Rollout of Outlook security changes

Background

We are currently carrying out a phased move of the University's Email Security Service to Exchange Online Protection (EOP) and Microsoft Defender for Office (MDO), and are getting in touch to let you know that these adjustments will soon be applied to your email account. These changes will deploy one of the key functional services and deliverables of project COM079: the **Email Quarantine Process**.

The project has already piloted these alterations successfully with an initial test group and then the whole of ISG. The project team are now extending the rollout of these new settings to all of SSPS and we are taking a number of steps to ensure that the user experience is as trouble-free as possible.

This document will give you more detail on how these modifications will process mail items that are suspected to be unsolicited and potentially dangerous; the steps you can take to have more control of these items, and where you can find additional information and communicate with colleagues who are supporting these changes.

Rollout Dates

The deployment of the changes in SSPS is planned to run for 3 weeks in the first instance. A review will be carried out at the end of this period when it is expected that we will keep the modifications in place, unless there are major difficulties reported.

Please note the dates and activities below.

- Rollout Start Date for SSPS: **Wednesday 19th February 2025.** (Members will be added to the pilot group)
- Rollout Review Date: **Wednesday 12th March 2025.**

Discussions and Feedback

This pilot will be utilizing Viva Engage for collaboration. All pilot members will be added to the Viva Engage community: **Quarantine Pilot Platform,** where communication, discussions and feedback will take place.

Viva Engage channel:
https://engage.cloud.microsoft/main/org/ed.ac.uk/groups/eyJfdHlwZSI6Ikdyb3VwIiwiaWQiOiIxOTkwMDUwMjgzNTIifQ

What will change: the new experience

Our current email security setup is configured to deliver all approved emails to a user Inbox and reject all other mails that fail security. Microsoft Defender on the other hand, utilises the **Junk mail folder** and the **Quarantine folder** to manage email security.

This means that users will now receive and can preview emails that have been categorized as unsolicited and spam, in their junk mail folders, as well as preview blocked emails in their quarantine folder.

To summarise:

- Emails that are detected as **spam and unsolicited** will be delivered into your junk mail folder. You should begin to check this regularly. Mail items in the Junk Email Folder are auto deleted after 30 days if you do nothing else with them.

- Emails, files, and Teams messages that are detected as **malicious** will be quarantined. You will not be notified that a mail has been quarantined, hence you should check your individual quarantine directory regularly, especially if you are expecting an email. Quarantined emails are auto deleted in 30 days if not attended to.

In addition, users may begin to get notifications/warning banners on top of their emails, like those advising about external senders, relating to the below:

- First contact safety tips
- User impersonation safety tips
- Domain impersonation safety tips
- Unusual characters safety tips
- Spam safety tips

An example of this would be a banner on the top of an incoming email that states:

You don't often get email from emailaddress@domain.com. Learn why this is important at https://aka.ms/LearnAboutSenderIdentification

Delivered Mails

Legitimate emails will be delivered to your inbox while unsolicited mails will be delivered into your junk mail. On rare occasions, a legitimate mail may be categorised as spam and you may find a mail you believe is spam in your inbox, these are called false positive (good mail marked as bad) or a false negative (bad email allowed). When the above occurs, you can report the message to Microsoft, which will help the system to learn better and avoid such in the future.

The Microsoft Report Message add-ins for Outlook and the built-in Report button in supported versions of Outlook make it easy for users to report false positives and false negatives to Microsoft for analysis. False positives are good email that was blocked or sent to the Junk Email folder. False negatives are unwanted email or phishing that was delivered

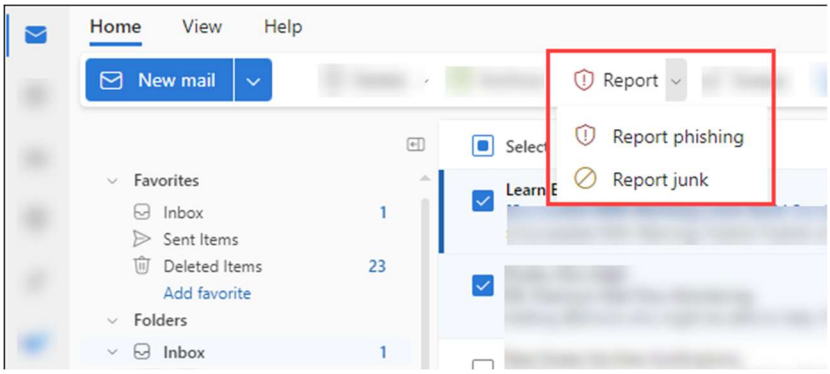
to the Inbox. Microsoft uses these user-reported messages to improve the effectiveness of email protection technologies.

Use the built-in Report button in Outlook to report junk and phishing messages

Users can report a message as junk from the Inbox or any email folder other than Junk Email folder.

Users can report a message as phishing from any email folder.

In a supported version of Outlook, select one or more messages, select Report, and then select Report phishing or Report junk in the dropdown list.

