eHealth Saskatchewan

Encrypted and Quarantined Email Notifications from eHealth Saskatchewan User Guide

As of May 15, 2023

Version 1.0

Encrypted and Quarantined Email Notifications from eHealth Saskatchewan User Guide

Microsoft 365 Project

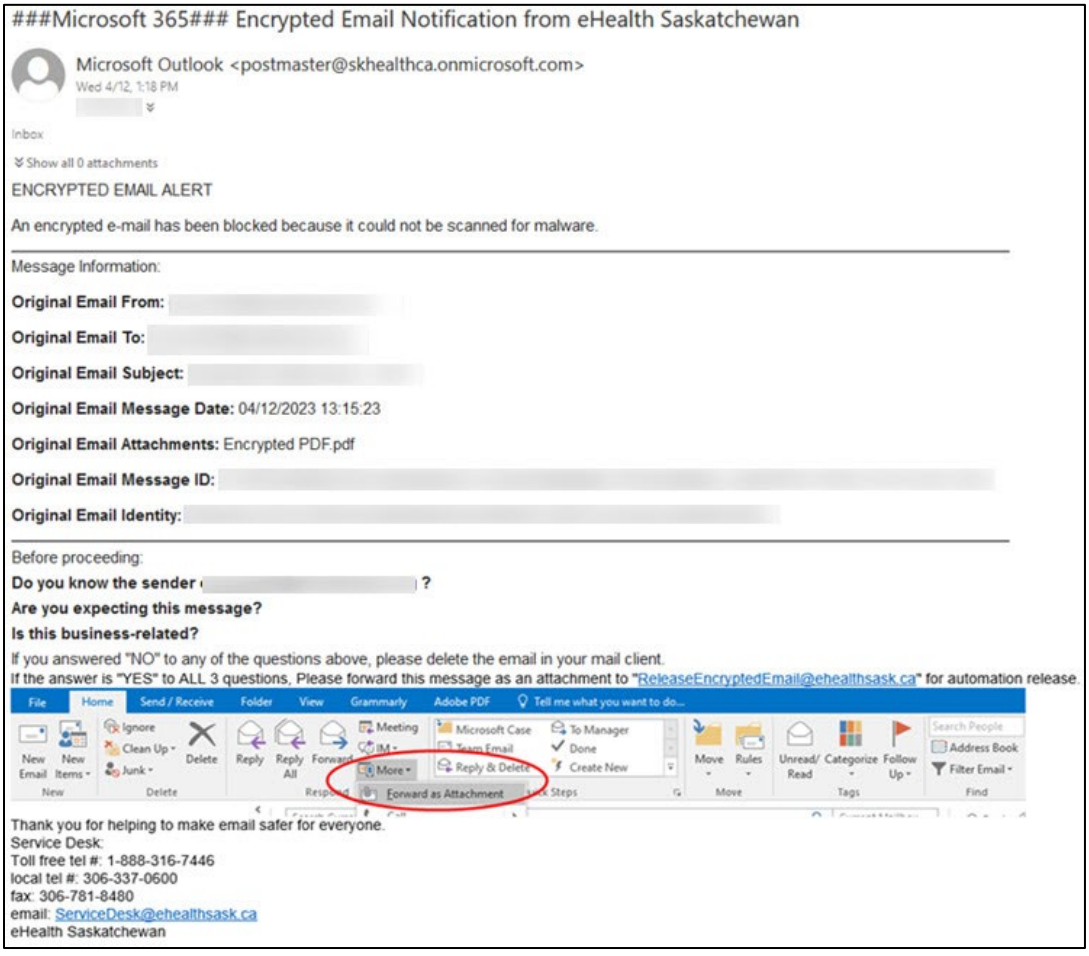
1. Moving to Exchange Online

As part of the Microsoft 365 modernization project, eHealth is moving to Exchange Online Protection (EOP). Exchange Online Protection (EOP) is the cloud-based filtering service that helps to protect our organization against spam, malware and other email threats. The key difference is that all encrypted emails will now be quarantined and the way Outlook handles those quarantined messages. When a message is quarantined you will receive an email notification message.

