SPAM EMAIL FILTERING IS CHANGING. HERE’S WHAT YOU NEED TO KNOW.

ISD HAVE IMPLEMENTED A NEW SYSTEM FOR CATCHING AND MANAGING MALICIOUS OR UNWANTED EMAILS.

THE NEW SYSTEM IS CALLED EXCHANGE ONLINE PROTECTION (EOP). THIS REPLACES CANIT.

READ ON TO SEE HOW EOP CAN IMPROVE YOUR SPAM FILTERING AND ALLOW YOU TO SEE JUST THE EMAILS THAT MATTER.
WHAT IS SPAM?
Due to its size and status the university receives 1000’s of emails each day. Whilst the vast majority of these messages are legitimate some are known as ‘spam’. A spam message is often one that you do not wish to see or that poses a security risk.

The type of unwanted or spam email can be varied. Often an email you receive could be the result of your email address being on a mailing list or if you have made a purchase or enquiry via a particular website. These can take the form of newsletters or advertising emails. Whilst these sorts of message are not malicious they can be annoying if they are too frequent or not relevant to you or your work.

The other type of unwanted/spam emails you may receive are more serious. Some messages may try to fool you into thinking they are from someone you know or that they contain a common document (e.g. ‘invoice’). These malicious emails try to use this sense of familiarity to get you to click on malicious links. These links could contain a virus or link to a location that attempts to gather further information from you. These are known as phishing emails.

Using EOP the University can improve its proficiency at catching these irrelevant, unsolicited or malicious messages before they ever reach your inbox.
DAILY DIGESTS

To help you manage your spam messages you will receive a ‘daily digest’ from EOP. The senders address will be quarantine@messaging.microsoft.com. This message is delivered between 1.00am and 3.00am providing you have received some spam in the last 24 hours which EOP has held in quarantine.

Emails held in quarantine are kept for 15 days following their delivery. However, your digest will only show you the spam messages received in the last 24 hours. For more information about the quarantine procedures turn to page 7.

When you receive a Daily Digest email from EOP it will look like this. Please note how the message is shown in both the Outlook desktop application and Outlook Web App (Webmail). Other applications/mobile apps will present the message in a similar format.

![Daily Digest Email Example](https://example.com/daily_digest_email.png)
Outlook Web App (Webmail)

**KEEP A MESSAGE**

Click on the ‘Release to Inbox’ link next to a message and it will be moved to your inbox within a few seconds of the request. Repeat this process for each message you wish to keep. If you find a sender is regularly marked as spam you can specify them as a ‘safe sender’. For instructions on how to do this please turn to page 16.

**REPORT AN ERROR**

If you find a message has been quarantined when it shouldn’t have been you can make a report to Microsoft. Doing so will help Microsoft build up a better picture of what messages are legitimate and what should remain as spam. Click the ‘Report as Not Junk’ link to send this information. Please note that this does not release the message to your inbox, it only sends the report.

**SEE ALL YOUR SPAM MESSAGES**

The Daily Digest message only shows spam messages delivered in the last 24 hours. To see all messages currently held in quarantine click the [office365.uea.ac.uk/spam](http://office365.uea.ac.uk/spam) link at the bottom of the email. Further details about the spam/quarantine portal is available on the next page.
SPAM QUARANTINE

Whenever an email is thought to be spam by EOP it will be delivered to a holding area known as quarantine. This area sits outside of your inbox meaning potentially dangerous or annoying emails do not fill up your inbox. This also maintains the safety of you and your IT account. Access the quarantine area by going to office365.uea.ac.uk/spam. Login using your UEA credentials with your username in the format abc15xyz@uea.ac.uk.

