



## **Improved email security with Mimecast**

OMES has partnered with Mimecast, an industry leader in email security and protection, to improve the state's security posture while improving your email experience.

The transition to Mimecast will remove the need for the temporary \_NoClick solution we put in place last year as the analysis for whether a URL, file or other attachment is malicious and will be done automatically behind the scenes.

The transition to Mimecast will occur on May 1, 2020. Since many state employees are currently teleworking, we have taken additional measures to make sure this transition is not disruptive. It is important that we persist in mitigating security risks as the threat landscape continues to evolve.

Additional resources and features related to the Mimecast rollout are below.

If you have concerns or questions regarding specific settings you may have currently configured on your account, please contact the [OMES Service Desk](#) or try our new chat feature on the [OMES webpage](#) where you can chat directly with a Service Desk representative.

## **Digest email**

Mimecast will send a digest email to help manage potential spam, junk content and malware threats. You will receive a digest message, like you did when we used Symantec, if emails are blocked by the Mimecast system. These messages will be sent by [postmaster@omes.ok.gov](mailto:postmaster@omes.ok.gov). You won't receive a quarantine message if there are no emails requiring your review.

To learn more about the digest email, [view this resource](#).

**Digest options:** There are three actions that can be taken for each blocked email item.

- **Permit:** Allows all future messages from this sender. You will receive this message for this action: **This option should be selected only for known and trusted senders.**
- **Block:** Blocks all future messages from the sender and you will not receive the message.
- **Release:** Delivers the particular message from the sender but messages from this sender may be blocked in the future.

**Release**

- You are interested in the content.
- You don't want to add the sender(s) to your personal "permitted senders" list.
- Message(s) released to your inbox.

**Permit all**

- Message(s) are expected.
- You recognize the sender(s).
- You want to receive future messages from the sender(s) directly to your inbox.

**Block all**

- You don't recognize the sender(s) or content.
- Suspicious looking message(s).
- Will not deliver the message(s) to your inbox.
- Sender(s) will be added to your personal block list.

**You have new held messages**

You can release all of your held messages and permit or block future emails from senders, or manage messages individually.

[Release all](#) [Permit all](#) [Block all](#)

You can also manage held messages in your [Personal Portal](#).

**Spam Policy**  
[sent\\_from@mailservice.com](#)  
 Relaxed  
 2020-04-07 20:48  
[Release](#) [Permit](#) [Block](#)

**Spam Policy**  
[sent\\_from@mailservice.com](#)  
 Testing Malicious URL  
 2020-04-07 20:59  
[Release](#) [Permit](#) [Block](#)

[Release all](#) [Permit all](#) [Block all](#)

**Personal Portal**

- Login with your State email address and network login password.
- The Portal allows further review of the suspect message(s), and more message management options beyond the simple Release, Permit, and Block.

Powered by **mimecast**

## Mimecast Personal Portal

You can log in to the [Mimecast Personal Portal](#) at any time to review your quarantine list and perform the actions noted above.

Your login will be your email address 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.