Managing Your Personal Portal

Mimecast is PVAMU's first line of defense against unwanted email solicitations and malicious phishing attempts.

When Mimecast detects an email that may be a solicitation or malicious intent email, you will receive an email from **PV Mimecast Email Digest <emaildigest@pvamu.edu>** in your inbox notifying you that "**You have new held messages**."

These emails can be reviewed and acted upon by "**Individual PVAMU Email**" or via your "**Personal Portal**."

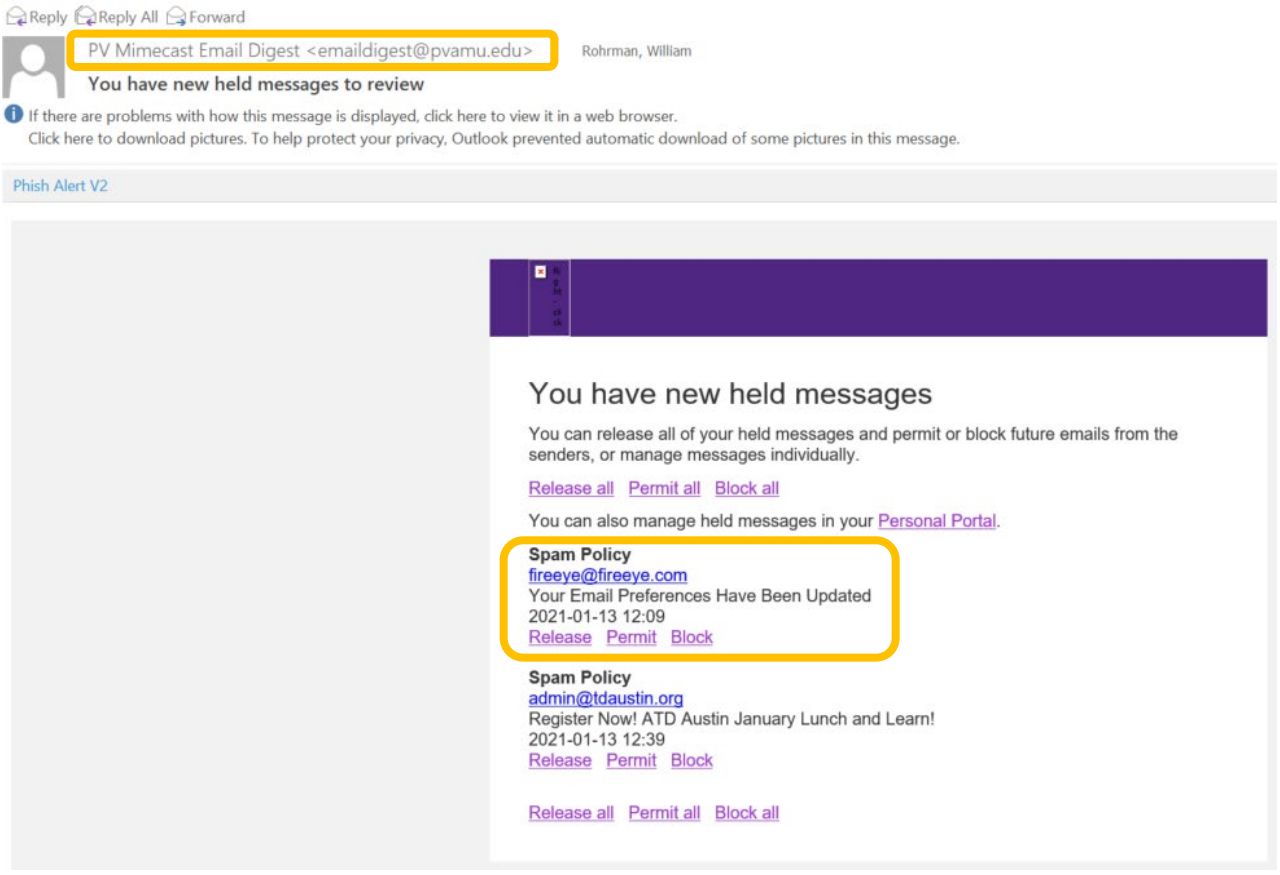
"Individual PVAMU Email" action will allow you to view and take action directly from the email received.

