Microsoft Defender Quarantine

What's Happening?

In our ongoing commitment to safeguarding our digital communication, we are making improvements to the university's Microsoft Defender service.

The university employs Microsoft Defender to evaluate emails for potential threats. It analyses incoming and outgoing messages, assigning a confidence score to each based on the likelihood of being spam or malicious. Depending on this score, Microsoft Defender automatically directs emails to the Microsoft Defender Quarantine area, the user's Junk folder, or safely to the Inbox.

From now on, emails that Microsoft Defender suspects to be malicious or spam will be directed to Microsoft Defender Quarantine rather than the previously used Junk folder. This change aims to enhance the security and management of potentially harmful emails.

Other mailbox-specific settings, such as the Blocked Sender List, may still put emails in the Junk folder.

This does not mean that you need to be less cautious about any unexpected email that you receive. If you are at all concerned about an email in a university mailbox, please use the Report Phishing function in Outlook to report it. More details on how to report suspicious emails or Teams messages is on the University portal:

- Reporting suspicious emails: https://students.solent.ac.uk/support-documents/studying/technology/report-phishing-how-to-guide.pdf
- Reporting suspicious Microsoft Teams messages: https://students.solent.ac.uk/news/teams-cyberthreats

Why Quarantine Instead of Junk?

The Junk folder does not show why an email is in Junk, so it is not possible to know if Microsoft Defender assessed it as possibly spam or phishing. The Quarantine portal shows what method of assessment has led Microsoft Defender to quarantine an email, such as Spam, Phish, High Confidence Phish, or Malware.

Depending on Microsoft Defender's confidence level as to how likely an email is to be phishing or spam, you will have an option to release a quarantined email or request release for a quarantined email.

How Do I Access the Quarantine Portal?

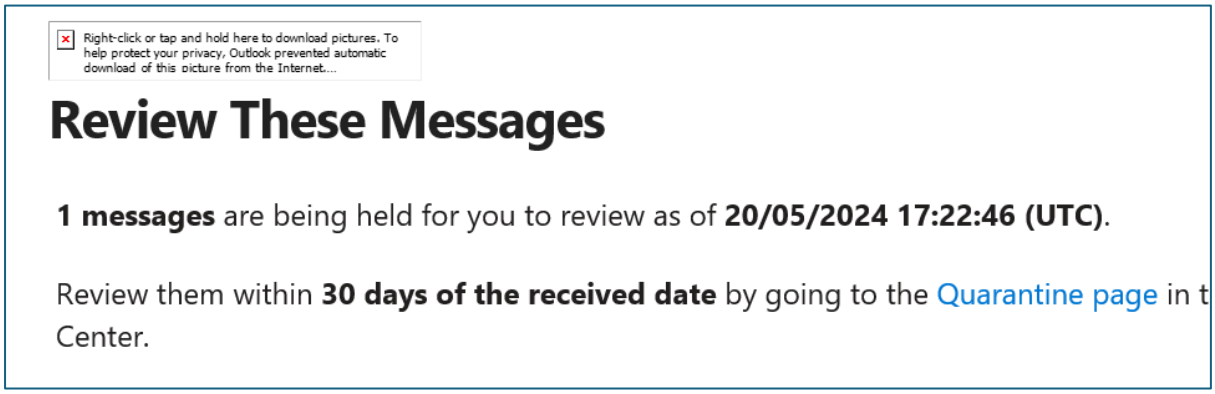
You can check if Microsoft Defender has quarantined any email messages intended for delivery to you, or to a shared mailbox you have full access to, by using your university account to access the Quarantine portal: https://security.microsoft.com/quarantine

Please note that accessing the Quarantine portal will require you to complete multi-factor-authentication.

Alternatively, you should normally receive an automated notification email of any email message(s) quarantined in the past 4 hours. This automated email will have the following properties:

- From: quarantine@messaging.microsoft.com
- Subject: Microsoft 365 security: You have messages in quarantine

This automated email will provide summary information about the quarantined email message(s) with options to review or release, similar to the following image:



You can use the “Quarantine page” or “Review Message” links within the notification email to access the Quarantine portal.

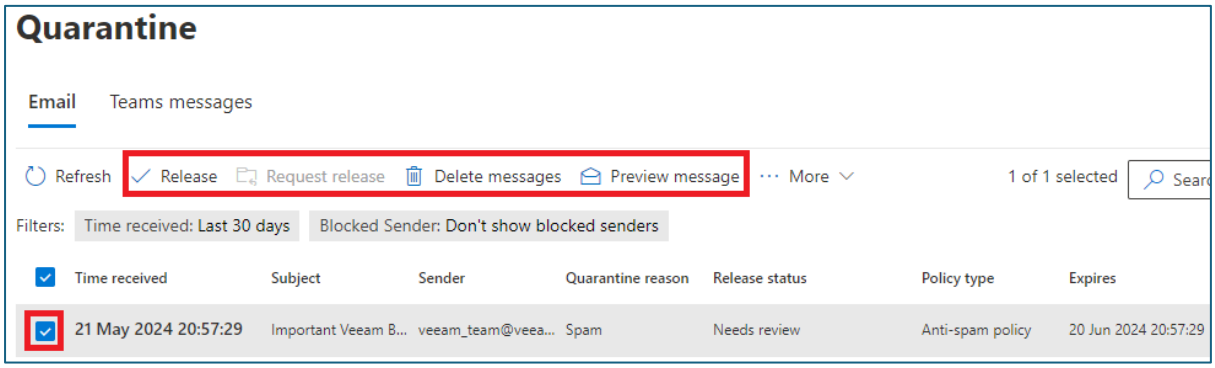
Please remember that Microsoft Defender has quarantined emails for a reason so always be cautious about releasing any quarantined email. We strongly recommend that you use the preview message option within the Quarantine portal, to safely review the content of the email, before deciding whether to release it or not.

