VERSION 1.0

Cyber Risk Aware
Creating your human firewall!

EXCHANGE/OUTLOOK AUTOMATIC IMAGE DOWNLOAD POLICY

HOW TO ENABLE

WWW.CYBERRISKAWARE.COM

CONTENTS

OBJECTIVE

To improve the monitoring and measurement accuracy of CyberRiskAware within your organization and to gain nearly 100% email view tracking rates, your organization's IT or Exchange administrators can configure group polices to enable automatic picture download for exchange email communications.

Automatic picture download allows CyberRiskAware to track email views more consistently, and therefore yielding more accurate email metrics reporting. This is done by simply placing a 1px image within the email content that is linked back to our site. When the email client tries to download the image, we know that the email has been viewed.

By default, Outlook does not download pictures or other content automatically, except when the external content comes from a Web site in the Trusted Sites zone, or from an address or domain specified in the Safe Senders List. Your IT or Exchange admins can change this default behavior and allow CyberRiskAware to track viewed emails by adding the relevant domains to your Exchange servers Safe Senders List.

OPTIONS

There are a few ways to achieve the above objective, below we have outlined the tasks involved to implement the two most common solutions.

1. Use Group Policy to add CyberRiskAware domains to the Safe Senders List
2. Allow Automatic Download of Images across your Organization

USE GROUP POLICY TO ADD CYBERRISKAWARE DOMAINS TO THE SAFE SENDERS LIST

The following procedures can be used to adjust your Safe Senders lists to allow CyberRiskAware to accurately record mock phishing email views.

CREATE THE JUNK EMAIL FILTER SAFE SENDERS LIST FILE

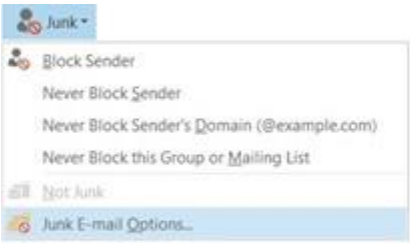
If your organization does not already have a Safe Senders list, then your first task should be to create one.

First, create the list on a test computer. This is the same procedure that a user would follow to create junk email filter lists. After you create it, configure it using the OCT, and deploy them using a network share.

To create the default junk email filter Safe Senders list

1. Install Outlook 2013 on a test computer.
2. Start Outlook 2013.
3. In Outlook 2013, click the **Home** tab. In the **Delete** group, click **Junk**, and click **Junk email options**.

   Junk menu, Junk email options drop-down list.

   
   Junk
Block Sender
Never Block Sender
Never Block Sender's Domain (@example.com)
Never Block this Group or Mailing List
Not Junk
Junk E-mail Options...

