Email Filtering (Mimecast) User Guide

Issued by: IT Integration Office
Last updated: 27-Oct-21

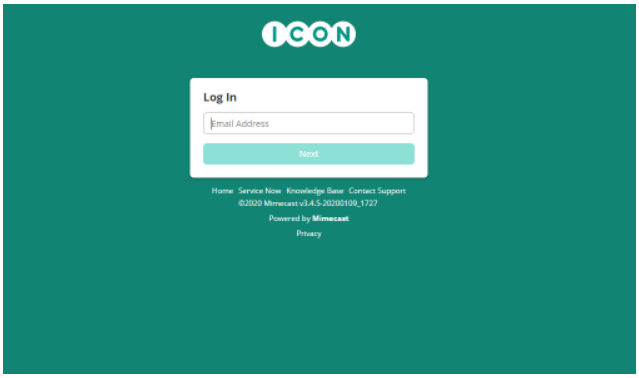
Mimecast User Guide

Table of Contents

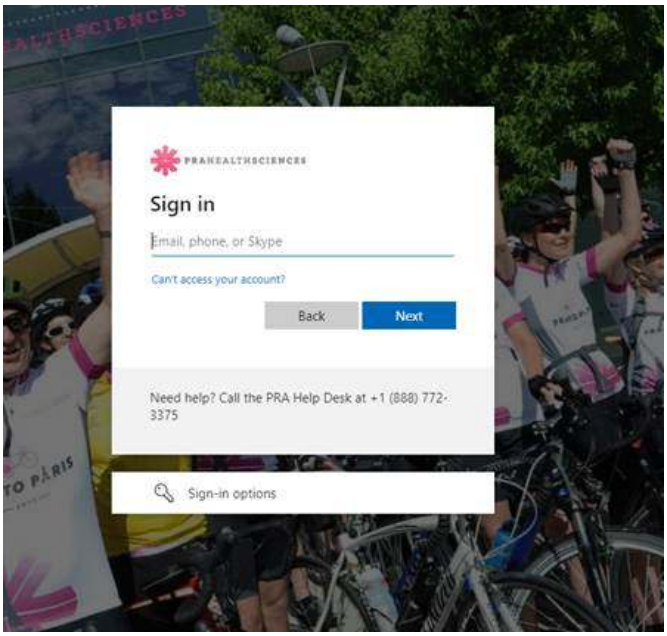
1. How to Log into the Mimecast Personal Portal

1. Open a browser and go to the following site:
   https://iconplc.login-uk.mimecast.com/m/portal/login/#/login

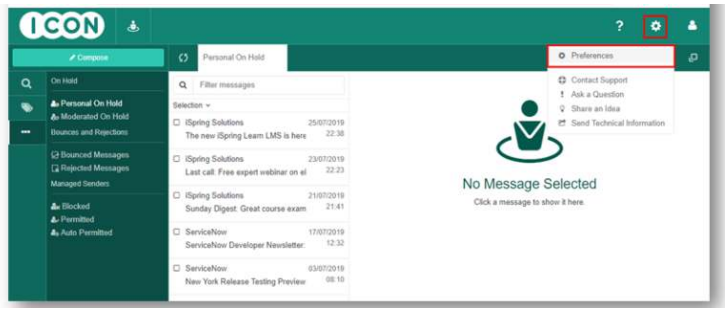
2. Once the page has loaded, the main login screen is displayed. Enter your primary email address and click Next.



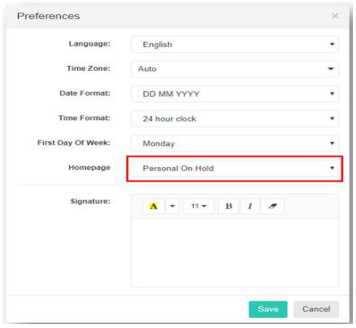
3. If you are accessing Mimecast Personal Portal outside LPRA Office you will be subject to LPRA Multi Factor Authentication. On the MFA screen, please authenticate as you normally would.



4. The first time you login the default home page view is your Inbox.
   For convenience many people prefer their home page to be the *Personal On Hold Queue.*
   To update the Home Page setting to open your *Personal On Hold queue…*
   Go to Settings - Preferences at the top right-hand corner of the page and configure as demonstrated in the screenshots below.



5. Select **Personal On Hold** on Homepage option and click **Save**.



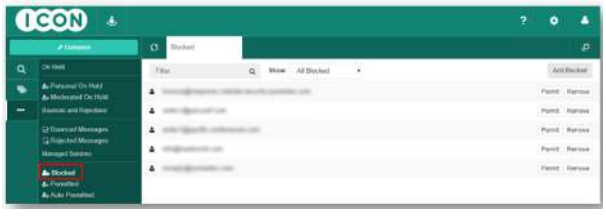
Note: other options available to change in **Preferences** are **Time Zone, Date Format, Time Format** and **First Day of Week.**

Managing Senders (Block, Permit and Delete an entry)

