 365 Security by Blocking File Types**

**Introduction:** Microsoft 365 offers default threat policies, but they may not cover all potential security risks. One critical aspect of improving Microsoft 365 security is blocking file types that can pose a threat to your organization. This report outlines the steps and rationale for implementing a file type blocking policy in Microsoft 365.

**Objective:** The primary objective of this initiative is to enhance the security posture of our organization by proactively blocking specific file types that could potentially contain malicious content. By implementing this measure, we aim to reduce the risk of cyber threats, protect sensitive data, and strengthen our overall security infrastructure.

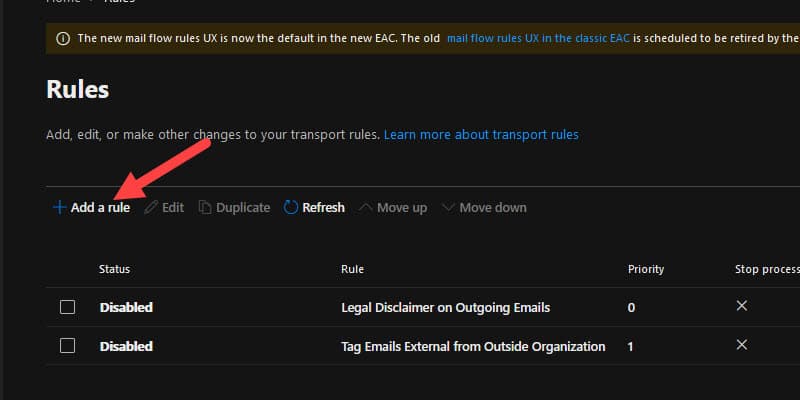
**Why Block File Types?**

Blocking file types in Microsoft 365 is essential for several reasons:

1. **Enhancing Security:** Adding an extra layer of security helps prevent malicious files from infiltrating our organization's network.
2. **Mitigating Risks:** Blocking dangerous file types reduces the risk of users inadvertently downloading and executing harmful content, minimizing the potential for data breaches and system downtime.
3. **Proactive Defense:** Taking proactive measures to block known risky file extensions helps prevent security incidents before they occur, keeping us ahead of emerging threats.
4. **Strengthening Infrastructure:** Blocking potentially harmful file types strengthens our overall infrastructure resilience against cyberattacks, ensuring the integrity and availability of critical systems and services.

**Implementation Steps:**

1. **Log into Exchange Admin Center:**
   * 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 a New Rule:**
   * Give the rule a descriptive name, such as "Block File Types."
   * Click on More options to see additional settings.
   * Set the condition to apply the rule.
2. **Set Rule Conditions:**
   * Under Apply this rule, select "The sender is located" and choose "Outside the organization."
   * Add another condition. Select "Any attachment" and then "file extension includes these words."
   * Following are the default file types suggested to and implemented to be blocked.

*ace, ani, apk, app, appx, arj, bat, cab, cmd, com, deb, dex, dll, docm, elf, exe, hta, img, iso, jar, jnlp, kext, lha, lib, library, lnk, lzh, macho, msc, msi, msix, msp, mst, pif, ppa, ppam, reg, rev, scf, scr, sct, sys, uif, vb, vbe, vbs, vxd, wsc, wsf, wsh, xll, xz, z*

* + Enter the file extensions you want to block.
  + Add any other condition if necessary.