2. The Different Types of Notifications Received

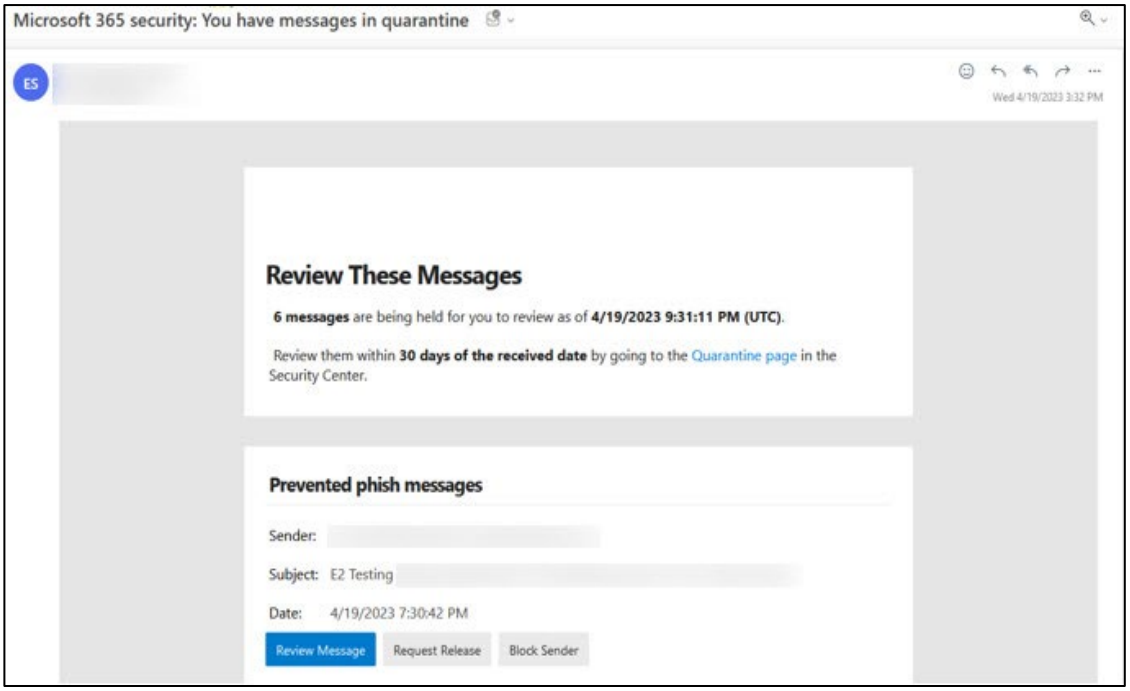
a. Encrypted Email Notification

When someone sends you an email with an encrypted attachment it is placed temporarily in the quarantine folder. You will receive the following **Encrypted Email Notification:**



b. "You have messages in quarantine" Email Notification

When someone sends you an email that may seem suspicious it is temporary blocked and placed in the quarantine folder. You will receive the below **"You have messages in quarantine"** email notification:



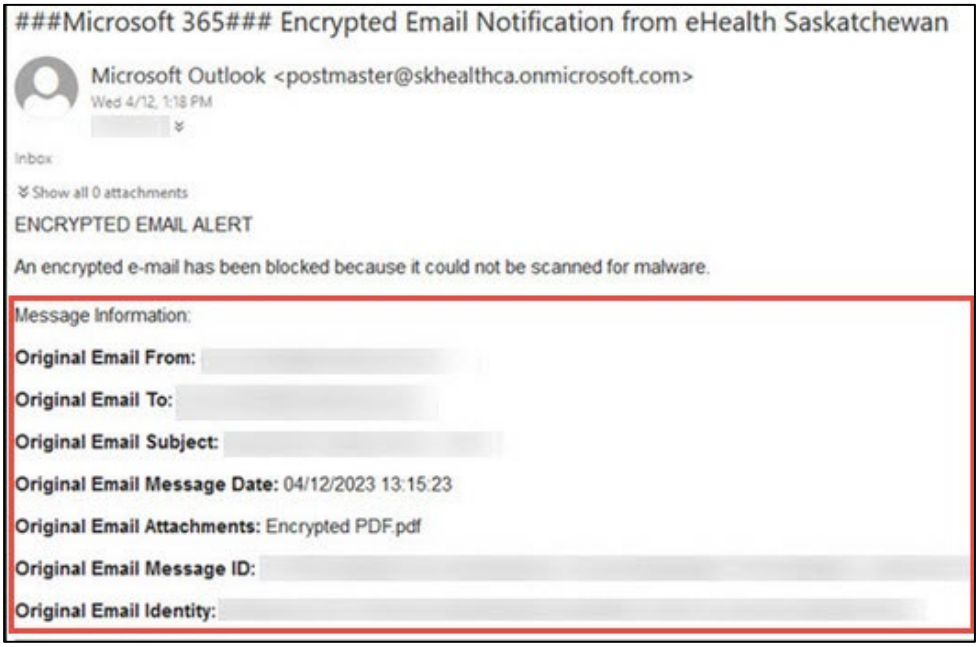
Contact the **eHS Service Desk** for assistance
Return to first page

Encrypted Email Notification

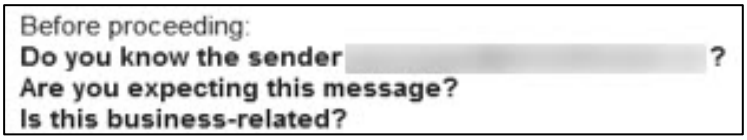
Background: This is in reference to when someone sends you an email with an encrypted attachment.

1. Request to Release Quarantined Message and Attachment

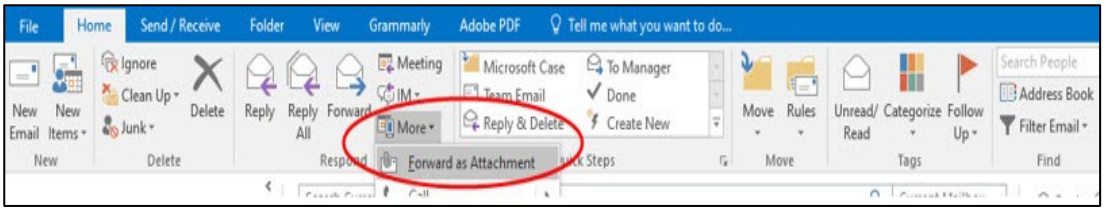
a. Review the **Message Information** from the Encrypted Email Notification and determine whether you are expecting this email.



b. Before requesting to release the quarantined message and attachment, ensure you are able to answer **YES** to all 3 questions.



c. If you were able to answer **YES** to all 3 questions, forward the email as an attachment to **ReleaseEncryptedEmail@ehealthsask.ca**



NOTE: You only have 30 days to respond to the email notification, after which the encrypted email is deleted. If deleted you will need to reach out to original sender to request them to resend you the email.

2. Delete Unwanted Email Notification

a. Determine whether the email is possible spam, junk or a part of a phishing email:

NOTE: This refers to an email (usually some form of advertising) sent to multiple customers. (e.g. Prescription drug sales). They appear to come from legitimate sources and contains external links which may be a part of a Phishing attack.

- **Yes -** Contact the eHealth Service Desk at **1-888-316-7446.**
- **No –** Continue to next step.

b. If you have determined the email is unexpected and not spam or junk email, you may either:

i. **Delete** the email in question.

ii. Disregard the email and do not respond or forward the attachment as it will automatically be deleted from quarantine within 30 days.

