

Lab 07: Encrypted phishing with Unified Labeling

Table of Contents

Lab 07: Encrypted phishing with Unified Labeling.....	1
Goals	1
Requirements.....	1
1. Enable Unified Labeling in Azure and Microsoft 365.....	1
2. Send an encrypted email with Unified Labeling	3
3. Observe the encrypted email from the recipient's point of view.....	7

Goals

- Enable Unified Labeling on your domain.
- Send an encrypted email message and observe the email from the recipient's point of view.

Requirements

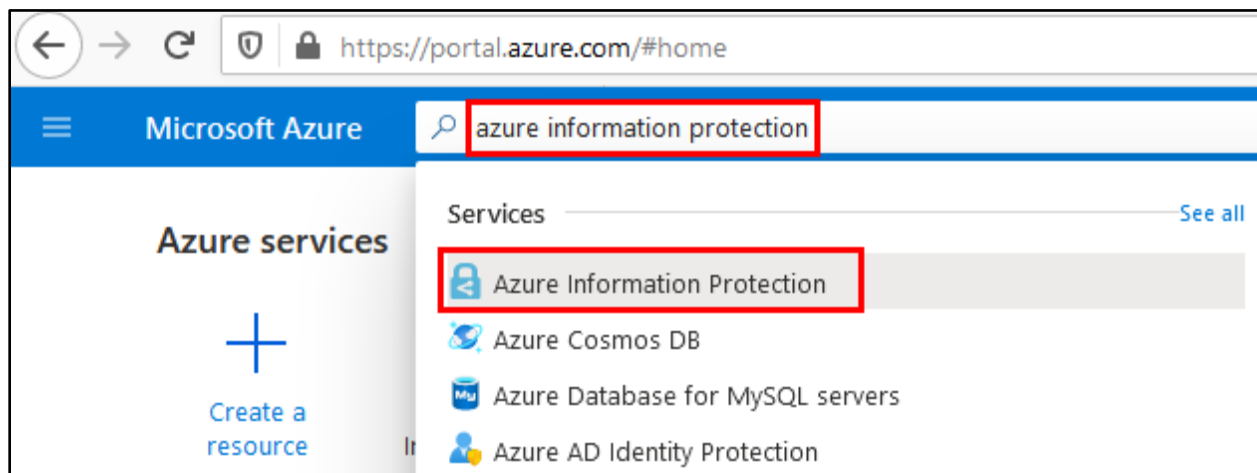
- Microsoft 365 Business Premium trial account.
- Microsoft Azure trial account.
- Optional: A work/personal email account to be used as a recipient.

1. Enable Unified Labeling in Azure and Microsoft 365

1. Log in to portal.azure.com with your organization administrator account.

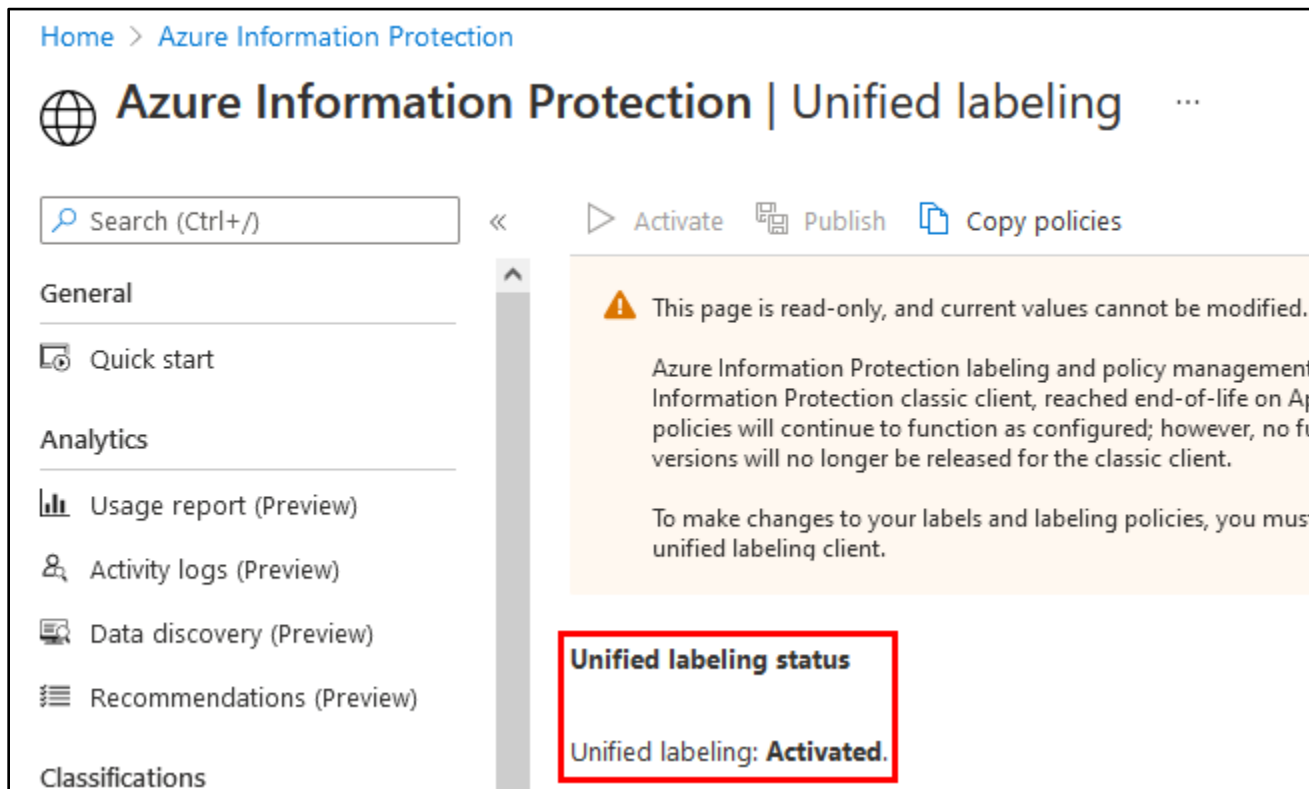
`https://portal.azure.com`

2. Use the search box at the top of the Azure Portal to search for "Azure Information Protection". Press Enter or click on the "Azure Information Protection" item that appears under "Services".