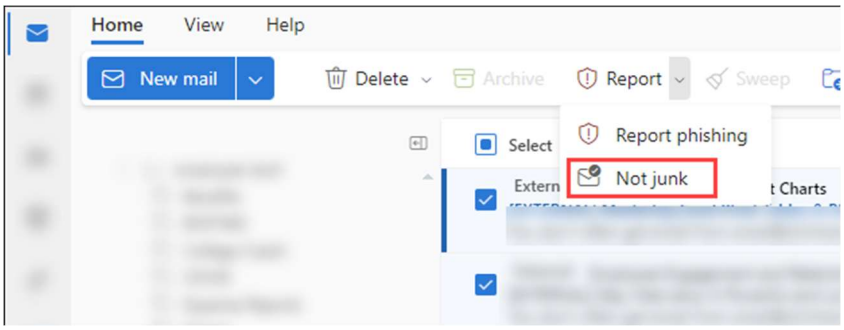


the messages are sent to Microsoft. The following actions are also taken on the reported messages in the mailbox:

- Reported as junk: The messages are moved to the Junk Email folder.
- Reported as phishing: The messages are deleted.

Use the built-in Report button in Outlook to report messages that are not junk

In a supported version of Outlook, select one or more messages in the Junk Email folder, select Report, and then select Not junk in the dropdown list.



the messages are sent to Microsoft. The messages are also moved out of Junk Email to the Inbox.

Use the Report Message add-in to report junk and phishing messages

Users can report a message as junk from the Inbox or any email folder other than the Junk Email folder.

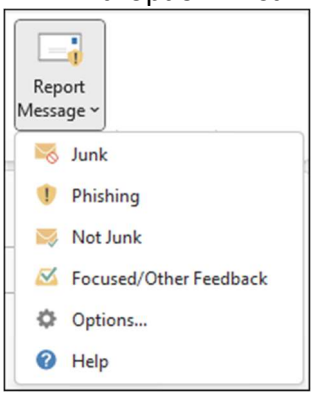
Users can report a message as phishing from any email folder.

In Outlook, do one of the following steps:

- Select an email message from the list.
- Open a message.

Do one of the following steps based on your Ribbon Layout configuration in Outlook:

- Classic Ribbon: Select Report Message, and then select Junk or Phishing in the dropdown list.



The messages are sent to Microsoft. The following actions are also taken on the reported messages in the mailbox:

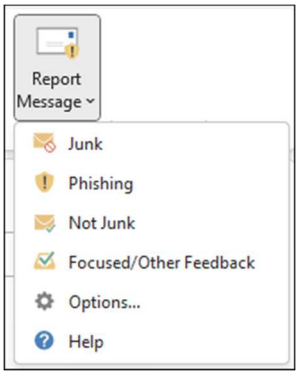
- Reported as junk: The messages are moved to the Junk Email folder.
- Reported as phishing: The messages are deleted.

Use the Report Message add-in to report messages that are not junk

In Outlook, open a message in the Junk Email folder.

Do one of the following steps based on your Ribbon Layout configuration in Outlook:

- Classic Ribbon: Select Report Message, and then select Not Junk in the dropdown list.



The messages are sent to Microsoft. The messages are also moved out of Junk Email to the Inbox.

For more information on reporting messages, visit: [Use the Report Message add-in - Microsoft Support]

Quarantined Emails

Quarantined emails will not be delivered to your account, unless released by an administrator. Our administrators will not release any mail items that are obviously malicious items. You can view items in the Quarantine folder and carry out the actions listed below on emails in the Quarantined folder, users can:

- Delete message
- Preview message
- Block Sender
- Allow Sender
- Request message to be released by Admin.

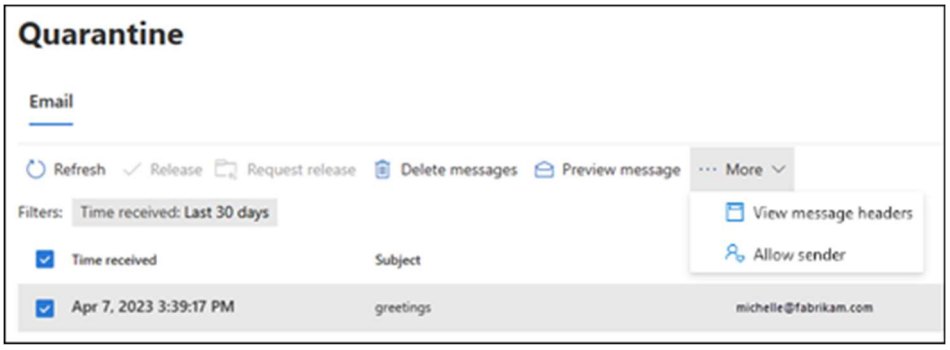
To view your emails that have been quarantined, you should click: https://security.microsoft.com/quarantine?viewid=Email.

The steps below provide more detail if you wish to act on quarantined emails.