4. On the **Safe Senders** tab, click **Add**.
5. Enter an email address, for example,

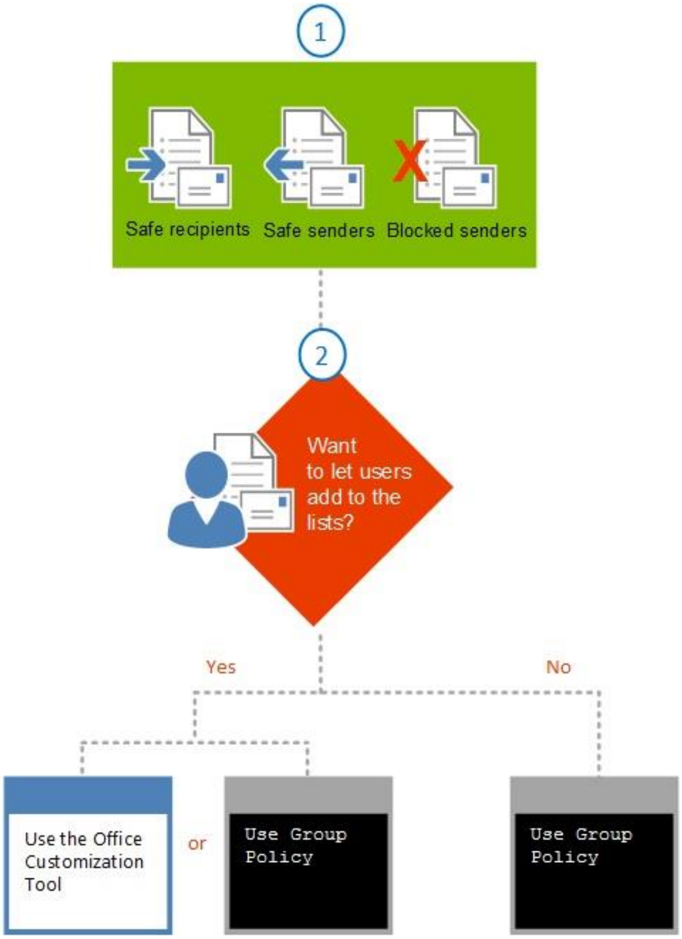
   someone@exchange.example.com

6. Click **OK**.
7. To add more email addresses, repeat steps 3 through 6.
8. Click **Export to file**. (*While this is a .txt file that can be created outside of Outlook, we do not recommend that you do so. When you create the file from within Outlook, file formatting and elements like carriage returns are all in the right places*.)
9. Enter a unique file name for the Safe Senders list, and click **Save**.

CONFIGURE JUNK EMAIL SETTINGS AND SAVE THE JUNK EMAIL FILTER FILE CHANGES

You can configure the junk email settings using either Group Policy or the Office Customization Tool (OCT). Which you should use depends on whether you want users to be able to add to the filter lists you've created and if so, whether you want their changes to persist after either they restart Outlook or they receive a junk email filter list update from you.

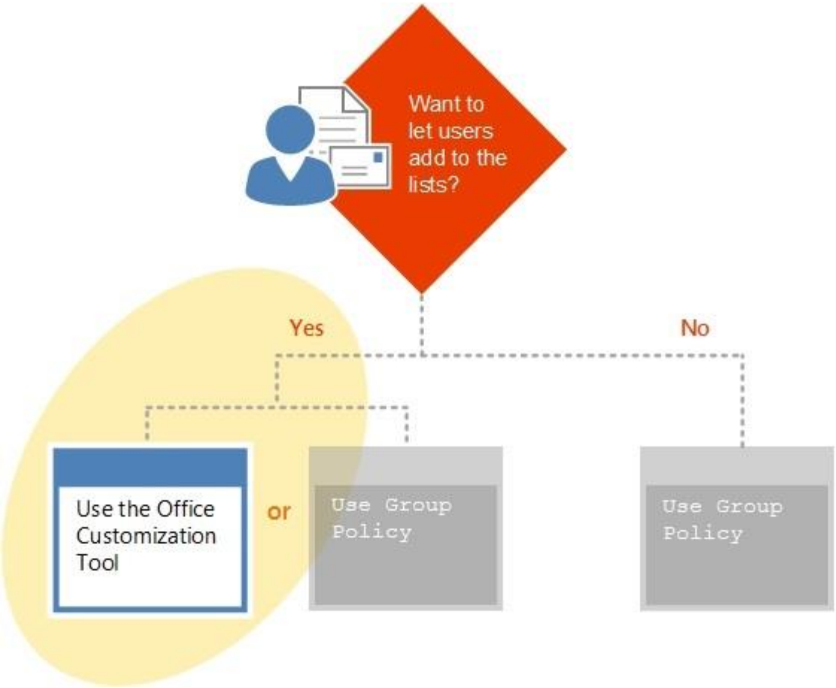
Junk email configuration tool decision tree. Use the OCT or Group Policy?



If you want users to be able to customize the filter files and retain their customizations, disable the Overwrite or Append Junk Mail Import List option using either the OCT or Group Policy. If you want to always overwrite users' customizations, use Group Policy and enable the Overwrite or Append Junk Mail Import List option.

To allow user customization of the filter files—use the Office Customization Tool (OCT)

1. **Use the OCT to configure junk email filter files for users.**


Want to let users add to the lists?
Yes
No
Use the Office Customization Tool
or
Use Group Policy
Use Group Policy

Copy the Safe Senders junk email filter files that you just created to a network file share.