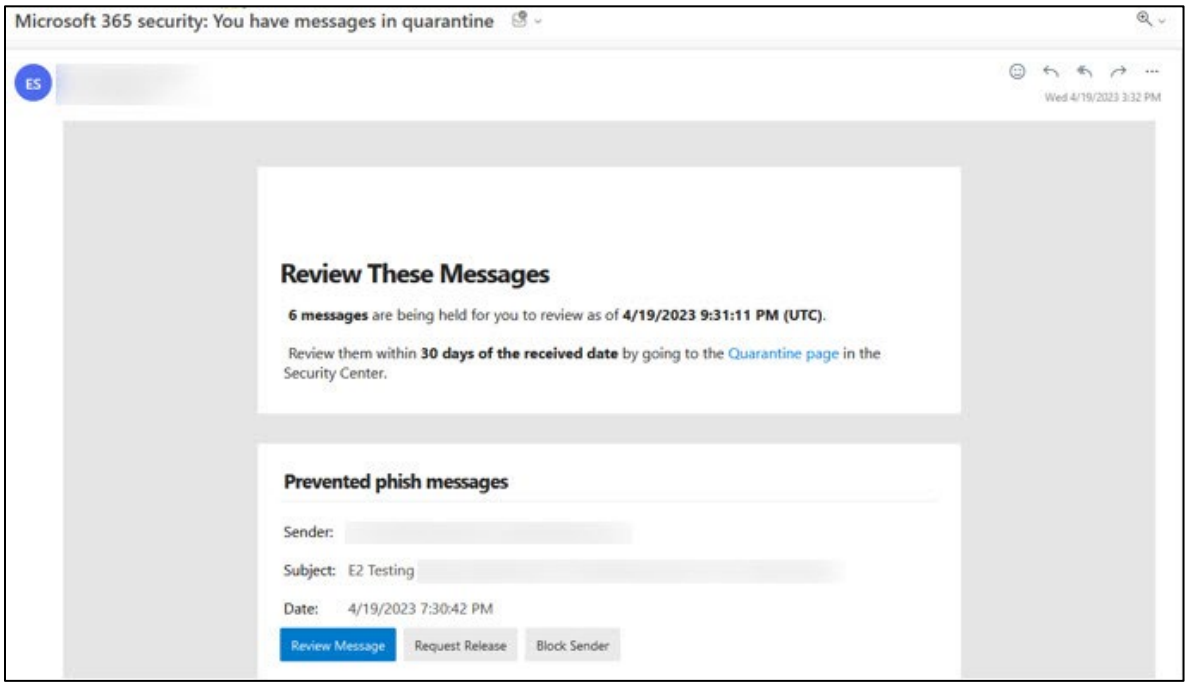
3. Did not Receive Released Encrypted Message and Attachment

a. After forwarding attachment to **ReleaseEncryptedEmail@ehealthsask.ca** , ensure **30 minutes** has elapsed since requesting the release of the encrypted message. If time has elapsed then contact the eHealth Service Desk at **1-888-316-7446** to log a service request to investigate further.

Contact the **eHS Service Desk** for assistance
Return to first page

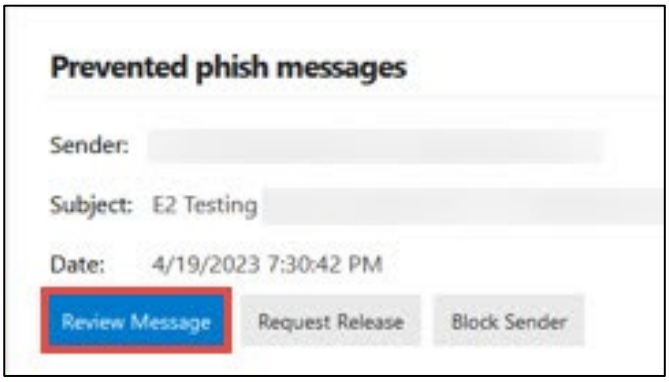
'You have messages in quarantine' Notification

Background: This is in reference to a suspicious email that is currently blocked and residing in the quarantine folder which needs to be actioned.



