Email Protection FAQs
# Table of Contents

Email Protection FAQs ........................................................................................................................................... 3  
General Information ............................................................................................................................................... 3  
  Which University email domains are configured to use Email Protection for Anti-Spam? .................. 3  
  What are Spam Quarantine Notification emails? ......................................................................................... 3  
  How do I use the digest email message? ........................................................................................................ 4  
  How do I get an email that is not spam out of my quarantine? ............................................................... 4  
  What does the error: “Message No Longer Available” mean? ................................................................. 5  
  How long do the messages stay in my quarantine? ..................................................................................... 5  
  How can I delete messages in my quarantine? ......................................................................................... 5  
  What if I am still receiving spam email to my inbox? ........................................................................... 5  
  What is Advanced Threat Protection (ATP)? ......................................................................................... 5  
Using the Web Interface .................................................................................................................................... 7  
  How do I manage my quarantine? .............................................................................................................. 7  
  How do I use the web interface? ............................................................................................................. 7  
  How do I add/remove addresses to my Safe Senders List and Blocked Senders List? .................... 8  
  What can I do to consolidate my Safe Senders List and/or Blocked Senders List? .......................... 8
Email Protection FAQs

General Information

Which University email domains are configured to use Email Protection for Anti-Spam?
- aeeas.physics.miami.edu
- arc.miami.edu
- as.miami.edu
- eng.miami.edu
- exchange.ir.miami.edu
- g.law.miami.edu
- law.miami.edu
- listserv.cgcent.miami.edu
- mail.as.miami.edu
- medlistserv.med.miami.edu
- miami.edu
- physics.miami.edu
- phyvax.physics.miami.edu
- rsmas.miami.edu
- students.law.miami.edu
- umail.law.miami.edu
- umiami.edu

What are Spam Quarantine Notification emails?
If you opted-in, you will receive a daily message listing all the spam email that has been quarantined. Normally, you would look at the listing to see if any email were incorrectly identified as a spam. If you find an email that was quarantined but is not spam, just click on the Release to Inbox link for that email and it will be delivered to your mailbox.
How do I use the digest email message?
The digest email message is sent daily (per opt-in status) and contains information about suspected spam email quarantined since your last digest. The digest email message includes the sender, the subject line, and the date for each spam email.

Normally, no action will need to be taken on the spam emails listed in the digest. However, if you find an email in the Digest that you suspect is not spam, you can release the item to your mailbox.

How do I get an email that is not spam out of my quarantine?
There are two ways of managing your quarantine, through the digest email message and through the web interface.

If you are using the digest email message, you can click on Release to Inbox for the appropriate email. Release to Inbox will deliver the email to your mailbox.

If you are logged into the web interface, you can view email in your quarantine in the Messages list. Select the checkbox for the desired message and click Release Message at the top of the message list.
What does the error: “Message No Longer Available” mean?
Any email that is trapped in your quarantine will remain there for 14 days. After the 14 days, email will automatically be removed from the system. You should regularly check your quarantine either through your digest email message or by logging into the web interface, to ensure that all email stored in your quarantine is actually spam.

How long do the messages stay in my quarantine?
Any email that is trapped in your quarantine will remain there for 14 days. After the 14 days, email will automatically be removed from the system. You should regularly check your quarantine, either through your digest email message or by logging into the web interface, to ensure that all email stored in your quarantine is actually spam.

How can I delete messages in my quarantine?
Each message in your quarantine will automatically be deleted after 14 days. If you wish to clean out all the messages in your quarantine, prior to the 14 days, you can click on Options and select Delete All.

What if I am still receiving spam email to my inbox?
No anti-spam system is 100% accurate. Spammers are constantly coming up with new and improved methods of sending spam and vendors of anti-spam software are constantly updating their software to detect the latest spamming trends. It is possible for spam messages to make it past the University's spam filtering system and into your mailbox. If you find this is the case and you occasionally have more than a reasonable amount of spam making its way to your mailbox, you can add the offending address to your Blocked Senders List (see Block a mail sender and Filter junk email and spam in Outlook on the web). For additional assistance, please contact the IT Support Center at 305-284-6565, option 3.