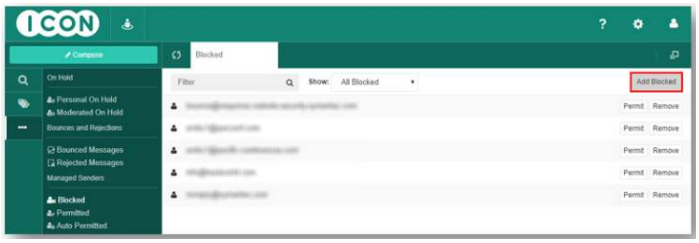
You can manage personal Blocked Senders, Permitted Senders and Auto Permitted Senders, as follows:

Add a Blocked Sender

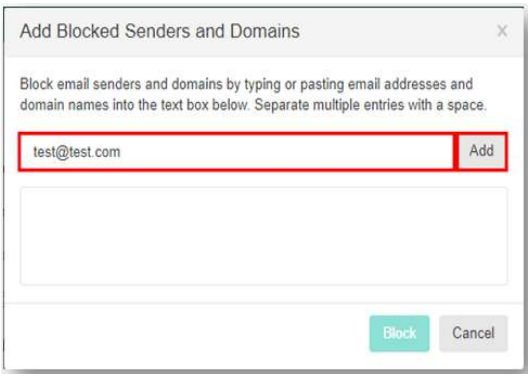
1. Select **Blocked** from the left-hand menu



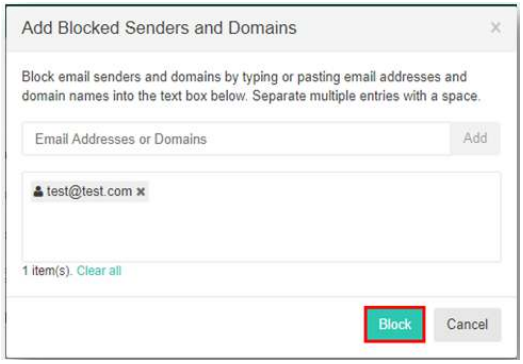
2. Click **Add Blocked**



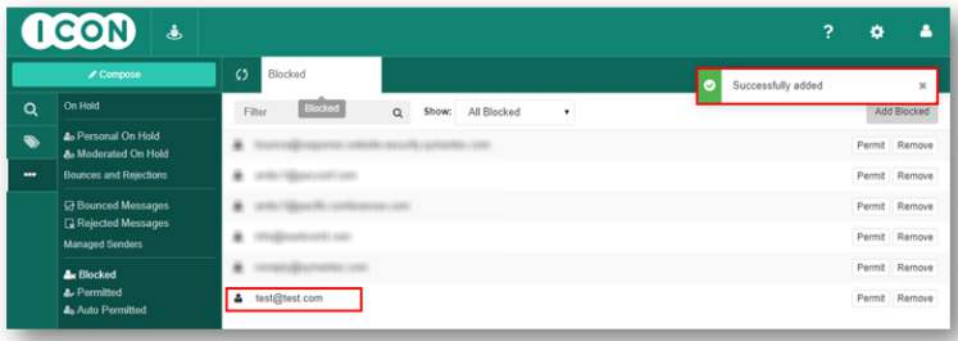
3. Enter single or multiple email addresses or domains in the box and click **Add.**



4. Click **Add Blocked**.



5. A notification will display confirming the sender has been successfully added to the list.

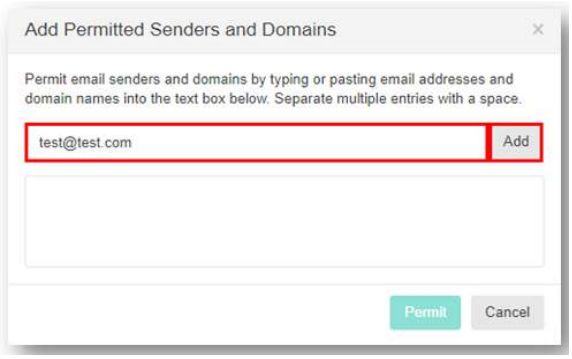


2. Add a Permitted Sender

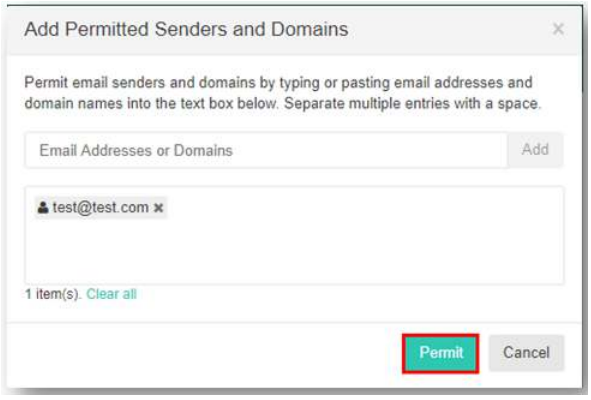
Mimecast provides a feature called auto allowed senders. This is an automatically configured when the user send a message to an external recipient, the recipient is then automatically considered a trusted sender. An auto allow entry is automatically deleted if no messages are sent to the address for 120 days.