<table>
<thead>
<tr>
<th>SENDER</th>
<th>SUBJECT</th>
<th>RECEIVED</th>
<th>EXPIRES</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:itcs.staff@uea.ac.uk">itcs.staff@uea.ac.uk</a></td>
<td>(Spam?) Play with me?</td>
<td>28/10/2015 14:04</td>
<td>12/11/2015 01:00</td>
</tr>
<tr>
<td><a href="mailto:itcs.staff@uea.ac.uk">itcs.staff@uea.ac.uk</a></td>
<td>(Spam?) Play with me?</td>
<td>28/10/2015 14:04</td>
<td>12/11/2015 01:00</td>
</tr>
<tr>
<td><a href="mailto:communications@beyondtrust.com">communications@beyondtrust.com</a></td>
<td>(Today) Join Security MVP. Paula Januszkiewicz in &quot;...&quot;</td>
<td>28/10/2015 15:57</td>
<td>12/11/2015 01:00</td>
</tr>
<tr>
<td><a href="mailto:bfm@lmsual.uea.ac.uk">bfm@lmsual.uea.ac.uk</a></td>
<td>Hi sweetie!</td>
<td>20/10/2015 13:09</td>
<td>12/11/2015 01:00</td>
</tr>
<tr>
<td><a href="mailto:message@inbound.efax.com">message@inbound.efax.com</a></td>
<td>eFax message from &quot;Booking.com - HylaFa&quot; - 1 pa...</td>
<td>28/10/2015 12:14</td>
<td>12/11/2015 01:00</td>
</tr>
<tr>
<td><a href="mailto:email@worldpay-news.com">email@worldpay-news.com</a></td>
<td>Accept customer payments securely in 2015</td>
<td>28/10/2015 11:33</td>
<td>12/11/2015 01:00</td>
</tr>
<tr>
<td><a href="mailto:thebookstore@bax.com">thebookstore@bax.com</a></td>
<td>BMEA Webinar - Best of BoxWorks with Box VP of P...</td>
<td>28/10/2015 11:20</td>
<td>12/11/2015 01:00</td>
</tr>
<tr>
<td><a href="mailto:message@inbound.efax.com">message@inbound.efax.com</a></td>
<td>eFax message from &quot;Booking.com - HylaFa&quot; - 1 pa...</td>
<td>28/10/2015 11:09</td>
<td>12/11/2015 01:00</td>
</tr>
<tr>
<td><a href="mailto:freeads-bounces@uea.ac.uk">freeads-bounces@uea.ac.uk</a></td>
<td>(FreeAds@UEA) (Spam?) For Sale: Tommee Tippee ...</td>
<td>28/10/2015 10:25</td>
<td>12/11/2015 01:00</td>
</tr>
<tr>
<td></td>
<td>Hi!</td>
<td>28/10/2015 09:56</td>
<td>12/11/2015 01:00</td>
</tr>
<tr>
<td><a href="mailto:itcs.staff@uea.ac.uk">itcs.staff@uea.ac.uk</a></td>
<td>(Spam?) Hello!</td>
<td>28/10/2015 09:52</td>
<td>12/11/2015 01:00</td>
</tr>
<tr>
<td><a href="mailto:itcs.staff@uea.ac.uk">itcs.staff@uea.ac.uk</a></td>
<td>(Spam?) Hello!</td>
<td>28/10/2015 09:52</td>
<td>12/11/2015 01:00</td>
</tr>
<tr>
<td><a href="mailto:bfm@lmsual.uea.ac.uk">bfm@lmsual.uea.ac.uk</a></td>
<td>Hi dear!</td>
<td>28/10/2015 09:17</td>
<td>11/11/2015 01:00</td>
</tr>
<tr>
<td><a href="mailto:julie.arias@stormwind.com">julie.arias@stormwind.com</a></td>
<td>The 8 Windows 10 Shortcuts You Didn't Know You ...</td>
<td>27/10/2015 19:46</td>
<td>11/11/2015 01:00</td>
</tr>
<tr>
<td><a href="mailto:itcs.staff@uea.ac.uk">itcs.staff@uea.ac.uk</a></td>
<td>(Spam?) Hello!</td>
<td>27/10/2015 18:36</td>
<td>11/11/2015 01:00</td>
</tr>
<tr>
<td><a href="mailto:itcs.staff@uea.ac.uk">itcs.staff@uea.ac.uk</a></td>
<td>(Spam?) Hello!</td>
<td>27/10/2015 18:38</td>
<td>11/11/2015 01:00</td>
</tr>
<tr>
<td><a href="mailto:bfm@lmsual.uea.ac.uk">bfm@lmsual.uea.ac.uk</a></td>
<td>Hello!</td>
<td>27/10/2015 16:22</td>
<td>11/11/2015 01:00</td>
</tr>
</tbody>
</table>

Quarantine

This page will display all messages that have been quarantined within the last 15 days. Messages older than 15 days will be automatically removed. Be sure to check this page regularly if you have not processed your messages via the Daily Digest email.
QUARANTINE OPTIONS

Clicking the pencil icon will reveal more details about the message currently highlighted in the list.