To take action by "**Individual PVAMU Email**," review the cited email and use the following options to determine the desired action for the email:

- **Release**: This will release the current email On Hold to your inbox, but future emails from this sender will still be placed On Hold.

- **Permit**: Delivers the email and adds the sender's address to your personal Permit list, so future emails are not put On Hold.

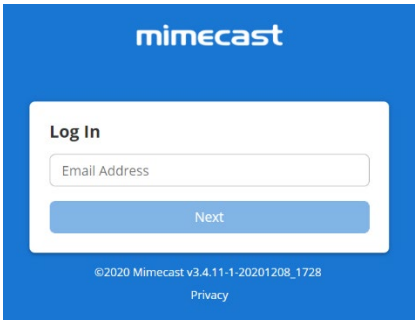
- **Block**: This will reject the email and adds the sender's address to your personal Block list to block future emails from this sender.



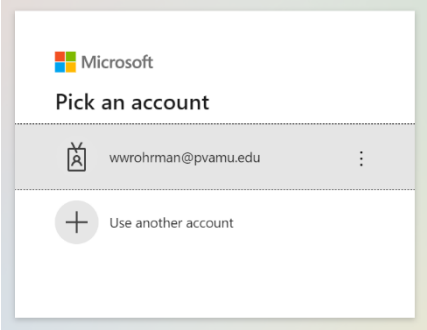
Your "Personal Portal" allows you to login directly to the mimecast dashboard to manually release your emails, as well as manage your individual blocked and permitted lists.

To utilize this method, click on the "**Personal Portal**" icon within the email received:

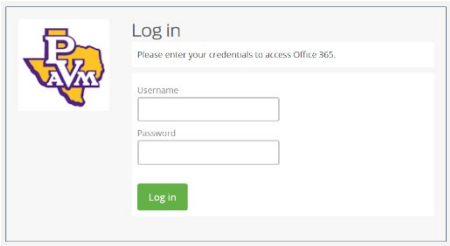
Login to mimecast using your **PVAMU email address** and click on "**Next**":