1. Select **Permitted** from the left-hand menu and click **Add Permitted**.

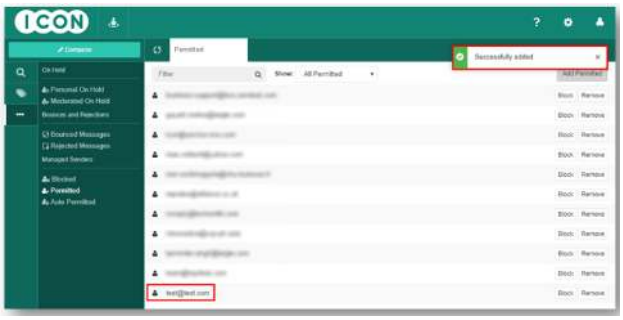
2. Enter single or multiple email addresses or domains in the box and click **Add.**



3. Click **Permit**



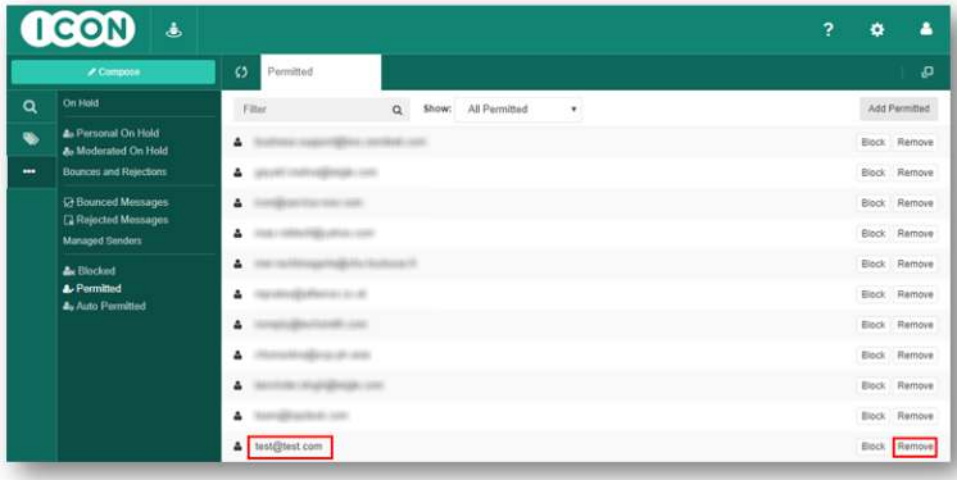
4. A notification will display confirming the sender has been successfully added to the list.