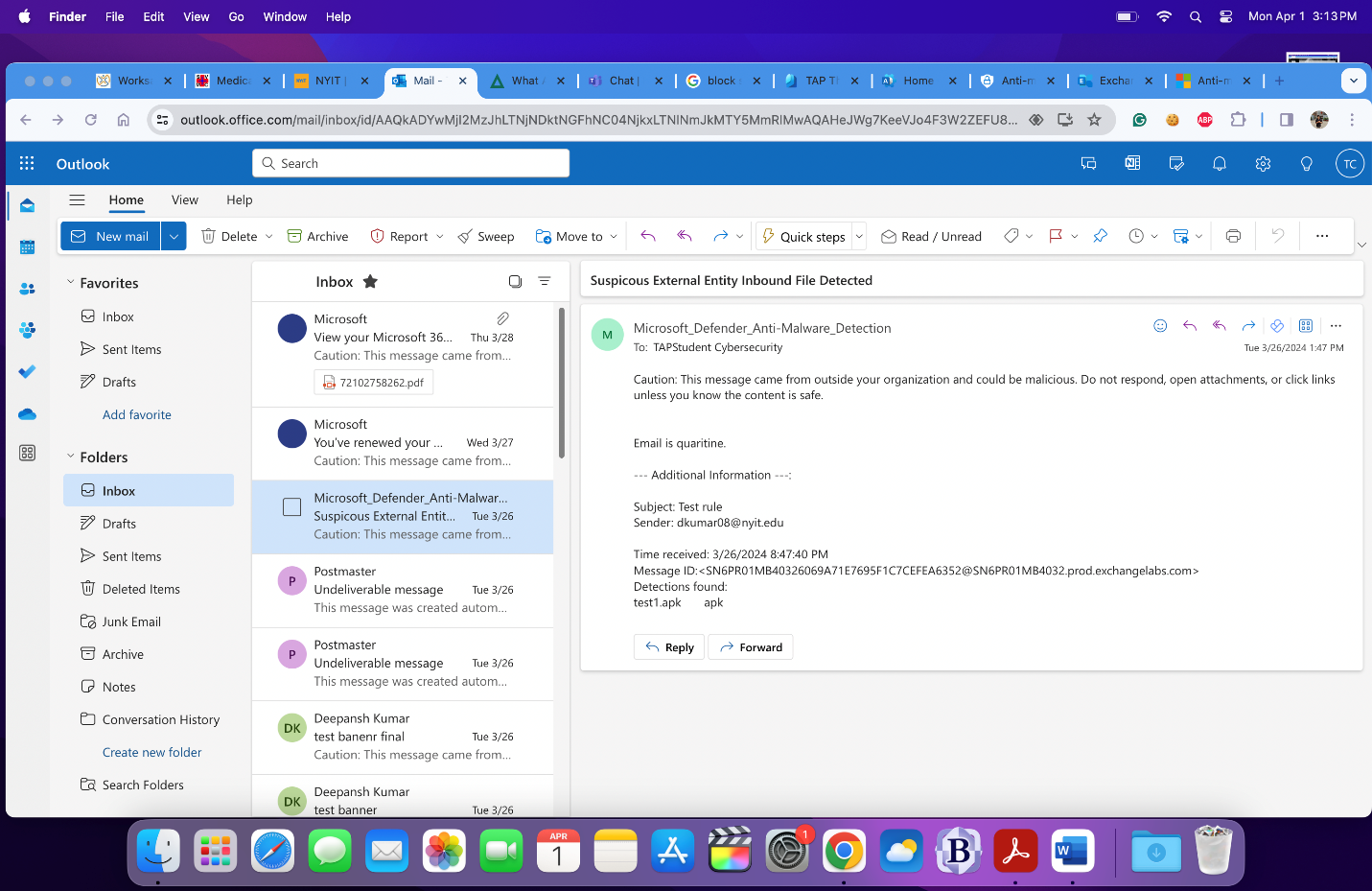
1. **Add Action and Define Rejection Reason:**
   * Under Do the following, select "Block the message" or "Delete the message without notifying anyone."
   * Click on "Modify the message properties" to specify a rejection reason.
   * Enter a brief explanation for why the message was blocked which would be seen on the emails when such email is received, any message such as "File type blocked for security reasons."
   * Added message as suggested by the organization.

*“Subject Line: QUARANTINE ALERT: Suspicious File Detected*

*Body text: This email has been quarantined. To review, please go to instructions on how to access quarantine”*

1. **Add Exception for Trusted Senders:**
   * Click on "Except if..." to add exceptions to the rule.
   * Choose "The sender is located" and select "Inside the organization" if you want to allow trusted internal senders to bypass the rule.
   * Alternatively, select "The sender..." to specify specific trusted senders by email address or domain.
   * Configure the exception criteria based on your organization's requirements.
   * Added exceptions for the following domains as suggested by the organization.

1. **Enable the Rule:**
   * Review the rule settings to ensure they are correct.
   * Click on Save to create the rule.
   * Go back to the Rules tab and find the newly created rule.
   * Toggle the status from "Off" to "On" to enable the rule.
2. **Test and Monitor:**
   * Send test emails with attachments that match the blocked file types to ensure they are being blocked as expected. It should look something like below image.



* + Monitor the rule's performance and adjust settings if necessary.
  + Regularly review and update the rule to adapt to changing security threats.

**Conclusion:** Implementing a file type blocking policy in Microsoft 365 is a proactive step towards enhancing our organization's security posture. By blocking specific file types known to carry malicious content, we can reduce the risk of cyber threats, protect sensitive data, and fortify our infrastructure against evolving security challenges. Moving forward, we will continue to evaluate and optimize our security measures to ensure robust protection against emerging threats.