2. (*Optional*) If you have remote users not connected to the domain, do the following:
   a. In the OCT, click **Add Files** > **Add**.
   b. In the **Add Files to MSP File** dialog box, browse to the Safe Senders junk email filter file that you just created, and select it.
   c. Click **Add**.
   d. In the **File Destination Path** dialog box, in the **Destination path on the user's computer** box, enter the folder where you want to install the file on users' computers, and click **OK**.
3. In the OCT, in the tree view, click **Modify User Settings**.
4. In the reading pane, expand **Microsoft Outlook 2013**, expand **Outlook Options**, expand **Preferences**, and click **Junk email**.
5. Double-click **Trigger to apply junk email list settings**, and click **Enabled** > **OK** to apply the settings and import the junk email filter lists for users.
6. **Important:** This is the step that will cause user customizations to the junk email filter lists that you deploy to be appended to the files or overwritten after you initially deploy the default lists.

   To keep user changes to an existing junk email filter both after the user restarts Outlook and when new email filter lists are deployed, double-click **Overwrite or Append Junk Mail Import List**, then click **Enabled** > **OK**.

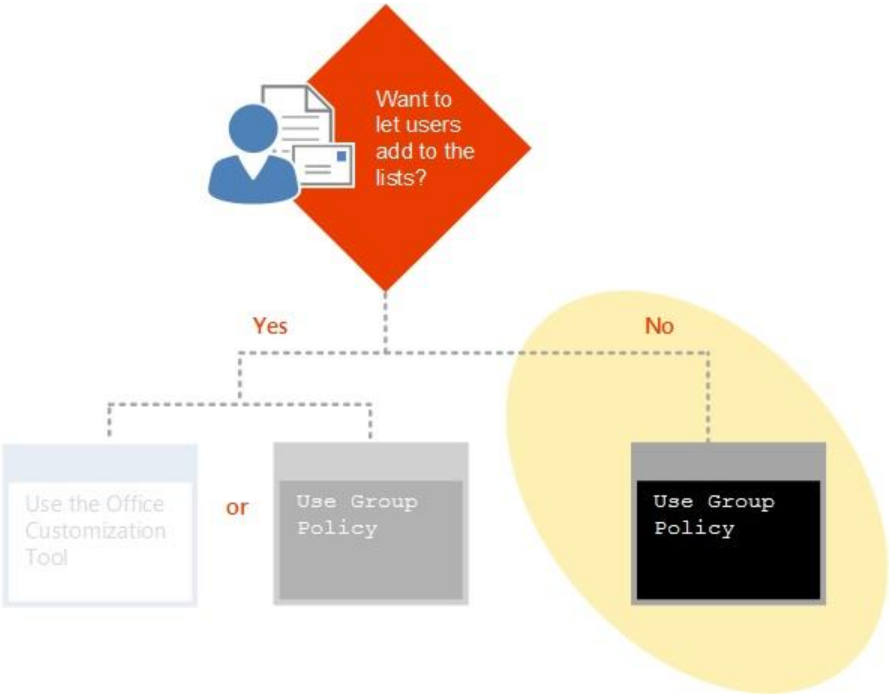
7. To specify a path for each junk email filter list, open the settings for the list, **Specify path to Safe Senders**, click **Enabled**, and enter a path and file name in the.
8. Click **OK**.
9. On the **File** menu, click **Save** to create the customization file that you can deploy to users.

Later, you can change an existing Outlook 2013 installation to update the junk email filter lists by following this same procedure and specifying your updated junk email filter files.

The **Office Customization Tool (OCT) reference** (*http://go.microsoft.com/fwlink/p/?linkid=212778*) for Office 2013 tells you lots more about how to use the OCT to configure an Office installation before deployment.

To lock out user filter file customizations so that any changes users make are always overwritten in a new Outlook session—use Group Policy

1. **Use Group Policy to configure junk email filter files for users.**


Want to let users add to the lists?
Yes
No
Use the Office Customization Tool
or
Use Group Policy
Use Group Policy

In Group Policy, load the Outlook 2013 template, and open **User Configuration\Administrative Templates\Microsoft Outlook 2013\Outlook Options\Preferences\Junk Email**.

2. Configure the appropriate Junk Email settings:

Automatic picture download option	Description
Automatically download content for e-mail from people in Safe Senders and Safe Recipients lists	Enable this option to automatically download content when e-mail message is from someone in the user's Safe Senders list or to someone in the user's Safe Recipients list.
Block Trusted Zones	Disable this option to include Trusted Zones in the Safe Zones for Automatic Picture Download.
Display pictures and external content in HTML e-mail	Enable this option to automatically display external content in HTML mail.