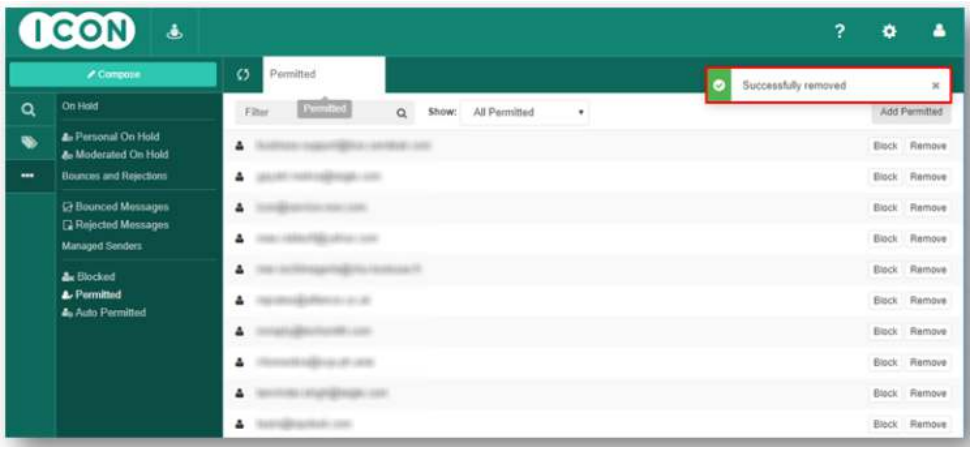
3. Delete an Entry

1. Select the required tab from the **Managed Senders** view (**Blocked, Permitted or Auto Permitted)**

2. Select **Remove** for the relevant entry in the list.



3. A notification will display confirming the sender has been successfully removed.

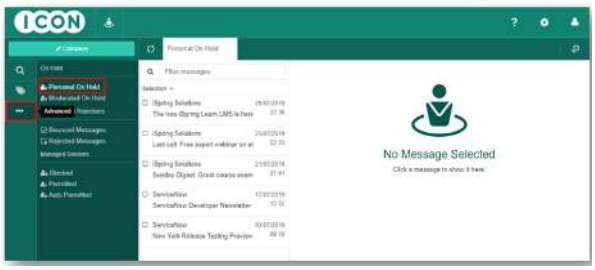


4. Managing *Personal on Hold* Messages

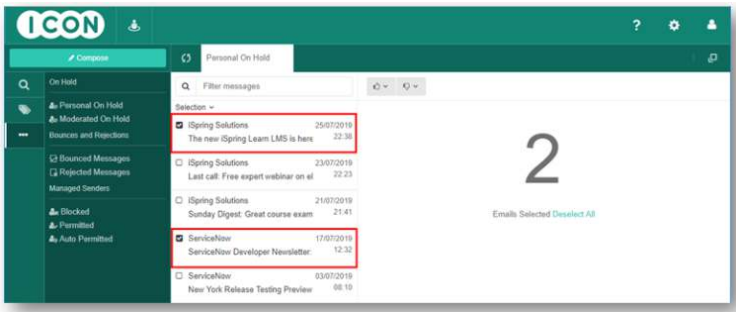
Emails can be released or rejected either individually or in bulk. Addresses or domains can also be blocked when emails are released or rejected.

5. How to Reject Messages

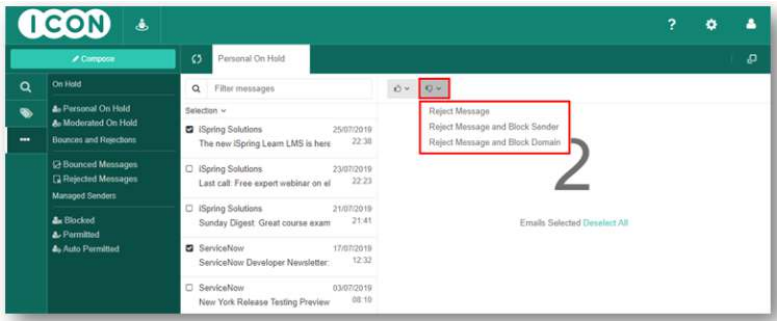
1. Click the **Advanced**  icon and select **Personal On Hold**.



2. Select single or multiple emails.



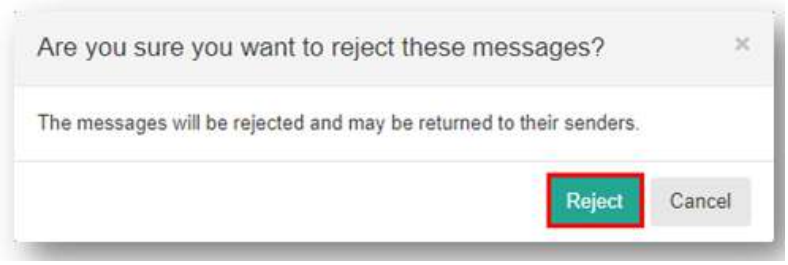
3. Select the  icon and select the appropriate action.



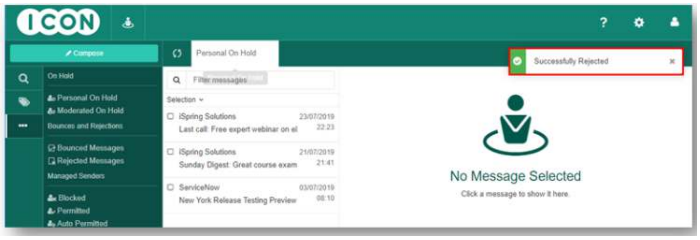
Descriptions for each action are shown below:

Menu option	Description
Reject Email	The email is removed from the viewer and a notification is sent to the sender. Future emails from this sender may be Held
Reject Email & Block Sender	The email is removed from the viewer, a notification is sent to the sender, and a Block Policy is created for their email address (e.g. sender@company.com). This means that the sender will be unable to send emails to you in future, but you are able to remove this policy using Managed Senders.
Reject Email & Block Domain	The email is removed from the viewer, a notification is sent to the sender, and a Block Policy is created for their domain name (e.g. company.com). This means that any senders from that domain will be unable to send emails to you in future, but you are able to remove this policy using Managed Senders.

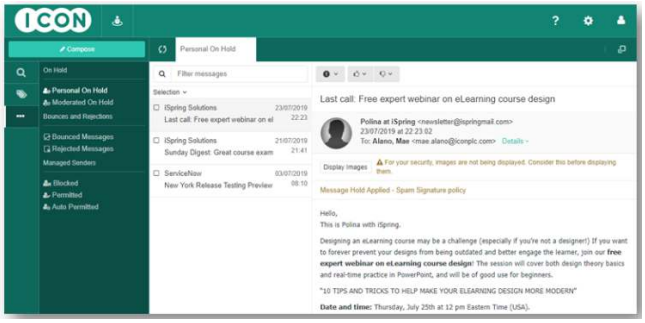
4. Depending of your desire selection a box will present as follow, e.g. **Reject**