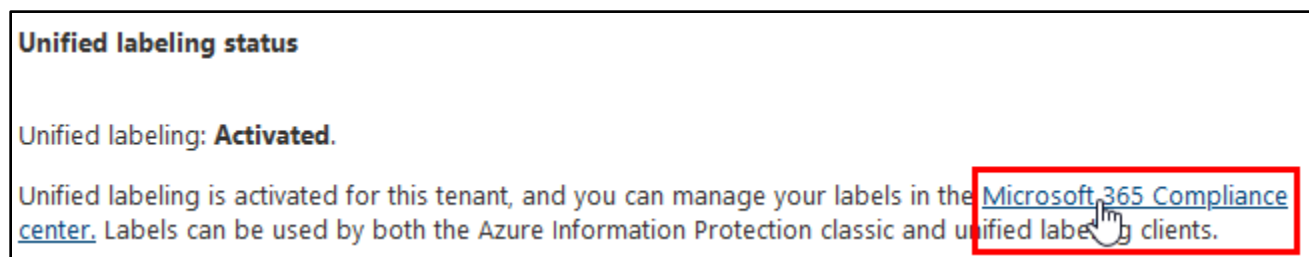
Searching for Azure Information Protection

3. Unified Labeling is activated by default on new Microsoft 365 Business Premium accounts. You should see a message confirming that Unified Labeling is Activated on the page.



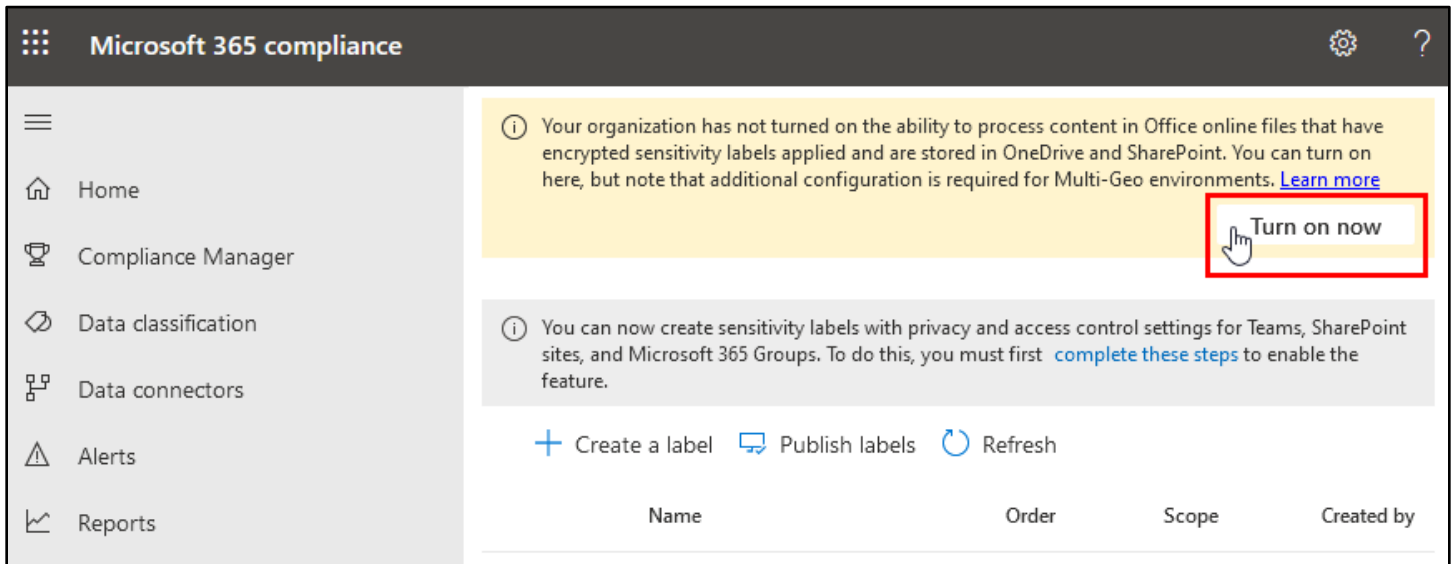
Confirmation that Unified Labeling is Activated in Azure

4. Although the Unified Labeling status is "Activated", you still need to turn on content processing to enable sending encrypted emails. To do this, click on the link to the Microsoft 365 Compliance center on the right side of the page.



Link to Microsoft 365 Compliance Center

5. Scroll down the main page of the Microsoft 365 Compliance center until you see a button that says "Turn on now" beneath a message about turning on content processing for your environment. Then click the "Turn on now" button. This will enable your users to send emails encrypted by Unified Labeling.

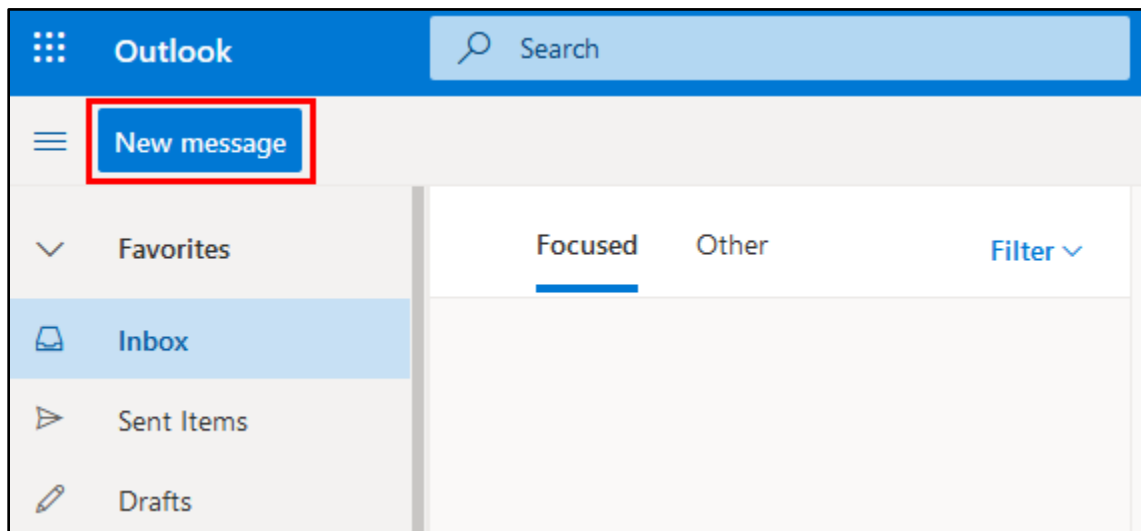


Clicking "Turn on Now"