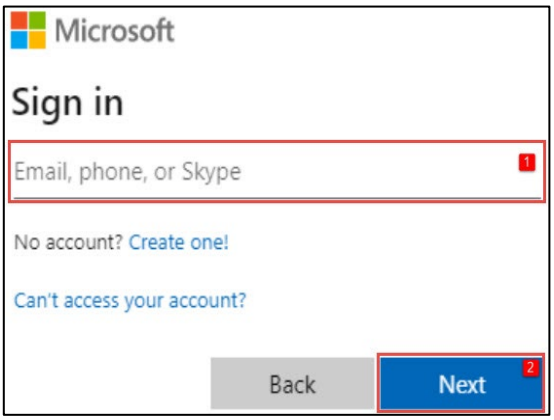
1. Review Message

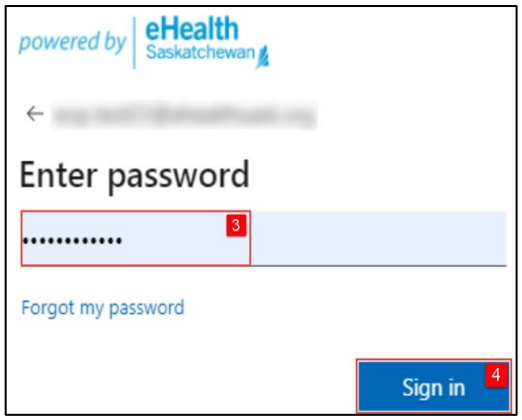
a. To preview the email message, click **Review Message** from the **Prevented phish messages** section:



b. Determine whether presented with the Microsoft Sign in screen:

- **No –** Continue to next step.
- **Yes -** Enter your **ehealthsask.ca** email address, click **Next**, enter **network password** and then click **Sign in**.

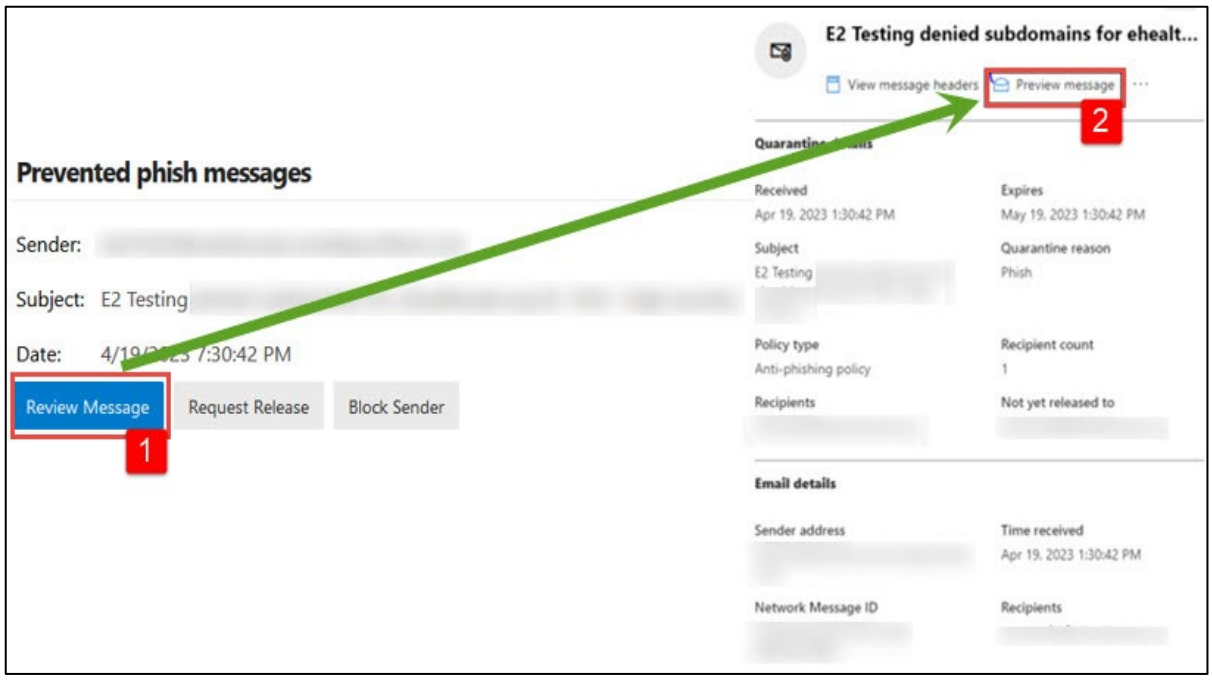




NOTE: Should you encounter any problems with signing in, please contact the **eHealth Service Desk** at **1-888-316-7446**.

c. Click on the **Outlook** icon from the left hand side of the **Microsoft 365** home screen.

d. From the quarantine message in question, click **Review Message** and then click **Preview message**.