What is Advanced Threat Protection (ATP)?
Advanced Threat Protection is a protection service, which replaces all the URLs (web addresses/links) in an email with ATP URLs (e.g. https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2F...).

These ATP web addresses are routed through email protection services to determine if the destination website is a safe site. If the destination website proves to be a safe site, the user is allowed to access the destination.
In the event a user tries to visit a site flagged as malicious, they will receive the following webpage.

Below is a more technical explanation of ATP:

Dynamically analyze and block, in real-time, malicious URLs and attachments that evade traditional antivirus and reputation filters delivering banking Trojans, ransomware, and other malware.

Detect sophisticated malware attacks, including:
- Polymorphic and zero-day malware
- Malicious attachments
- Other advanced exploits

In order to detect such advanced malware effectively—whether malware spread via spear-phishing emails containing a malicious attachment, watering hole URLs over email, or longline phishing campaigns — our malware analysis system technology uses a combination of sophisticated techniques to evaluate advance threats, including:
- Real-time checks against emerging campaigns and new malicious websites that are being detected across organizations.
- Static code analysis that looks for suspicious behavior, obfuscated scripts, malicious code snippets, and redirects to other malicious sites.
- Dynamic malware analysis that sandboxes the destination URL or suspicious attachments to simulate a real user on a machine, with the goal of observing any changes made to the system.

Our anti-evasion technology, in the dynamic analysis, tricks malware into revealing itself by creating virtual environments that accurately reproduce real system and real user behavior and interactions. This process provides comprehensive detection analysis that determines whether the destination URL or an attachment under suspicion is malicious, even finding malware that is sophisticated enough to conceal itself from detection leveraging techniques, e.g., IP rotation, mouse movement simulation, real browser sessions, time-delayed analysis.
### Using the Web Interface

**How do I manage my quarantine?**
Your quarantine can be accessed in two ways; using the digest email message or logging into the web interface [here](#).

**How do I use the web interface?**
Through the web interface, you can manage your spam quarantined messages. To access the web interface, open a web browser and go [here](#). You will need to log in using your CaneID and password. The web interface shows all suspected spam messages with sender’s address, subject line, date, size, and the spam score of the email.

<table>
<thead>
<tr>
<th>Sender</th>
<th>Subject</th>
<th>Date</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:o365mc@email2.microsoft.com">o365mc@email2.microsoft.com</a></td>
<td>Weekly digest: Office 3...</td>
<td>8/21/2017 5:26 AM</td>
<td>9/4/2017 8:00 PM</td>
</tr>
</tbody>
</table>

The following options are available in the Spam quarantine web interface:

- **Pencil**: View Message Details
- **Release Message**: Release message to Inbox
- **Advanced Search**: Filter out messages based on a set of criteria.
- **Refresh**: Refresh the list of Quarantined messages.
How do I add/remove addresses to my Safe Senders List and Blocked Senders List?
Please review Block a mail sender and Filter junk email and spam in Outlook on the web.

What can I do to consolidate my Safe Senders List and/or Blocked Senders List?
You can include entire domains in your Safe Senders List and Blocked Senders List. For example, you can add "@company.com" in your Safe Senders List. This would allow ALL incoming email coming from an address ending in exactly @company.com to be delivered to your mailbox without any spam checking. Alternatively, you could add "spammer.com" in your Blocked Senders List. This would prevent ALL email from getting to your mailbox that came from an address ending in exactly "spammer.com" (this would include addresses such as spam@us.spammer.com and spam@fr.spammer.com).

It is not recommended that you include entire domains unless you are sure that all incoming email are either safe or spam. This includes adding @miami.edu in your Safe Senders List and/or Blocked Senders List, since some spammers attempt to send out email messages with invalid @miami.edu addresses.