As you've all been reading, phishing attempts and computer ransomware are on the rise, especially following COVID. We're implementing a new solution called Mimecast, to help protect the YWCA from these attacks. On **JUNE 23RD** we will be changing our Anti-Virus/Anti-Spam/Anti-Phishing email filtering solution to this new format.

Transition to Mimecast

The transition to Mimecast will take place on **JUNE 23RD, AT 10AM**. During the transition it is possible that you will receive Quarantine summaries from both Mimecast and Sonicwall Email Security for a short period of time (1-2 days maximum). No email will be lost; it is just a matter of timing as to which provider will scan the incoming messages. Should you have questions regarding migrating specific settings that you may have configured on your Sonicwall Email Security account to Mimecast, please contact Donna Connelly by email or at extension 1217 for assistance.

Anti-Spam Options for Quarantine Messages

As with Sonicwall Email Security you will receive a quarantine message if emails are blocked by the Mimecast system. Quarantine messages will now be sent **TWICE A DAY, BEGINNING JUNE 24TH** and will be sent by "Postmaster" rather than the Admin Junk Summary from thinkCSC that you currently receive. If there are no emails requiring your review at the time specified then you will not receive a Quarantine message.

https://community.mimecast.com/docs/DOC-1724

Digest Options: For each blocked email item you will have 3 actions that can be taken.

- **Permit**: Allows all future messages from this sender and delivers the message. This option should be selected only for known and trusted senders!
- **Block**: Blocks all future messages from this sender (does not deliver the message).
- **Release**: Delivers this particular message from the sender (messages from this sender may be blocked in the future).

On-hold Message Options: Another way to take action on quarantined messages is by logging into Mimecast and checking the "On-hold Message" area.

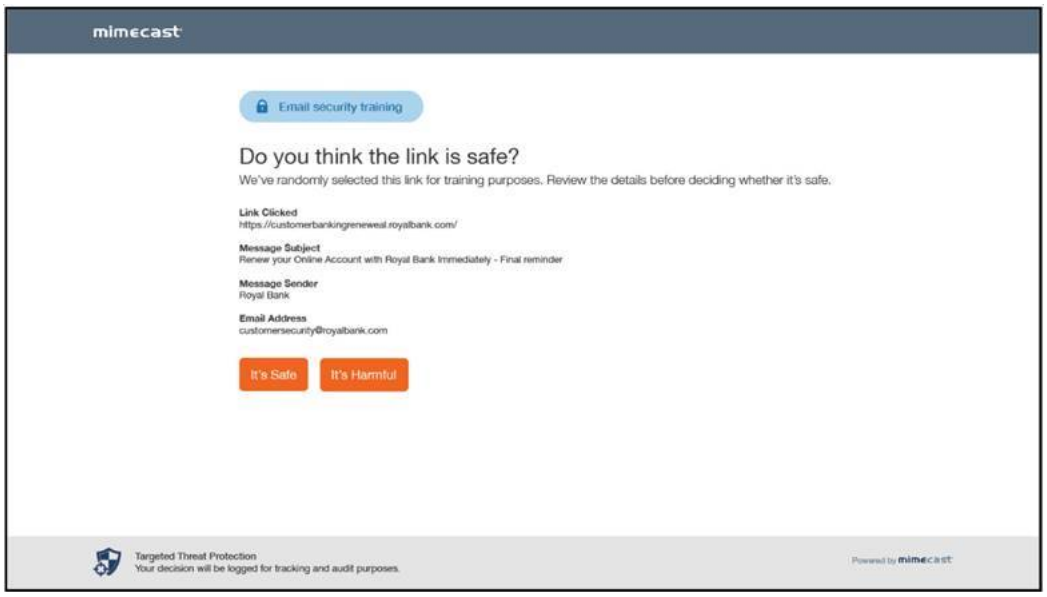
Mimecast Personal Portal (MPP): By clicking this link https://login.mimecast.com/ you will be able to log into Mimecast at any time to review your quarantine list and perform the same actions noted above. Your login will be your email address (i.e. <user@domain.com>) and your password will be the same as your office computer password. The Mimecast password will automatically remain in sync as your office password changes.

Anti-Phishing Options

You will notice a change to how Links and Attachments are handled. Messages including Links and Attachments will now be subject to further hygiene scanning to protect against phishing and whaling attacks.

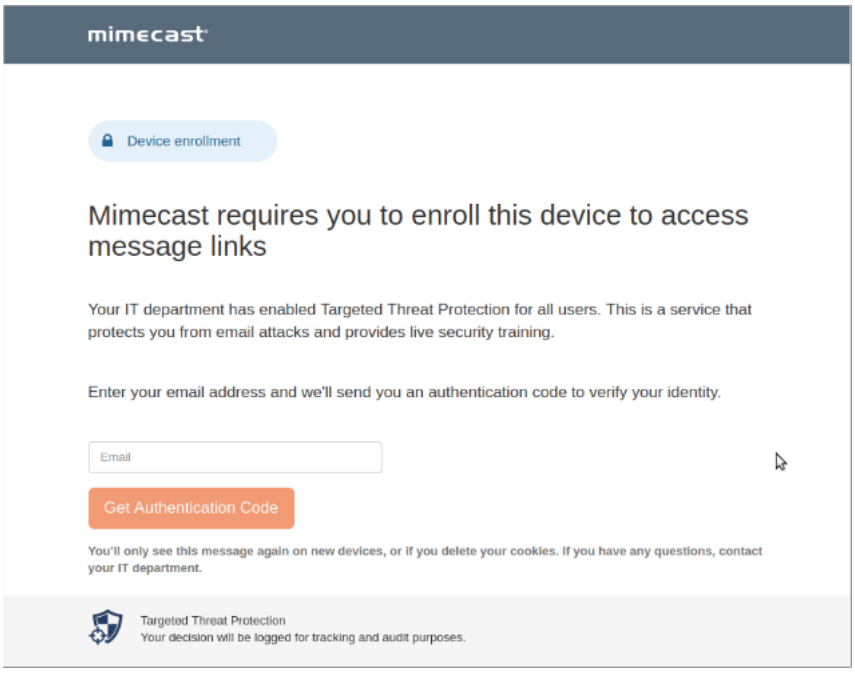
Handling Links Via Email: For a small percentage of links you receive via email, you will be presented with a webpage with information about the email you received and the website you are trying to access. You will be asked to make a decision about whether you are happy to continue to the website,

or if you want to change your mind. By prompting you to think before you click, you will help us strengthen our defenses.



What do I need to do?

The next time you click a link in email, or request the release of an original email attachment, you will be asked to enroll in the Mimecast Targeted Threat Protection service in order to continue. You will only be asked to enroll once on each device you use to access your work email. When prompted in the browser, enter your work email address and hit “Next”. We will send you a one-time authentication code by email which you will need to enter into your browser where indicated.



Should you have any questions or concerns regarding this new service, please do not hesitate to contact the Donna Connelly by email or at extension 1217.