Do not permit download of content from safe zones	Disable this option to automatically download content for sites in Safe Zones (as defined by Trusted Zones, Internet, and Intranet settings).
Include Internet in Safe Zones for Automatic Picture Download	Automatically download pictures for all Internet e-mail.
Include Intranet in Safe Zones for Automatic Picture Download	Automatically download pictures for all Intranet e-mail

3. Click OK.

CONFIGURE AUTOMATIC PICTURE DOWNLOAD—WEB BEACON PROTECTION

As with the filter file settings described above, you can lock down the setting to customize how Outlook automatically downloads pictures by using the Outlook 2013 Group Policy template. Or, if you want to allow users to change this, set it using the OCT.

To prevent automatic download of Internet content—use Group Policy

1. In Group Policy, load the Outlook 2013 template.
2. Under **User Configuration\Administrative Templates\Microsoft Outlook 2013\Security**, click **Automatic Picture Download Settings**.
3. Open **Automatically Download Content for E-Mail from People in Safe Senders and Safe Recipients Lists**.
4. Click **Enabled** > **OK**.

To allow automatic download of Internet content—use the Office Customization Tool

1. In the OCT, on the **Modify user settings** page, under **Microsoft Outlook 2013\Security\Automatic Picture Download Settings**, open **Automatically Download Content for E-Mail from People in Safe Senders and Safe Recipients Lists**, and click **OK**.
2. On the **File** menu, click **Save** to create the customization file that you can deploy to users.

THE CYBERRISKAWARE DOMAINS

CYBERRISKAWARE CONTROLLED DOMAINS

The following are the CyberRiskAware default domains where our mock phishing emails are sent from, these domains should be added to the safe senders list:

cyberriskaware.com	e-messages.com
emessages.com	e-citrix.com
ecompliants.com	e-compliants.com
efaax.com	e-faax.com
e-gmail.com	eonline-shopping.com
e-outlook.com	e-owa.com
evpnn.com	e-vpnn.com
orders-processed.com	storage-limit.com

CUSTOM SEND FROM DOMAINS

If your organization intends to use the Custom From feature to send phishing emails from domains other than your own or the CyberRiskAware domains, then these should be added to the safe senders list also.

CYBERRISKAWARE EMAIL SERVER IP

If your IT admins would prefer to whitelist using an IP address, then they can use our mail server address which is: 192.254.120.51

ALLOW AUTOMATIC DOWNLOAD OF IMAGES ACROSS YOUR ORGANIZATION

To allow automatic download of Internet content—use Group Policy

1. In Group Policy, load the Outlook 2013 template.
2. Under **User Configuration\Administrative Templates\Microsoft Outlook 2013\Security**, click **Automatic Picture Download Settings**.
3. Open **Display pictures and external content in HTML e-mail**
4. Click **Enabled** > **OK**.

To allow automatic download of Internet content—use the Office Customization Tool

3. In the OCT, on the **Modify user settings** page, under **Microsoft Outlook 2013\Security\Automatic Picture Download Settings**, open **Display pictures and external content in HTML e-mail**, and click **OK**.
4. On the **File** menu, click **Save** to create the customization file that you can deploy to users.

EXCHANGE AUTOMATIC DOWNLOAD POLICY REFERENCES

*AUTOMATICALLY DOWNLOAD CONTENT FOR E-MAIL FROM PEOPLE IN SAFE SENDERS AND SAFE RECIPIENTS LISTS

This policy setting controls whether Outlook automatically downloads external content in e-mail from senders in the Safe Senders List or Safe Recipients List.

If you enable this policy setting, Outlook automatically downloads content for e-mail from people in Safe Senders and Safe Recipients lists.

If you disable this policy setting, Outlook will not automatically download content from external servers for messages sent by people listed in users' Safe Senders Lists or Safe Recipients Lists. Recipients can choose to download external content on a message-by-message basis.

If you do not configure this policy setting, downloads are permitted when users receive e-mail from people listed in the user's Safe Senders List or Safe Recipients List.

Registry Hive:	HKEY_CURRENT_USER
Registry Path:	software\policies\microsoft\office\15.0\outlook\options\mail
Value Name:	unblockspecificsenders
Value Type:	REG_DWORD
Enabled Value:	1
Disabled Value:	0

CyberRiskAware Requirement: This setting should either be unconfigured or set to enabled.