2. Send an encrypted email with Unified Labeling

1. Log in to outlook.office.com with either your Alice or Bob user account, and create a new email message.

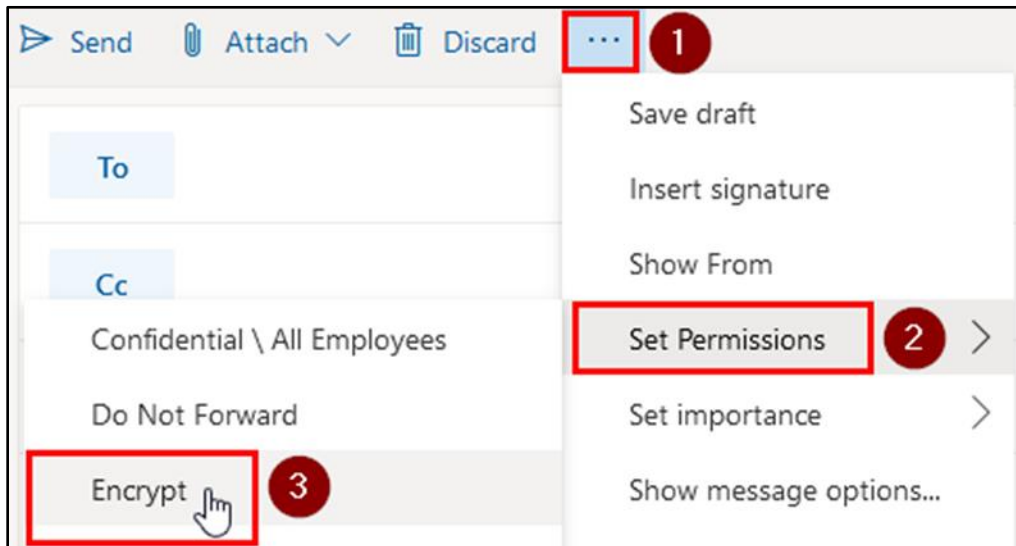
https://outlook.office.com



Creating a New Email Message

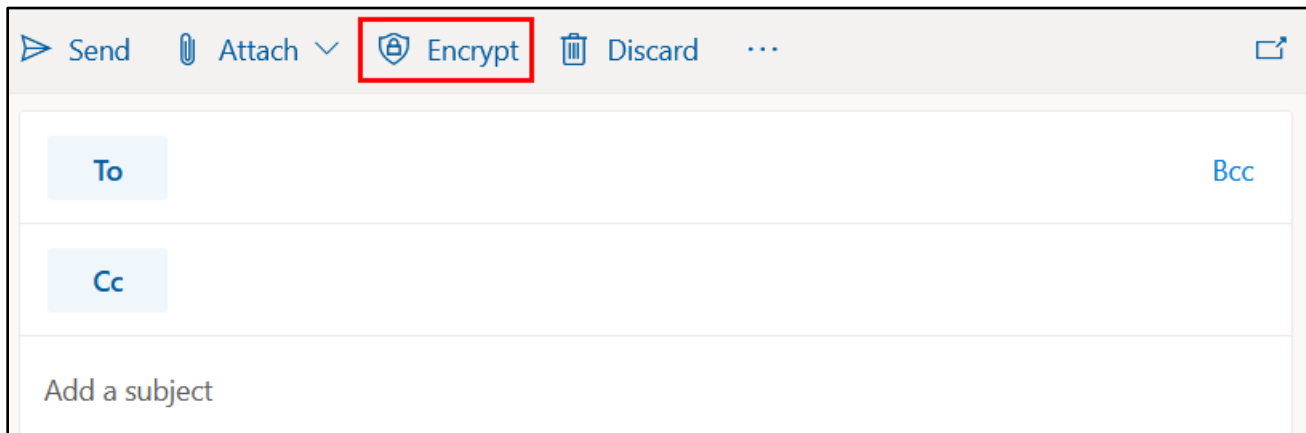
2. Next, click the three dots in the menu bar at the top of the new message interface. You should now see a menu item labeled "Set Permissions". Click on "Set Permissions" in the menu, and in the sub-menu that appears, you

can assign permissions to the email message, such as "Encrypt" or "Do Not Forward". For this example, click "Encrypt" to enable encryption on your email.



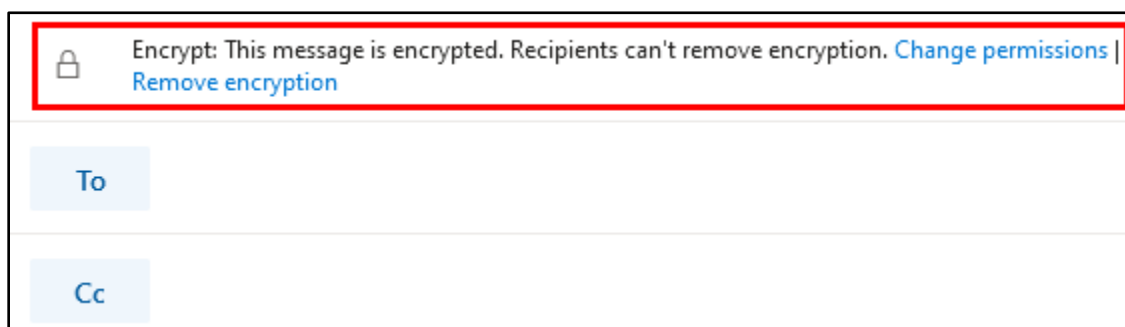
"Encrypt" Button Shown in the "Set Permissions" Sub-Menu

In some instances, the Encrypt button may appear directly in the toolbar, as shown below. Either way, the effect will be the same.



