EMAIL FILTERING FAQ

The implementation of a University wide email filtering system will enhance the security of sensitive data across the entire community.

What is happening? (Keeping our email system secure)

- A new email filtering system has been put into place – it is called Mimecast.

- The new system is robust, performs sophisticated filtering, and integrates well with other recent security updates

- All incoming and outgoing emails are filtered for malicious or phishing messages, spam, dangerous attachments and other security-related issues. If nothing suspicious is detected, your email(s) will be delivered normally.

- This filtering is constantly occurring. However, if an email is held, notifications for these 'Held Messages' will be sent first thing each morning, and each hour through our business hours. If there are no 'Held Messages' for your emails, you will not receive these notifications

Why is this happening?

- The new system is more robust, better at filtering suspicious actions, and able to better integrate with the other security updates the University has recently put into place

What do I need to do about it?

- Nothing – there is no need to manually install or update anything. Most of the work is happening behind the scenes.

- Only if you are a sender or recipient of a suspicious email, you will receive an email from the Mimecast system for you to action

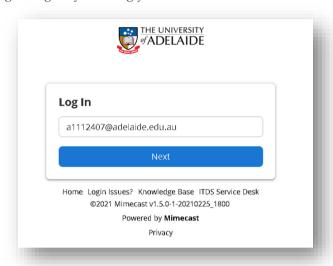- If you do nothing, the message(s) will be purged automatically after 30 days.

Handling Held Messages

- If an incoming message is considered borderline suspicious (sometimes called "graymail") , it will be held for you in Mimecast and you will receive an automated email asking you to make a decision about its safety

- Notifications for held messages will be sent each morning, and each hour during business hours:

  - You will only receive a notification if a message is being held for you.

  - Refer to the screenshot below for an example held message notification.

- You can choose from the following actions for each email or for all email mentioned in the same notification:

  - **Release / Release all** - you agree that the email(s) are safe and wish them to be released to your inbox. This is a one-time action that will not affect how future emails from the same sender are treated.

  - **Permit / Permit all** - you allow this/these email(s) to be released once from this sender as well as add the sender to an "allow list" so that future messages from these senders will never be held.

  - **Block / Block all** - always block messages from this or all of these senders. The senders will be added to your personal "block list" and you will not be bothered again.

- Once you have permitted or blocked a sender, you can only change these settings from the Personal Portal, or by requesting Service Desk.

- You can also access your **Mimecast Personal Portal** (see below for further instructions) to interactively view held messages and configure block/allow rules based on sender..
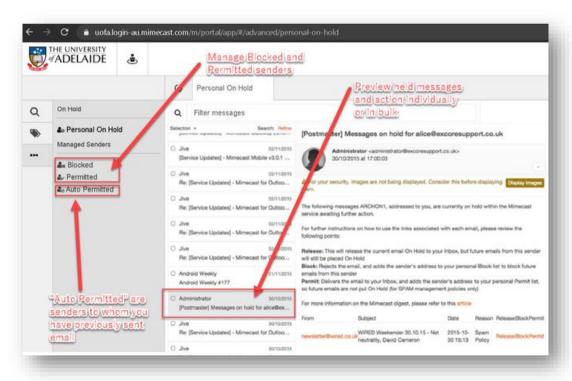
Accessing the Personal Portal

- You can access your Mimecast Personal Portal from this link:
  - https://uofa.login-au.mimecast.com/u/login/?gta=apps#/login.
  - To login, begin by entering your *a-number@adelaide.edu.au*

  - If you have not logged on to other systems, you will be redirected to Okta for authentication, and will be presented with the portal that looks like this:

You cannot access held messages sent to generic mailboxes at this time. Please process held messages individually. If you have accidentally allowed or blocked a sender, contact Service Desk to edit these lists on your behalf.

Blocked Attachment Types

- Some attachment types are deemed dangerous, as they are often used by malicious parties to spread malware or to harvest sensitive information.
- Here are some commonly blocked files, but the list is not exhaustive:
  - Windows executable files (*.exe, *.cmd, etc)
  - Dynamic libraries (*.dll, *.lib, etc)
  - Script files (*.js, *.py, *.sh etc)
- If you have a need to send or receive these file types, please use other means (e.g., sharing via Box or Teams) instead of using email.

What should I do if I need more information?

- For more information please refer to the example above, then https://www.adelaide.edu.au/technology/your-services/email#secure-email-filtering
- If your question is not covered on here, or on the website, please contact servicedesk@adelaide.edu.au