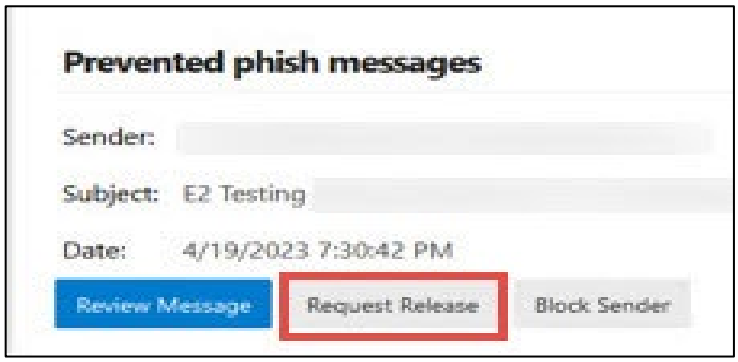
e. Determine whether the content in the email was legitimate:

- **Yes –** Continue to the **Request Release** section
- **No -** Delete email or continue to the **Block Sender** section.

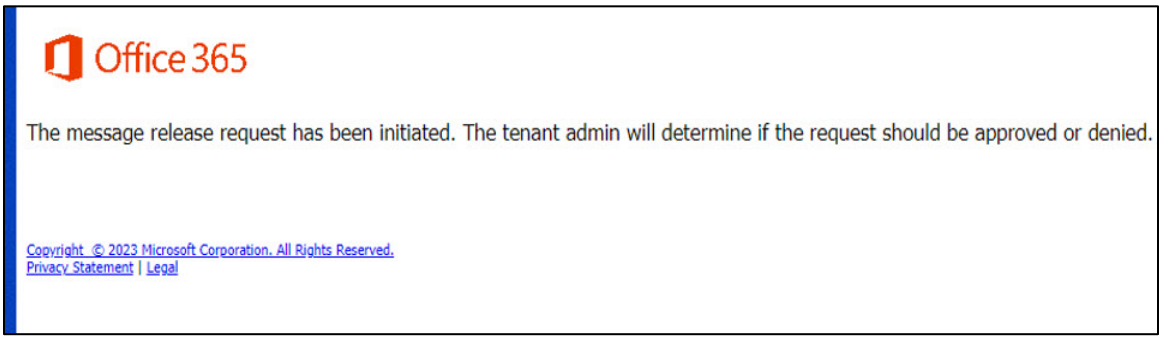
  NOTE: If you believe email is possible spam, junk or a part of a phishing email contact the eHealth Service Desk at **1-888-316-7446.**

2. Request Release

a. After determining the content of the email is legitimate, click on **Request Release:**



b. After clicking on **Request Release,** you will receive the following message:



c. After clicking the '**Request Release**' Button, ensure 30 minutes has elapsed since requesting the release of the Quarantined message. If time has elapsed then contact the eHealth Service Desk at **1-888-316-7446** to log a service request to investigate further.

3. Block Sender

a. After previewing the email and you determine the content of the email is not legitimate, either delete email or click on **Block Sender**.

b. After selecting **Block Sender** you will receive the following message:

NOTE: These emails will be directly delivered to the Junk email folder and automatically deleted within 24 days.

Contact the **eHS Service Desk** for assistance
Return to first page

Acronym List

eHS	eHealth Saskatchewan
SHA	Saskatchewan Health Authority

Version History

1.0	*KBA*	*May 15, 2023*
2.0	*KBA*	*May 15, 2023*
3.0	*KBA*	June 22, 2026

Contact eHS Service Desk

For **immediate technical assistance** call the **eHealth Service Desk** at **1-888-316-7446** For other **non-critical technical issues** please contact: ServiceDesk@eHealthsask.ca