5. A message will provide confirmation the entry has been rejected.

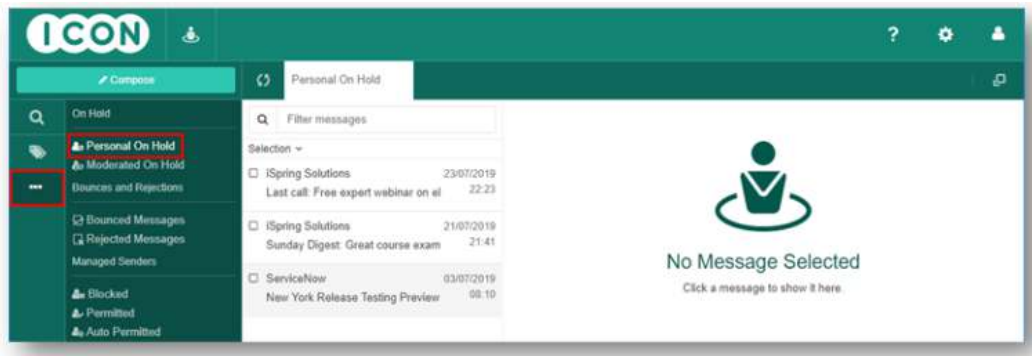


IMPORTANT: Once selected a message from **Personal On Hold**, in the right-hand side of the screen, the content of the message is shown. This can help to take the appropriate action e.g. rejecting it.

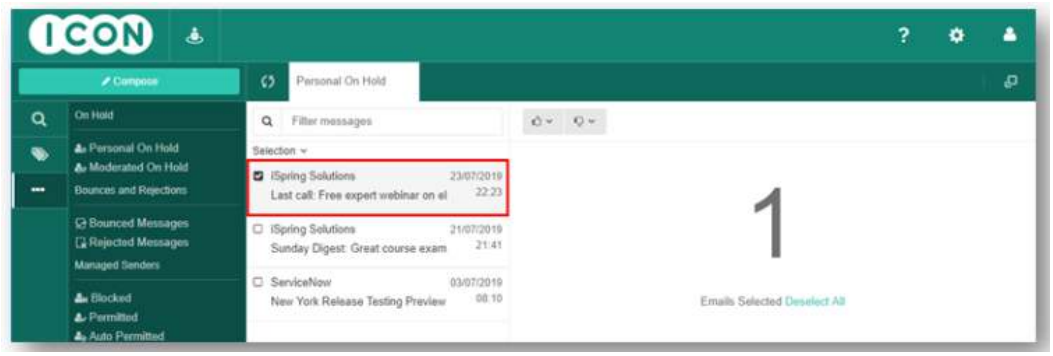


6. How to Release Messages

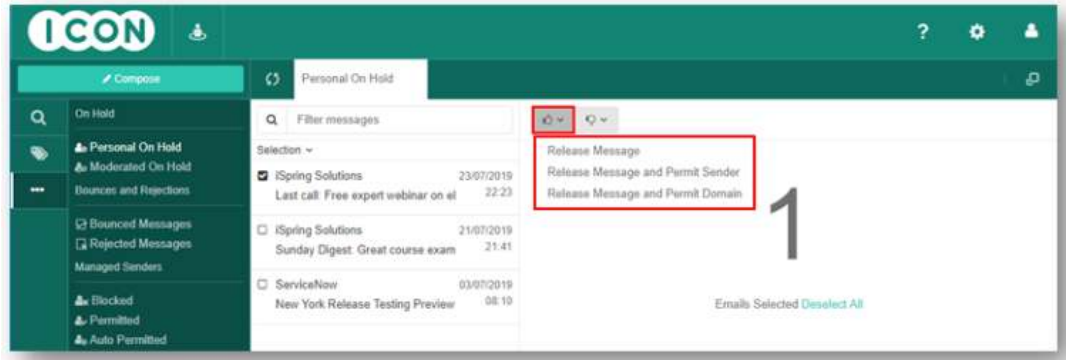
1. Click the **Advanced**  icon and select **Personal On Hold**.



2. Select single or multiple emails



3. Select the  icon and select the appropriate action.

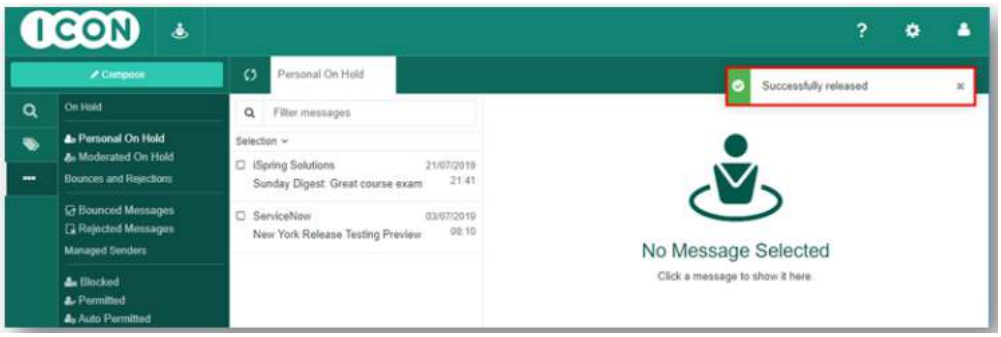


NOTE: Descriptions for each action are shown below:

Menu option	Description
Release Email	The email is removed from the viewer and is delivered to your Inbox. Future emails from the sender may be Held.
Release Email & Permit Address	The email is removed from the viewer, is delivered to your Inbox, and a Permit Policy is created for the email address of the sender(e.g. sender@company.com). A Permit Policy will bypass Spam checks on future emails from this sender, so that they are not Held by the Spam Policy. You are able to remove this policy using Managed Senders.
Release Email & Permit Domain	The email is removed from the viewer, is delivered to your Inbox, and a Permit Policy is created for the domain name of the sender (e.g. company.com). A Permit Policy will bypass Spam checks on future emails from senders of this domain so that they are not Held by the Spam Policy. You are able to remove this policy using Managed Senders.

