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 if I am still receiving spam email to my inbox? ......................................................................................................................... 3  
  What is Advanced Threat Protection (ATP)? ................................................................................................................................. 3

**Managing Quarantined Emails** .......................................................................................................................................................... 5
  How do I manage my quarantine? ......................................................................................................................................................... 5
  How long do the messages stay in my quarantine? ............................................................................................................................ 5
  How do I receive notifications that an email has been quarantined? .............................................................................................. 5
  How do I use the Quarantine Notification email? ............................................................................................................................ 5
  How do I get an email that is not spam out of my quarantine? ......................................................................................................... 5
  How do I use the web interface? ......................................................................................................................................................... 6
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 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%2...).

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 advanced 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.
Managing Quarantined Emails

**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 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 do I receive notifications that an email has been quarantined?**
You can sign up 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, and the size of the email.

**How do I use the Quarantine Notification email?**
If you opted-in, you will receive a daily message listing all the spam email that has been quarantined. Review the message for any emails that were incorrectly identified as a spam. 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?**
If you find an email that was quarantined but is not spam, click on the Release to Inbox link for that email and it will be delivered to your mailbox. Click Report as Not Junk to release the message to your Inbox and report the message as a false positive to Microsoft.

---

(User interface image of a spam notification email from Office 365, showing options to reply, mark as spam, view in web interface, and report as not junk.)

© 2017 Microsoft Corporation. All rights reserved. | Acceptable Use Policy | Privacy Notice
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.

![Spam quarantine web interface](image)

The following options are available in the Spam quarantine web interface:
- **Spam**: View messages based on classification – Spam, Bulk, and Phish
- **Search**: Filter out messages based on a set of criteria.
- **Refresh**: Refresh the list of Quarantined messages.
- **Release**: Release message to Inbox.
- **Release & Report**: Release message to Inbox and report the message as a false positive to Microsoft.

How do I release a quarantined message?
Select the message(s) you wish to release and click Release to release the quarantined message(s) to your Inbox. Click Release & Report to release the message to your Inbox and report the message as a false positive to Microsoft. The released message will have the current time and date stamp.

How do I see more details about the quarantined message?
Double click on a message to see a summary of the message properties in a pane on the right side of the page. You will see the following information:
- Message ID
- Sender Address
- Received
- Subject
- Type (Spam, Bulk, or Phish)
- Expires
- Released To
- Not yet Released To

You can also get even more details about the message by choosing Preview message. Any links inside the email will be disabled.
How do I search or filter my quarantined messages?
If you have a lot of quarantined items, you can reduce the number to a manageable amount by filtering them with search.

1. On the Quarantine page, choose Search.
2. Choose any combination of conditions by selecting the check boxes next to them (you can't use wildcards at this time). There are several conditions you can choose, including the following:
   - Message ID
   - Sender email address
   - Recipient email address
   - Subject
   - Received
   - Expires
   - Type
3. Choose Search to start the search. To see all the messages in quarantine again, choose Clear search.