This button will release the selected message to your inbox in the same way that you can release a message from your Daily Digest email.

Use this button to perform an advanced search within your quarantined messages. Read on for more details regarding the searching functions.

Performs a real-time refresh of the quarantine list. If any new messages have been delivered since you logged in they will appear following a refresh.

By default, spam-quarantined messages are sorted from newest to oldest on the ‘received’ field. ‘Sender,’ ‘Subject’ and ‘Expires’ values are also listed for each message. You can sort on any of these fields by clicking their headers. Clicking a column header a second time will reverse the sort order. A maximum of 500 messages can be displayed in spam quarantine.

You can view a list of all your quarantined messages, or you can search for specific messages by specifying filter criteria (filtering can also help you reduce your result set if you have more than 500 messages). After searching for and locating a specific quarantined message, you can view details about the message. You can also release the message and report it as not junk to the Microsoft Spam Analysis Team.

ADVANCED SEARCH

You can filter your own quarantined items based on several different conditions using advanced search. You can use these conditions separately or in combination with one another. The search will provide a list of messages that meet all your filter criteria. Click the ‘Advanced Search’ icon to open the Advanced Search window.
Select any combination of the following conditions. Select the associated check box in order to enable each condition. Wildcards aren’t supported.

a. **Sender email address.** Specify the email address of the person who sent the message.
b. **Subject.** Specify the subject line text of the message.
c. **Received.** You can select that the message was received by the quarantine within the past 24 hours (**Today**), within the past 48 hours (**Last 2 days**), within the past week (**Last 7 days**), or you can select a custom time interval during which the message was received by the quarantine.
d. **Expires.** You can select that the message will be deleted from the quarantine within the next 24 hours (**Today**), within the next 48 hours (**Next 2 days**), within the next week (**Next 7 days**), or you can select a custom time interval during which the message will be deleted from the quarantine.

Click ‘OK’ to start running the advanced search.
VIEW DETAILS ON SPECIFIC QUARANTINED MESSAGES

In the spam quarantine, select a specific message and a summary of the properties of that message appear in the details pane on the right side of the screen.

**message status**

- **Type**: Spam
- **Expires**: 12/11/2015 01:00
- **Released to**: [Redacted]
- **Not yet released to**: [Redacted]

**message details**

- **Message ID**: <0.0.13F.151.1D1116f26AFBF12.0@mailer1.e-locationemail.com>
- **Sender**: email@worldpay-news.com
- **Subject**: Accept customer payments securely in 2015
- **Received**: 28/10/2015 11:55
- **Size**: 27 KB

**View message header...**

**Preview email message...**

**MESSAGE STATUS**

**Type**: This is always Spam.

**Expires**: The date when the message will be deleted from the quarantine.

**MESSAGE DETAILS**

**Sender**: The email address of the person who sent the message.

**Subject**: The subject line text of the message.

**Received**: The date on which the message was received by the quarantine.

**Size**: The size of the message, in kilobytes (KB), or, if the message size is greater than 999 KBs, in megabytes (MB).

**View message header**: Click this link to open the message header dialog box, which lets you view the message header text. You can also copy the message header text to your clipboard and paste it into the Message Header Analyzer. Access this at testconnectivity.microsoft.com. Once in the Message Header Analyzer tool, click ‘Analyze Headers’ in order to retrieve information about the header.
RELEASING MESSAGES

1. Select the message you wish to release to your inbox. Select multiple messages using ‘Ctrl’ or ‘Shift’ keys.
2. Click the ‘Release Message’ icon. Two options will appear.