4. Depending of your desire selection a box will present as follows, e.g. **Release and Permit Sender**

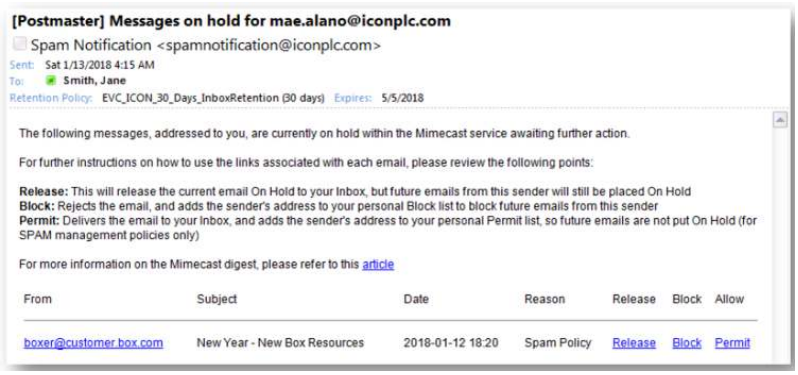
4. A message will provide confirmation the entry has been released.



7. How to Manage Incoming Email Held Back by the Mimecast Software (Digest Notification)

A Digest Notification is an email summary that will arrive in your inbox on several occasions during your working day. The Digest Notification allow you to view and control emails that have been placed on hold in the Mimecast Portal.

The Digest email will look similar to the screenshot below, and you will be given three choices on how you want to manage emails that are held in the Mimecast portal.



Digest Choices

The links in the Digest email allow you to ensure that emails are not missed and you can release them to your inbox. You can choose to RELEASE, BLOCK or PERMIT an email that is listed in the Digest notification. Explanations for each of these features is outlined in the table below.

Action	Email Delivery	Future Emails
Release	Releases the email from the Hold Queue, and immediately delivers the email to your Inbox	Emails from this sender may still be put On Hold in future
Block	Removes the email from the Hold Queue	Emails from this sender will be immediately Rejected to the Sender by Mimecast in future
Permit	Releases the email from the Hold Queue, and immediately delivers the email to your Inbox	Emails from this sender (if blocked for spam content) will not be put On Hold, and will immediately be delivered to your Inbox in future

Appendices

There following outlines the key changes Legacy PRA staff may notice following deployment of Mimecast Email Security:

Outbound Emails – Legal Disclaimer (Stationery)

All emails sent externally will have the ICON standard legal disclaimer appended, as follows:

ICON plc made the following annotations.

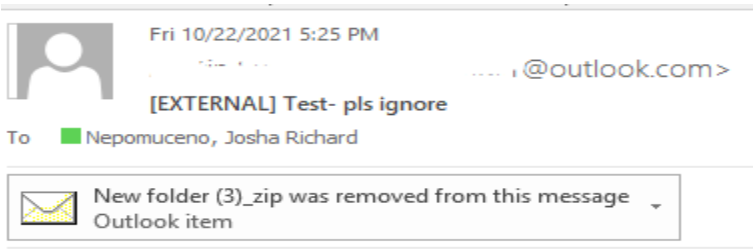
This e-mail transmission may contain confidential or legally privileged information that is intended only for the individual or entity named in the e-mail address. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or reliance upon the contents of this e-mail is strictly prohibited. If you have received this e-mail transmission in error, please reply to the sender, so that ICON plc can arrange for proper delivery, and then please delete the message.

Thank You,

ICON plc
South County Business Park
Leopardstown
Dublin 18
Ireland
Registered number: 145835

Inbound Email from an External Sender

All emails from external senders are appended with [EXTERNAL] on the message subject.



Sent from Mail for Windows

Following deployment of Mimecast, the existing external email notification (see below) will be removed.

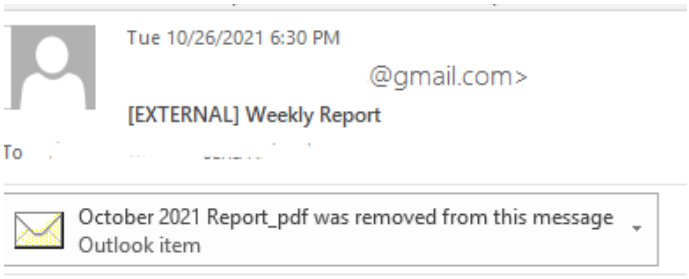
CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Inbound Email – Targeted Threat Protection: Attachments

Common attachments like Word, Excel, PowerPoint and PDFs are not always safe, and are regularly used by hackers to try and infect corporate computers with viruses and to steal valuable information.