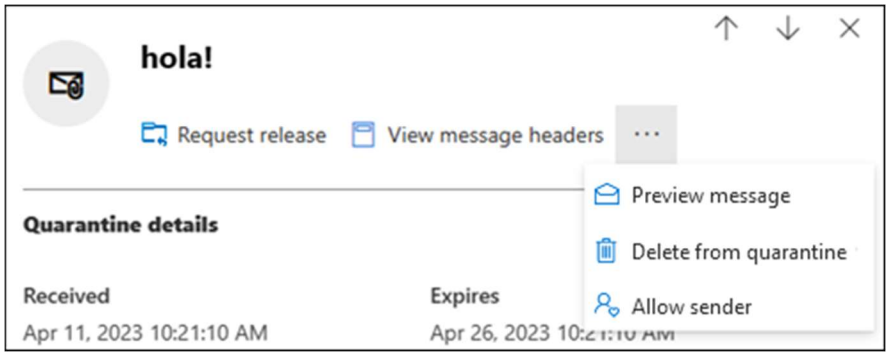
Act on quarantined email

On the **Email** tab, select the quarantined email message by using either of the following methods:

- Select the message from the list by selecting the check box next to the first column. The available actions are no longer greyed out.



- Select the message from the list by clicking anywhere in the row other than the check box. The available actions are in the details flyout that opens.



- Using either method to select the message, some actions are available under ··· **More** or **More options**.

After you select the quarantined message, the available actions you can take are described below.

➢ **Request the release of quarantined email**

After you select the message, use either of the following methods to request its release:

- **On the Email tab**: Select **Request release**.
- **In the details flyout of the selected message**: Select ··· **More options** > **Request release**.

In the **Request release** flyout that opens, review the information, select **Request release**. In the **Release requested** flyout that opens, select **Done**.

➢ **Delete email from quarantine**

After you select the message, use either of the following methods to remove it:

- **On the Email tab**: Select **Delete messages**.
- **In the details flyout of the selected message**: Select ··· **More options** > **Delete from quarantine**.

In the **Delete (n) messages from quarantine** flyout that opens, use one of the following methods to delete the message:

- Select **Permanently delete the message from quarantine** and then select **Delete**: The message is permanently deleted and is not recoverable.
- Select **Delete** only: The message is deleted but is potentially recoverable.

➢ **Preview email from quarantine**

After you select the message, use either of the following methods to preview it:

- **On the Email tab**: Select **Preview message**.
- **In the details flyout of the selected message**: Select **More options** > **Preview message**.

In the flyout that opens, choose one of the following tabs:

- **Source**: Shows the HTML version of the message body with all links disabled.
- **Plain text**: Shows the message body in plain text.

➢ **Allow email senders from quarantine**

Tip: If the sender is already in your **Junk email filter lists**, **allow sender** is not available.

The **Allow sender** action adds the message sender to the Safe Senders list in your mailbox.

After you select the message, use either of the following methods to add the message sender to the Safe Senders list in your mailbox:

- **On the Email tab**: Select **More** > **Allow sender**.
- **In the details flyout of the selected message**: Select **More options** > **Allow sender**.

The flyout that opens indicates when the sender was successfully added to your Safe Senders list. Select **Done**.

➢ **Block email senders from quarantine**

Tip: If the sender is already in your **Safe Senders list**, **Block sender** is not available. **Remove sender from user block list** is available instead.

The **Block sender** action adds the message sender to the Blocked Senders list in your mailbox.

After you select the message, use either of the following methods to add the message sender to the Blocked Senders list in your mailbox:

- **On the Email tab**: Select **More** > **Block sender**.

- **In the details flyout of the selected message**: Select ··· **More options** > **Block sender**.

In the **Block sender** flyout that opens, review the information about the sender, and then select **Block**.

If the sender is already in your **Safe Senders list**, Block sender is not available. **Remove sender from user block list** is available instead.

➢ Add Trusted names to the Safe Senders List

Email addresses and domain names in the Safe Senders List are never treated as junk email, regardless of the content of the message. You can add your Contacts and other correspondents to the Safe Senders list to confirm you will always receive their messages in your inbox.

To add a person to the Safe Senders List, (in Classic Outlook), click a message from the sender. On the Home tab, in the Delete group, click Junk, and then click Never Block Sender.

To add a specific address or domain to the Safe Recipients List, click a message from the sender. On the Home tab, in the Delete group, click Junk, and then click Never Block the Group or Mailing List.

To manually add names or domains to these lists, do the following:

1. On the Home tab, in the Delete group, click Junk, and then click Junk E-mail Options.
2. Do one of the following:
    - To add safe senders, on the Safe Senders tab, click Add.
    - To add safe recipients, on the Safe Recipients tab, click Add.



3. In the Enter an e-mail address or Internet domain name to be added to the list box, enter the name or address that you want to add. For example, you can add:
    - a specific email address, such as someone@example.com

- an Internet domain, such as @example.com, or example.com.

4. Click OK and repeat for each entry that you want to add.

    - If you want all Contacts to be considered safe senders, select the Also trust e-mail from my Contacts check box in the Safe Senders tab.

To learn more about Safe Senders list, check: Block or unblock senders in Outlook - Microsoft Support

Details of the general quarantine process can be found on the Microsoft website. https://learn.microsoft.com/en-us/defender-office-365/quarantine-end-user?view=o365-worldwide