![Release Options]

3. Click ‘Release selected message(s).’ to release the email directly to your inbox. Click ‘Release message(s) and report as not junk’ to release the message to your inbox and report it as not junk to the Microsoft Spam Analysis Team.
4. You may receive a warning message when you click either of these links. Click ‘Yes’ to proceed if you wish to release the message(s).

![Warning Message]

5. You will receive a message confirming the action.

![Release Confirmation]

6. Click the ‘Refresh’ icon to see the messages new status in the ‘Details Pane’.
MIGRATING YOUR SETTINGS FROM CANIT

The university’s old method for dealing with spam was via a system called CanIt. If you have previously been a user of CanIt, or think you may have previously setup some preferences, you may need to migrate some of your settings to EOP. Follow these instructions to check your setup and make the changes if required.

1. Go to canit.uea.ac.uk
2. Login using your UEA username and password. Ensure you type your username in the following format: abc15xy.z.uea.ac.uk

3a. If your Spam-Scanning Level is set to ‘SPAM emails have {Spam?} added to subject line’ it is likely you have no specific rules setup for your emails. If you wish to check for old rules please select ‘Enable Expert Interface’.

3b. If when you login you see the screen shown above it is likely that you have some email rules defined in CanIt. Please proceed to the next step.

4. When ‘Expert Interface’ is enabled you will be given more options within CanIt. Click on the ‘Rules’ tab to view ‘Senders’ rules and ‘Custom Rules’.
5. Click ‘Senders’ to access the senders rules. This will show rules for specific senders and how you have chosen to act on their emails.
6. If you have email addresses identified as safe senders with the ‘Always Allow’ option selected these senders need to be moved to EOP. If you have email addresses that you have chosen to block using the ‘Always Reject’ option these also need to be moved to EOP to maintain the block. Instructions for how to add safe and blocked senders into EOP are on page 16. Take a note of these addresses and the rules for later. Go to page 16 to see how you can import these settings into EOP.

7. Click ‘Custom Rules’ to see rules that have been created to block specific domains.

8. Make a note of any custom rules you have created for migration to EOP.
SETTING BLOCKED & SAFE SENDERS IN OUTLOOK

You can set specific email addresses to be ‘safe’ or ‘blocked’ senders in Outlook. Once an email address is listed in one of these groups EOP will know whether to deliver the message directly to your inbox or stop it before it even reaches the quarantine area.

These settings can be made in either the desktop Outlook application or via the Outlook Web App (Webmail).

OUTLOOK (DESKTOP)

1. Open Outlook on your desktop.

2. Click ‘Junk’ in the top menu bar under the ‘Home’ tab. Select ‘Junk E-Mail Options’ from the drop down list.
3. Click ‘Safe Senders’ or ‘Blocked Senders’ to see your current rules.

4. Click ‘Add’ to create a new rule. If you have noted down any previous setting from CanIt please input them here. These settings will be mirrored online at office365.uea.ac.uk/outlook.
OUTLOOK (WEBMAIL)

1. Go to office365.uea.ac.uk/outlook
2. Login using your UEA username and password. Ensure you type your username in the following format: abc15xyz.uea.ac.uk
3. Click the ‘gear’ settings icon in the upper right corner and select ‘Options’.

4. Select ‘Block or allow’ from the ‘Mail’ and ‘Account’ Menu on the left side of the screen. Expand the menu’s using the arrows.
5. Use the + button to add email addresses to your safe and blocked sender lists. If you wish to delete an entry highlight it using a left click and select the ‘Trash’ icon. Use the ‘Pencil’ icon to edit a highlighted entry. If you have noted down any previous setting from CanIt please input them here.

6. Click ‘Save’ at the top of the screen when you have finished creating your rules.

**REPORT/MARK AS JUNK**

When using the Outlook Web App you can right click any message in your inbox and select ‘Mark as junk’. You will be given the options to ‘Report’ or ‘Don’t report’. Reporting the message will inform the Microsoft Spam Analysis Team and then move the message to your Junk E-Mail folder. If you choose not to report the message it will simply be moved to your Junk E-Mail folder.