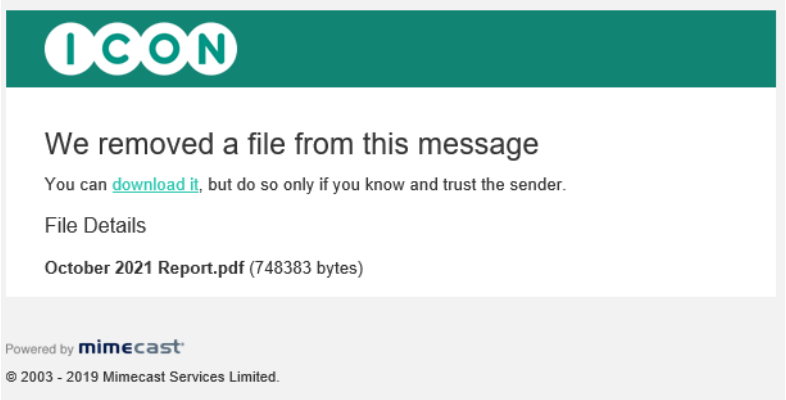
When a message comes in with an attachment:

1. It immediately goes into the Targeted Threat Protection - Attachment Protect sandbox for immediate scanning.
2. If the attachment is safe they are released to the recipient.
3. If the attachment is found to contain malicious code or is malicious, it is blocked. No user notification will be sent out.
4. If an attachment is found to be un-safe or encrypted the original email will be delivered, however the attachment will be linked and a notification will be attached in its place.



Hi,
See attached weekly report.

Regards
J



Note: Legacy PRA currently allows emails up to 35MB in total mail size regardless number of attachments. Individual email attachments greater than 25MB will now be replaced with a download link. The attachment link is accessible for 90 days.

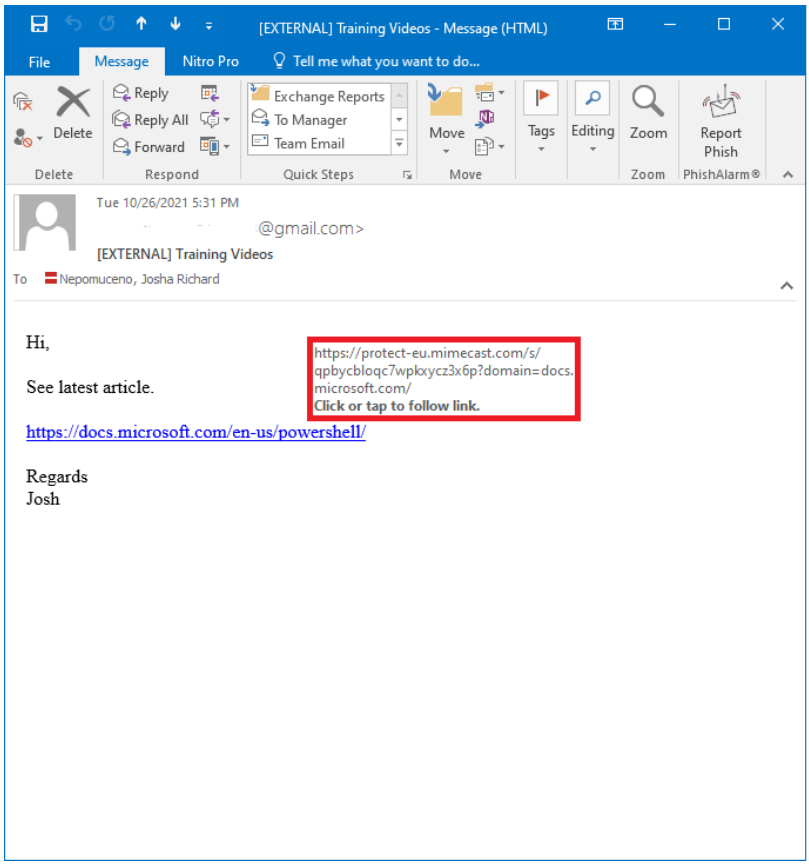
Inbound Email & Links to Websites (URLs)

We're so used to links in emails, we don't always think before clicking them.

Unfortunately, this can allow hackers to steal your login details which would give them access to our company's computers.