How Do I Release Emails from Quarantine?

If you are unsure about any email showing in quarantine then is it strongly advised that you preview it, using the “Preview message” option, before deciding to either release it or delete it.

If you are still unsure about any email after previewing its content, then do not release it.

Select the email message you want to preview by selecting the box in the first column of the row displaying the quarantined email details, as highlighted in the bottom-left of the following image:



Once you have selected an email then you will have options in the menu bar (highlighted in the image above) to either Release (tick icon) or Request release (folder with arrow icon), followed by options to Delete Messages (trashcan icon), or Preview Message (envelope icon). To preview, select the Envelope (Preview message) icon and a flyout window will appear allowing you to safely preview the message.

If you believe that the email is legitimate and want to release it, you will have the option to either:

- release the email yourself by selecting the Release (tick icon), or
- request release of the email by selecting the Request release (folder with arrow icon).

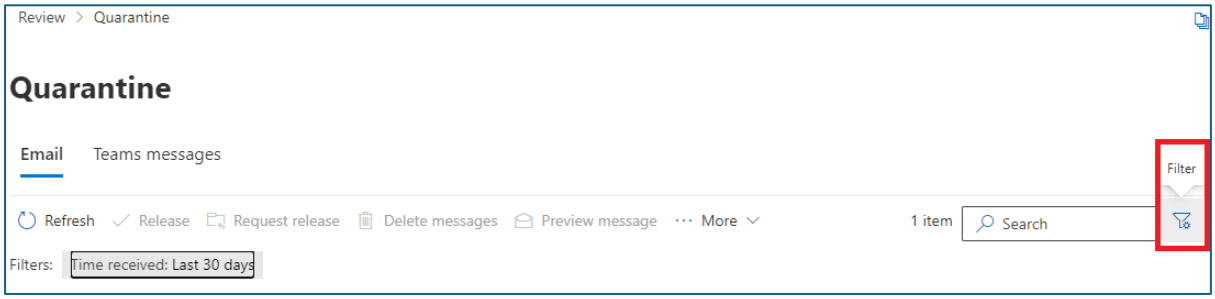
The Request release option sends a request to the university’s Information Security team, who will perform a manual assessment as to whether the email is malicious or not. If the Information Security team assess the email as safe then they will release the email from quarantine.

Emails released from quarantine should appear in your Inbox shortly afterwards.

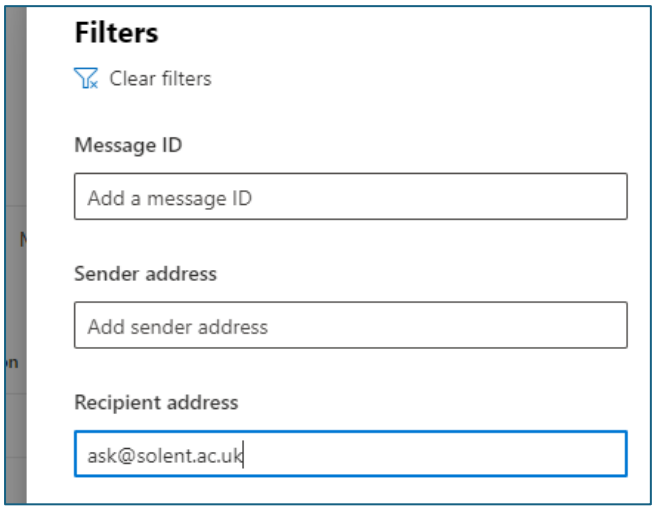
Shared Mailboxes

By default, the Quarantine portal only shows a list of quarantined emails intended for delivery to your university mailbox. If you want to see quarantined emails intended for delivery to a shared mailbox then you need to use the Filter option and filter the results by Recipient address using the full email address of that shared mailbox.

Here is an image of the Quarantine portal showing the Filter option highlighted in the menu bar, after the Search box option:



When you have selected the Filter option then a window will appear with various filtering options – "Recipient address" is the third filtering option from the top of the list. Here is an image of the Filters window, showing the "Recipient address" filtering option completed with the full email address of the shared mailbox "ask@solent.ac.uk":



Once you have entered all the filtering options that you want to use, you must select the "Apply" option at the bottom of the Filters window to make those filter settings active. Active filter options will be visible just below the Quarantine portal menu bar.

If you receive the error message "security. You are not authorized to perform this operation" then you do not have the required permissions to view quarantined emails for that mailbox. Reviewing quarantine for a mailbox requires your account to have "Full Access" and "Send As" or "Send on Behalf" permissions to that mailbox.

Any shared mailbox emails released from quarantine should appear in that shared mailbox Inbox shortly afterwards.