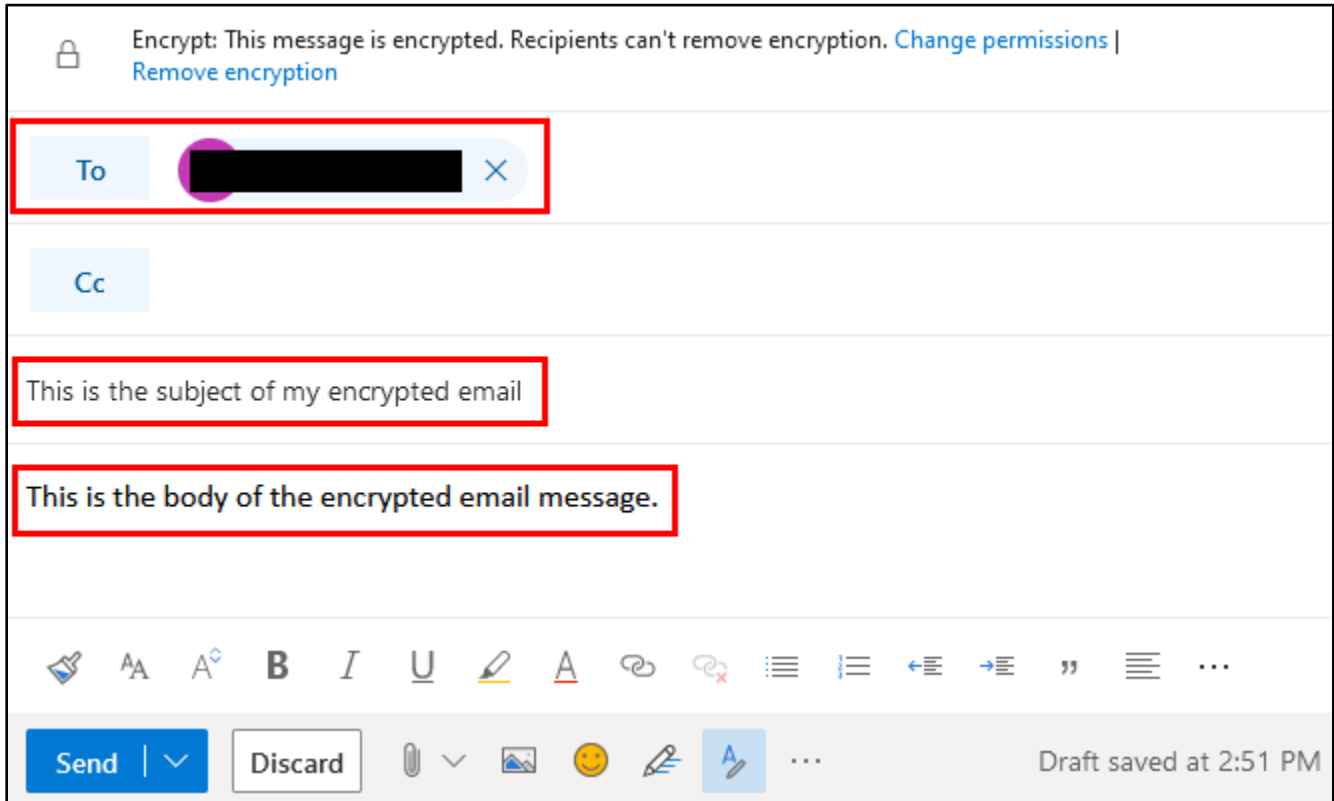
Alternate Location of the Encrypt Button

3. After clicking Encrypt, you should notice a message appear at the top of the new email interface, stating that the message is encrypted.



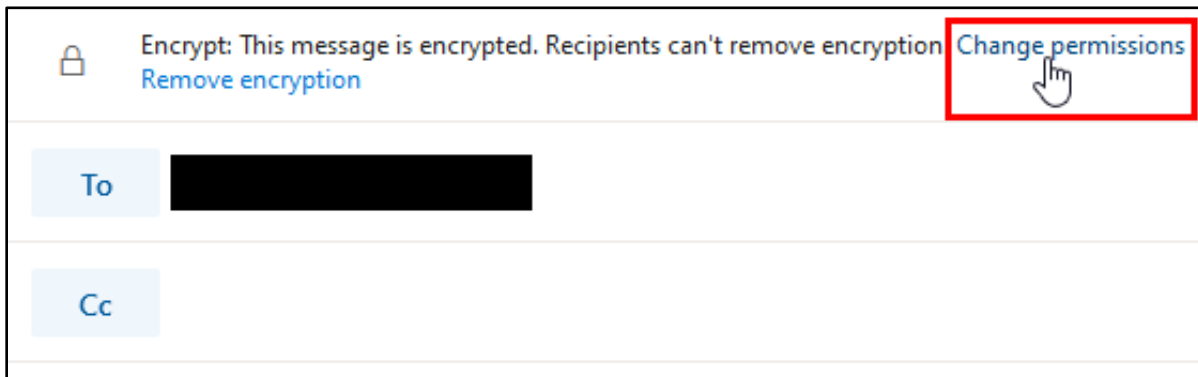
Confirmation of Email Encryption Shown

4. To see what an encrypted email message looks like when delivered to a user at another organization or email provider, fill in the recipient email address (To) with your work or personal email address. Fill in the Subject, and Message Body fields with sample text.



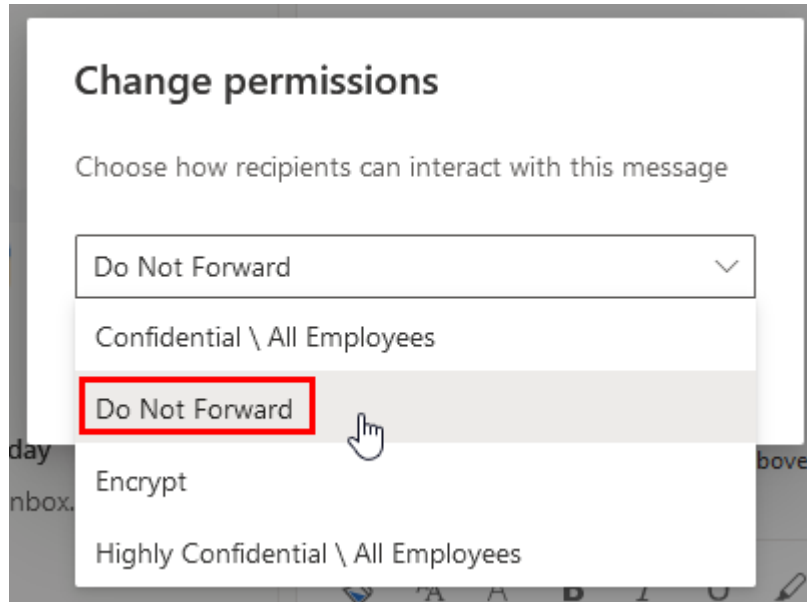
Sample Encrypted Email Creation

5. You can also use the "Change permissions" link in the message that appeared to add additional restrictions to the message.