DISPLAY PICTURES AND EXTERNAL CONTENT IN HTML E-MAIL

This policy setting controls whether Outlook downloads untrusted pictures and external content located in HTML e-mail messages without users explicitly choosing to download them.

If you enable this policy setting, Outlook will not automatically download content from external servers unless the sender is included in the Safe Senders list. Recipients can choose to download external content from untrusted senders on a message-by-message basis.

If you disable this policy setting, Outlook will display pictures and external content in HTML e-mail automatically.

If you do not configure this policy setting, Outlook does not download external content in HTML e-mail and RSS items unless the content is considered safe. Content that Outlook can be configured to consider safe includes:

- Content in e-mail messages from senders and to recipients defined in the Safe Senders and Safe Recipients lists.

- Content from Web sites in Internet Explorer's Trusted Sites security zone.
- Content in RSS items.
- Content from SharePoint Discussion Boards. Users can control what content is considered safe by changing the options in the "Automatic Download" section of the Trust Center. If Outlook's default blocking configuration is overridden, in the Trust Center or by some other method, Outlook will display external content in all HTML e-mail messages, including any that include Web beacons.

Registry Hive:	HKEY_CURRENT_USER
Registry Path:	software\policies\microsoft\office\15.0\outlook\options\mail
Value Name:	blockextcontent
Value Type:	REG_DWORD
Enabled Value:	1
Disabled Value:	0

CyberRiskAware Requirement: setting this value to enabled will blanket download email content for any messages in your org, although this will allow CyberRiskAware to function better, it is not required if the Safe Senders list is configured.

DO NOT PERMIT DOWNLOAD OF CONTENT FROM SAFE ZONES

This policy setting controls whether Outlook automatically downloads content from safe zones when displaying messages.

If you enable this policy setting content from safe zones will be downloaded automatically.

If you disable this policy Outlook will not automatically download content from safe zones. Recipients can choose to download external content from untrusted senders on a message-by-message basis.

If you do not configure this policy setting, Outlook automatically downloads content from sites that are considered "safe," as defined in the Security tab of the Internet Options dialog box in Internet Explorer.

Important - Note that this policy setting is "backward." Despite the name, disabling the policy setting prevents the download of content from safe zones and enabling the policy setting allows it.

Registry Hive:	HKEY_CURRENT_USER
Registry Path:	software\policies\microsoft\office\15.0\outlook\options\mail
Value Name:	unblocksafezone
Value Type:	REG_DWORD
Enabled Value:	0
Disabled Value:	1

CyberRiskAware Requirement: Not required

INCLUDE INTERNET IN SAFE ZONES FOR AUTOMATIC PICTURE DOWNLOAD

This policy setting controls whether pictures and external content in HTML e-mail messages from untrusted senders on the Internet are downloaded without Outlook users explicitly choosing to do so.

If you enable this policy setting, Outlook will automatically download external content in all e-mail messages sent over the Internet and users will not be able to change the setting.

If you disable or do not configure this policy setting, Outlook does not consider the Internet a safe zone, which means that Outlook will not automatically download content from external servers unless the sender is included in the Safe Senders list. Recipients can choose to download external content from untrusted senders on a message-by-message basis.

Registry Hive:	HKEY_CURRENT_USER
Registry Path:	software\policies\microsoft\office\15.0\outlook\options\mail
Value Name:	internet
Value Type:	REG_DWORD
Enabled Value:	1
Disabled Value:	0

CyberRiskAware Requirement: Not required

INCLUDE INTRANET IN SAFE ZONES FOR AUTOMATIC PICTURE DOWNLOAD

This policy setting controls whether pictures and external content in HTML e-mail messages from untrusted senders on the local intranet are downloaded without Outlook users explicitly choosing to do so.

If you enable this policy setting, Outlook will automatically download external content in all e-mail messages sent over the local intranet and users will not be able to change the setting.

If you disable or do not configure this policy setting, Outlook does not consider the local intranet a safe zone, which means that Outlook will not automatically download content from other servers in the Local Intranet zone unless the sender is included in the Safe Senders list. Recipients can choose to download external content from untrusted senders on a message-by-message basis.

Registry Hive:	HKEY_CURRENT_USER
Registry Path:	software\policies\microsoft\office\15.0\outlook\options\mail
Value Name:	intranet
Value Type:	REG_DWORD
Enabled Value:	1
Disabled Value:	0

CyberRiskAware Requirement: Not required