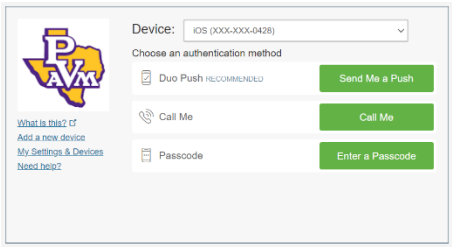


Select your account and you will be redirected to input your PVAMU credentials…

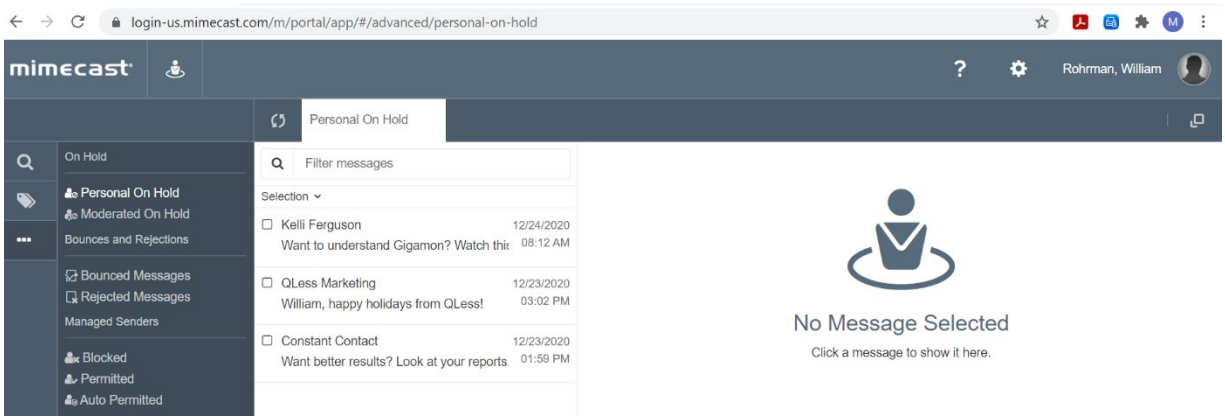


Input your **PVAMU credentials**, click "**log in**" and select your desired **mode of authentication** for Duo:



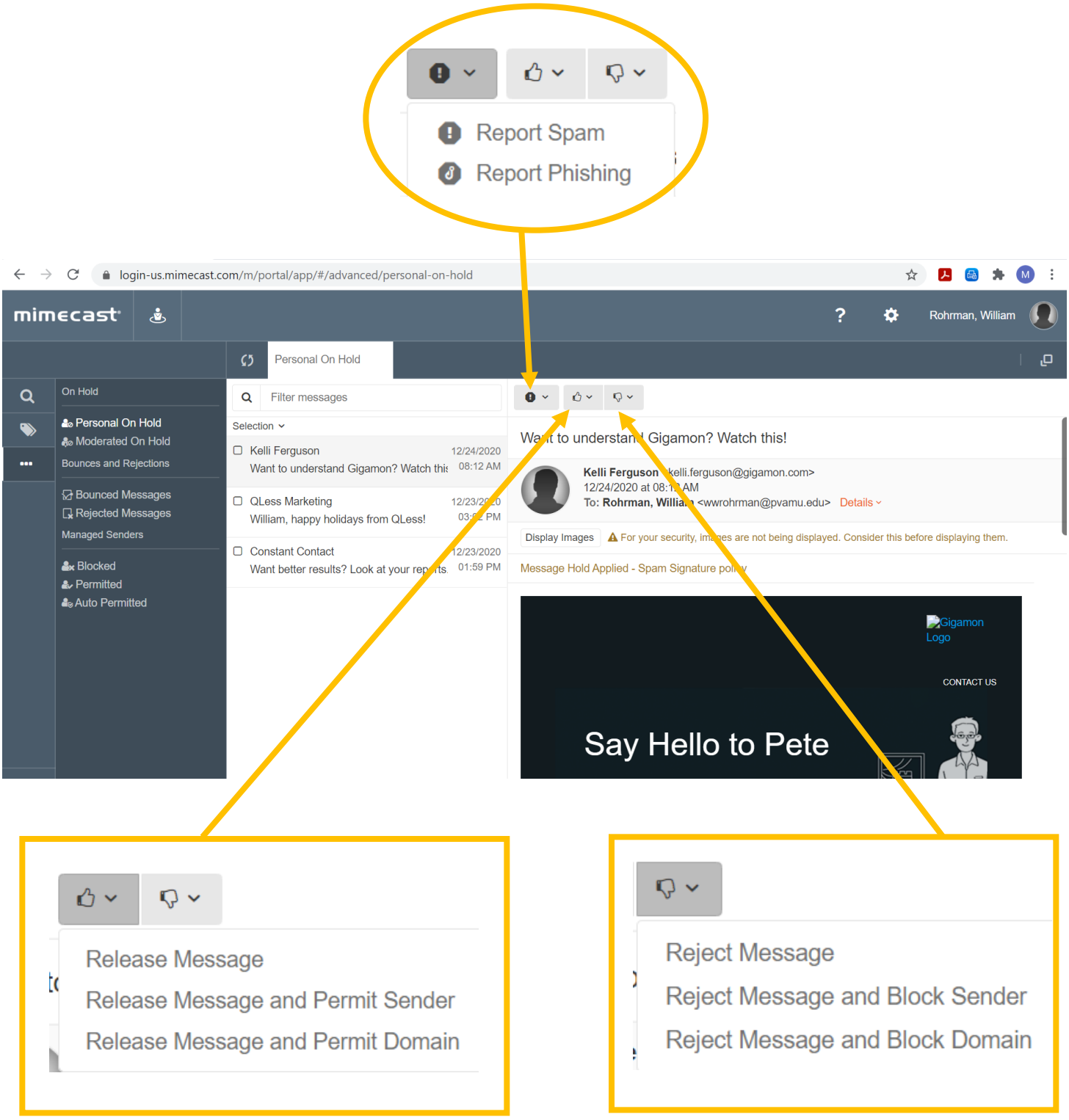


You will then be redirected to the **mimecast dashboard**:

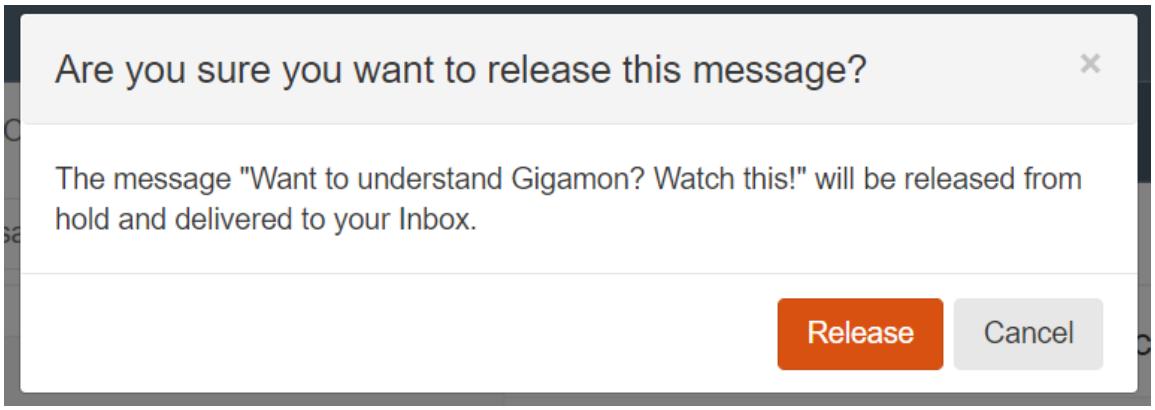


All emails detected by mimecast will be displayed on your dashboard.

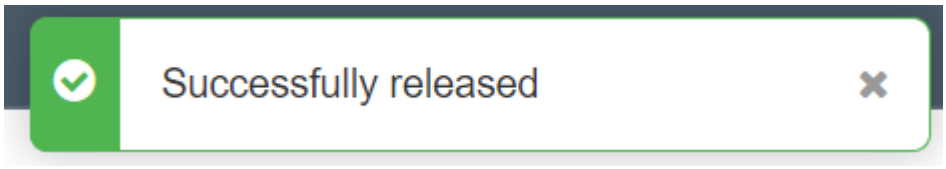
Review the cited email and use the following icons to determine the desired action for the email:



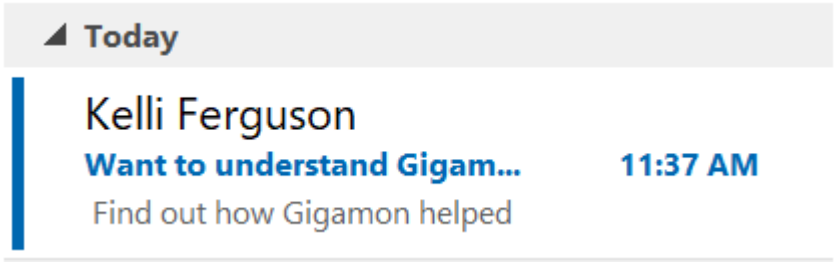
Once an action is selected, you will be prompted with an action message. For example, if you select the "**Release Message**" option, you will receive the following action confirmation message:



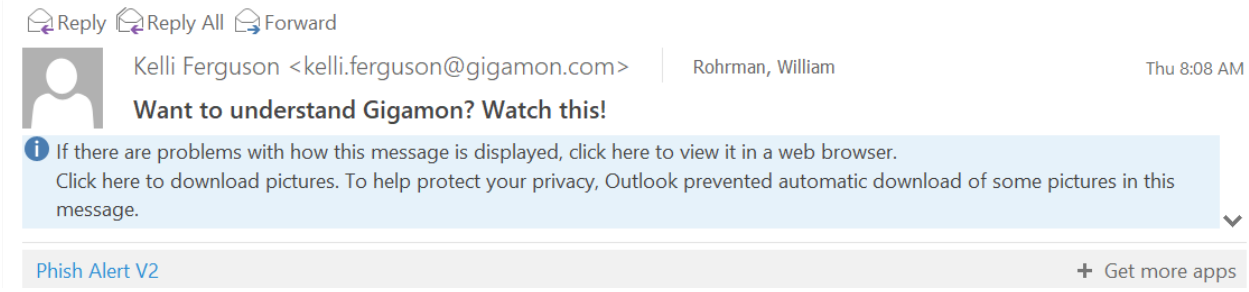
Verify the action by clicking on "**Release**" and the below confirmation message will be received:



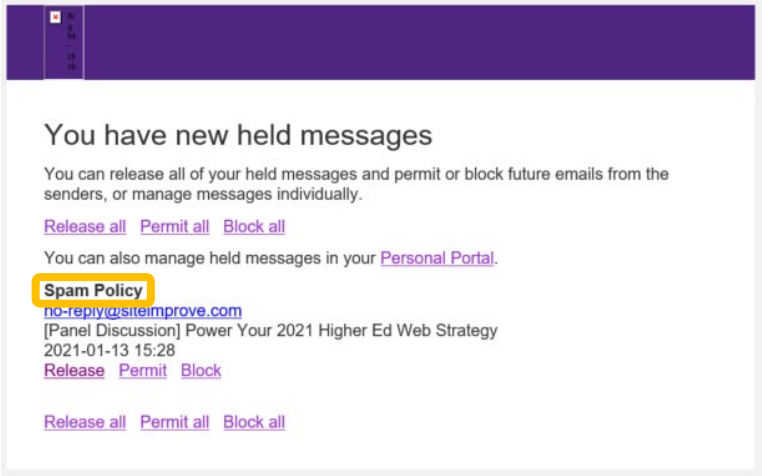
The email will then be released and delivered to your inbox (this may take a few minutes):



From your inbox, click on the email and take any appropriate action, if any:



As PVAMU's first line of defense against unwanted email solicitations and malicious phishing attempts, Mimecast will monitor all email traffic to ensure they fall within policy parameters. Emails not meeting the predefined policy parameters will trigger an alert and Mimecast will hold these emails for your review.



The below listed Policy statements provide an overview of PVAMU's policy parameters:

- **Spam Filter Policy** – This email has been flagged as Spam. This can be due to the email from a bulk email address or that have an unsubscribe or other button.
- **Zip File Attachment** – PVAMU does not allow Zip files.
- **Anti-Spoof Policy** – Users are sending email from a site that is imitating the PVAMU domain. If this is legitimate Site it must be whitelisted. Please contact the Information Security Team at informationsecurity@pvamu.edu for assistance.
- **Impersonation Protection** – This is triggered when a user with a PVAMU address uses a personal email address or an external address with the same name to email a PVAMU employee.
- **Suspected Malware** – A malware attachment has been sent to the user and the attachment has been removed.
- **Suspicious Message Structure**– The message has a suspicious message.
- **DMARC Fail** – The senders DMARC (used to properly identify the sender) is not configured.