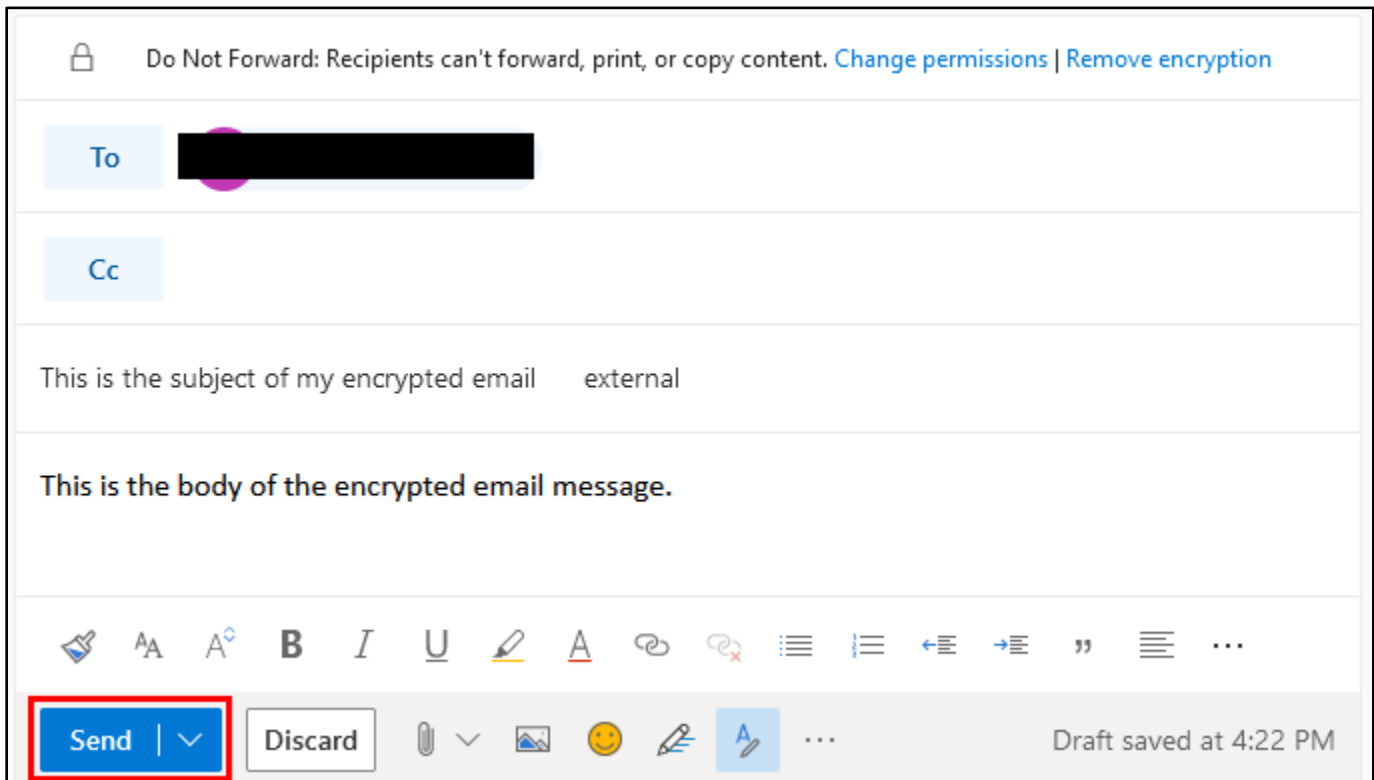
Change Permissions Link

6. Changing the permissions from "Encrypt" to "Do Not Forward" will prevent the recipient from forwarding the email message to other users **in addition** to encrypting the message. This can be useful for preventing end users from forwarding phishing messages to their security team.



"Do Not Forward" Feature

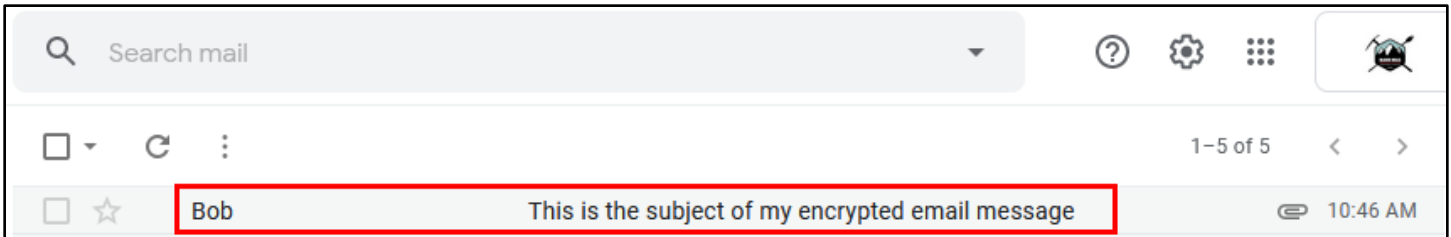
7. Once you have finished creating your email message, click the "Send" button to deliver the message to the recipient.



Send Button

3. Observe the encrypted email from the recipient's point of view

1. Login to the recipient email account where your encrypted email was delivered to view the email from the recipient's point of view. Regardless of email client, the sender's name and email subject are not encrypted and should appear as normal when listed in the recipient's inbox.