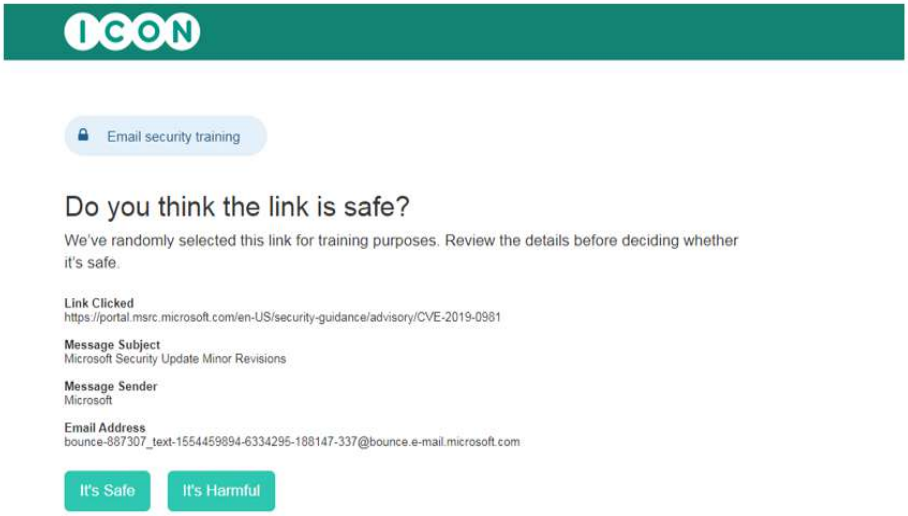
To help protect us, the following measures are in place:

- Every time you click a link in an email, Mimecast will check the site you are trying to access.
  - If the site is good, you will be allowed to continue as normal.
  - If the site is bad, access will be blocked.
- When you hover over a link in an email, you will see the address as: http://protect-eu.mimecast.com This means the Website Link has been scanned by Mimecast.



Clicking on Website Links in Email/Harmful and Safe Links

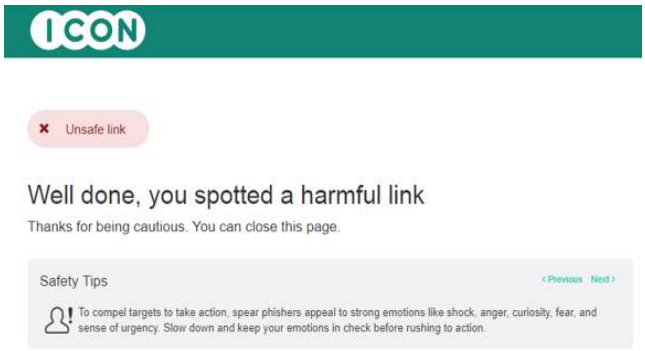
When you click on a Website (URL) link, you may be redirected to a page providing information about the destination of the link they have clicked, as shown in the picture below.



Harmful Website Links
If you click on '**It's Safe**"" and the link is harmful, no option to "Continue to Page" is shown.

If you click "**It's Harmful**" and the link is harmful, no option to "Continue to Page" is shown.

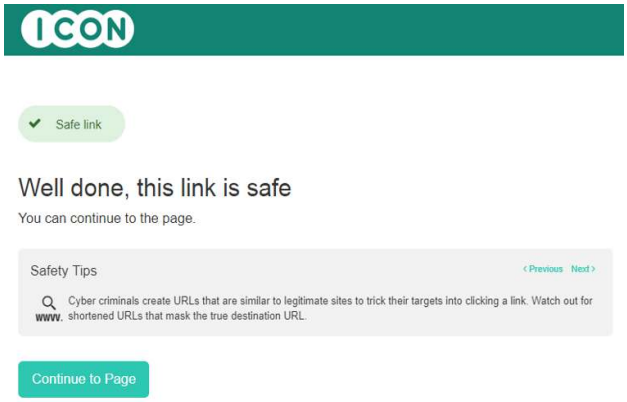
This means that you will not be able to access this Website Link – see picture below.



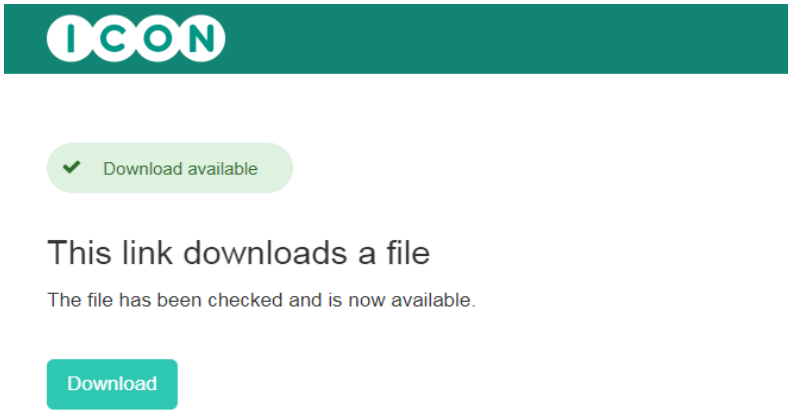
Safe Website Links
If you click "**It's Safe**" (and the link is safe) a "Continue to Page" is shown

If you click "**It's Harmful**", and the link is safe, a "Continue to Page" is shown.

This means that you will be able to access this Website Link – see picture below.



Downloading a Website File
When you click in an URL link that directly downloads a file, Mimecast will check the file, and if the file is safe, you can click "Download". If file is harmful you will not be able to download the file as it will be blocked by Mimecast.



If a valid URL or download attachment is blocked in error. Please log a ticket with the LPRA service desk.