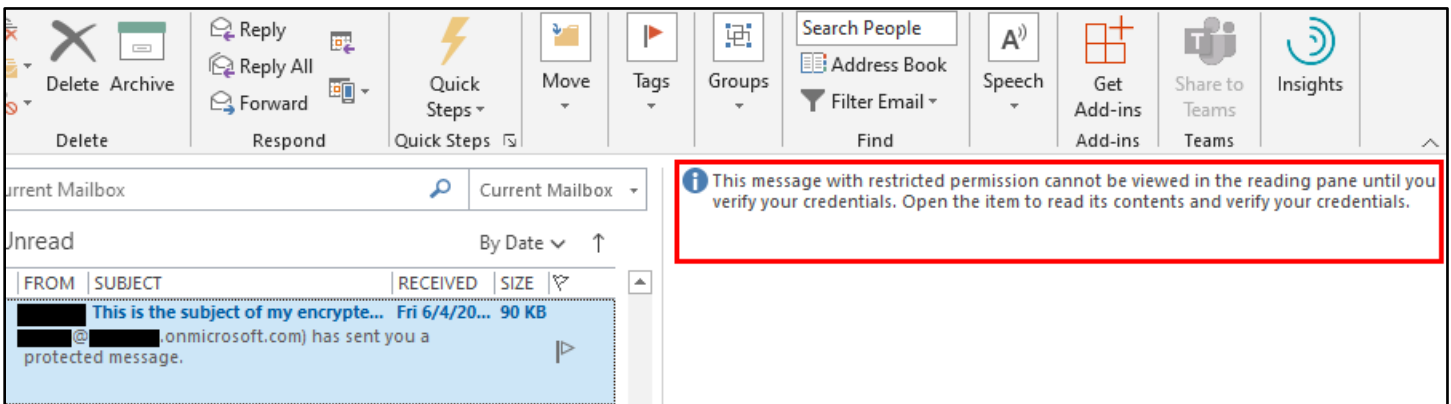


Sender Name and Subject are not Encrypted

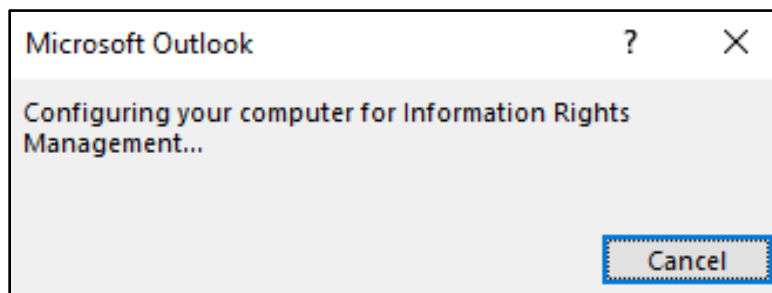
2. Examples of opening the encrypted message in various email clients are included below.

Opening the Message in Outlook

1. If the recipient uses the Outlook desktop application, the message may not be shown in the preview pane until the user double-clicks on the message to open it. The user may also see a pop-up message stating that Information Rights Management is being configured the first time they open a message that has a Unified Labeling policy applied.



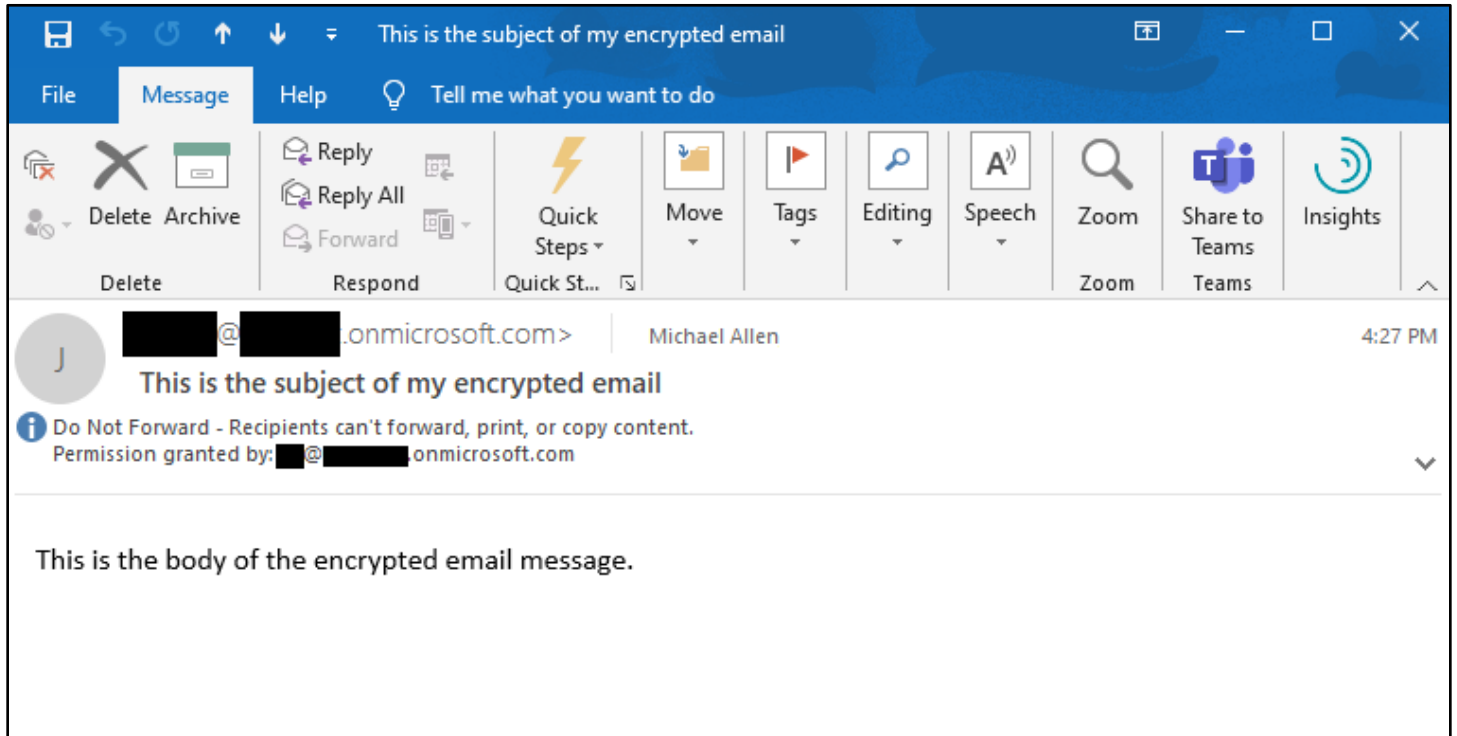
Encrypted Email Shown in the Outlook Desktop Inbox



A Pop-Up May Appear on First Use

2. After opening the message, it behaves as any normal email message - except that if the Do Not Forward permission was applied, Outlook prevents the user from forwarding the message or from taking screenshots of

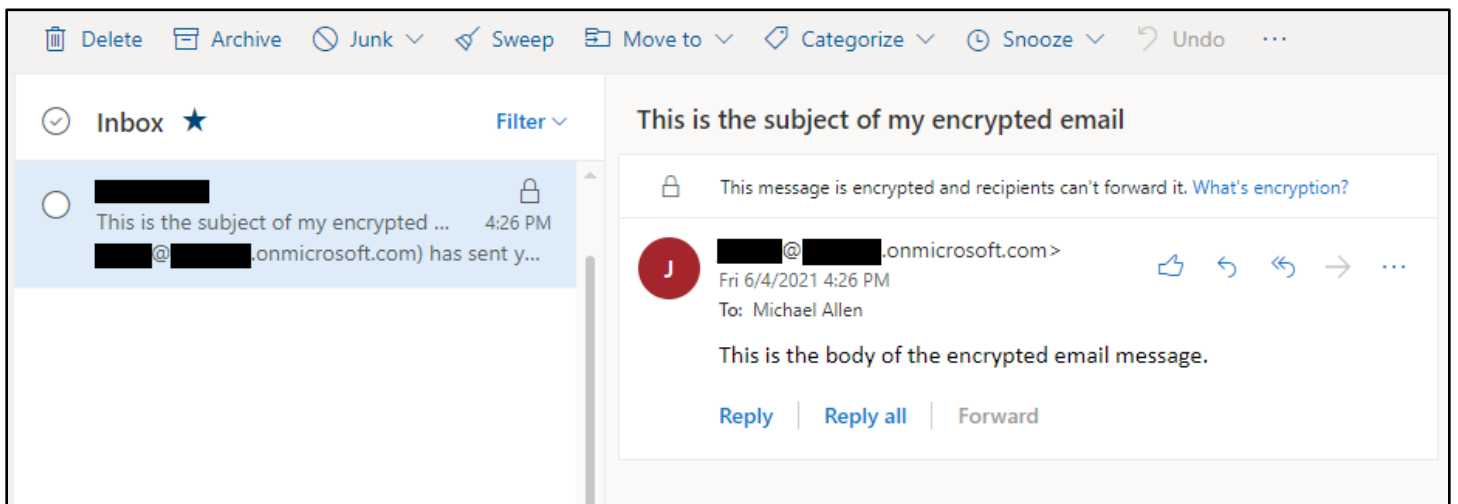
the message. (This screenshot had to be taken by running the Outlook application in a VM and taking a screenshot in the host OS.)



Encrypted Email Message Opened in the Outlook Desktop App

Opening the Message in the Outlook Web Interface

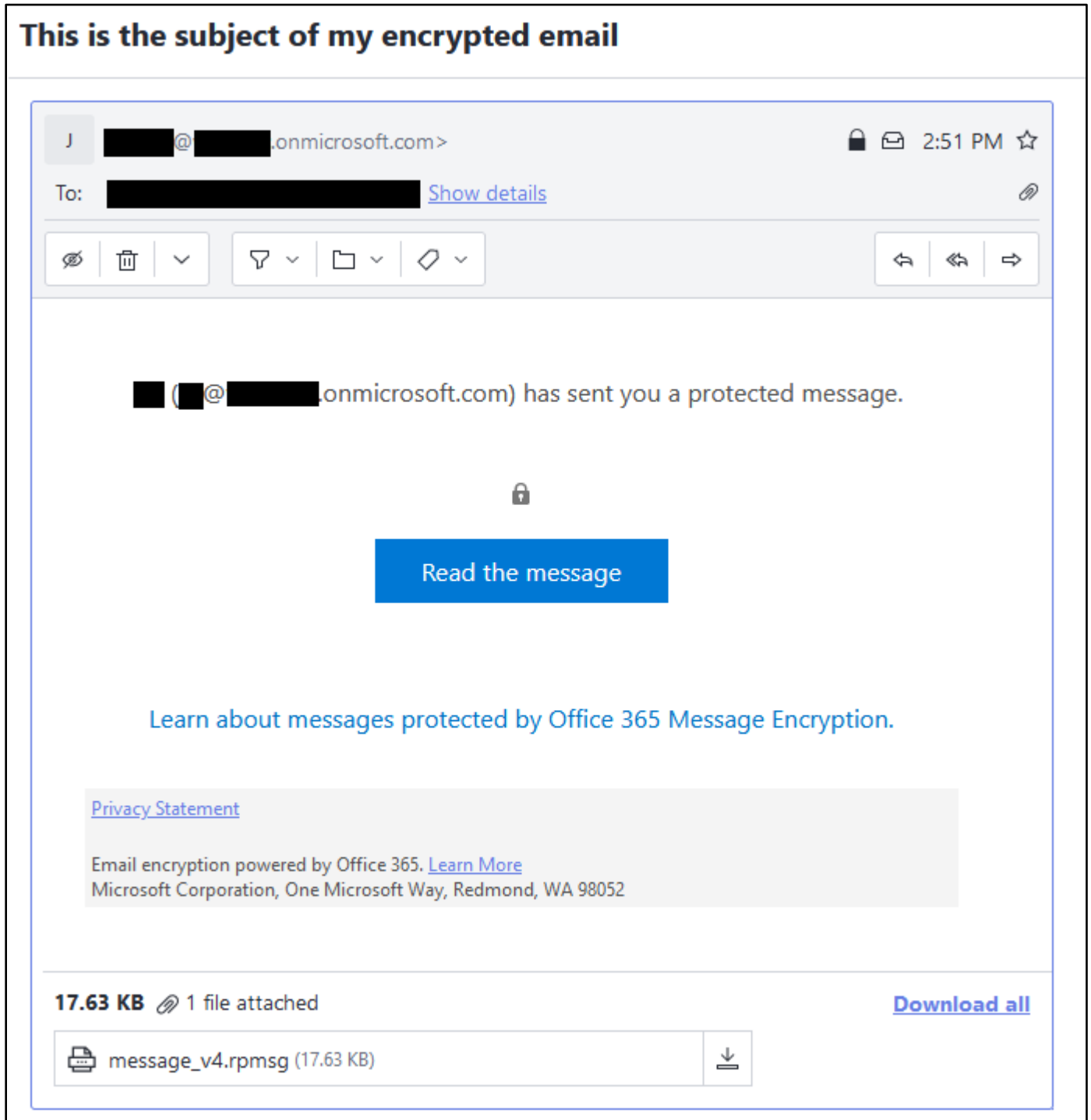
1. If the recipient opens the email from the Office 365 Outlook web interface, the message is displayed as normal in both the preview pane and when opened in new windows - again with the ability to forward the message disabled.



Encrypted Email Message After Opening in the Outlook Web Interface

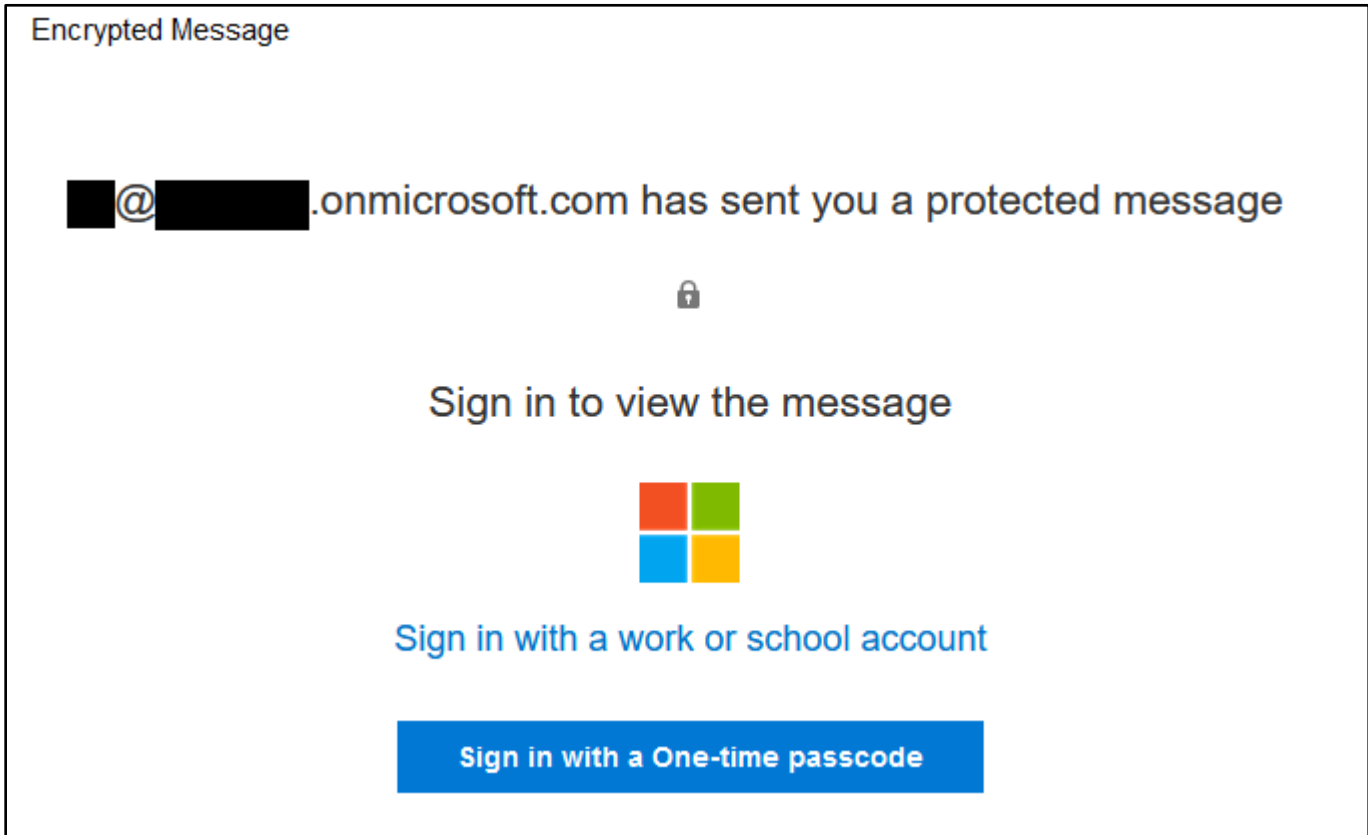
Opening the Message Outside of Outlook

1. If the recipient uses a non-Outlook client or service to open the encrypted message, the user is prompted to read the message by clicking a button in the message body.



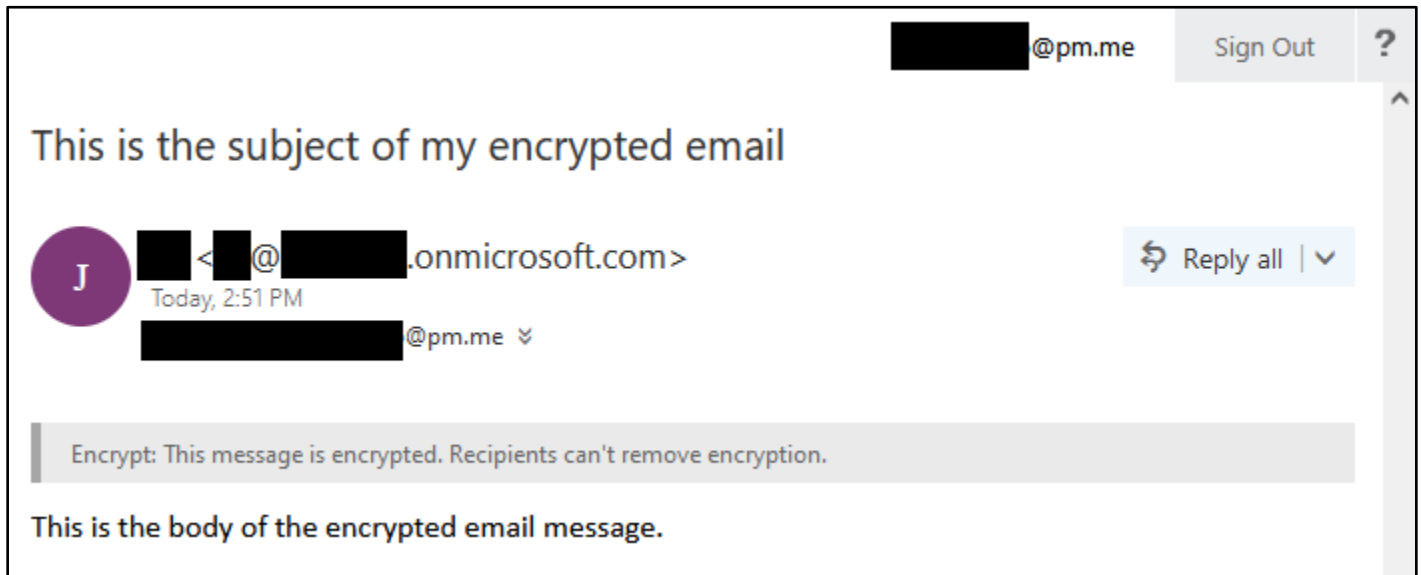
Encrypted Email Message as Shown in the Proton Mail Web Interface

- After clicking "Read the message", the user is prompted to verify their identity by logging in or by receiving a one-time code sent to their email.



Sign-in Page Shown After Clicking "Read the message"

- Once the user's identity has been verified, the message is displayed in the web browser via Outlook.com.



Encrypted Message Opened After Sign in