

EMAIL ENCRYPTION – HOW TO USE IT AND WHY

Section 1: Understanding Email Encryption

Email encryption is a technique that safeguards the content of email messages. It converts readable plain text into scrambled cipher text. The intended recipient - and only the intended recipient - can decipher the message, turning it back into readable text.

The primary aim of email encryption is to shield sensitive data from unauthorized access. This becomes especially vital when dealing with Personally Identifiable Information (PII).

Section 2: Understanding Personally Identifiable Information (PII)

PII refers to any information that can be used to identify an individual. It includes, but is not limited to:

- Social Security numbers
- Driver's license numbers or State identification card numbers
- Financial account numbers, credit or debit card numbers, accompanied by any necessary security code, access code, or password
- Medical information

When unencrypted or unredacted, these pieces of information can lead to identity theft or other forms of privacy invasion. Thus, it is essential to handle this data with utmost caution.

Section 3: Activating Encryption

To send an encrypted email, simply include "SecureMail" in either the subject line or body of your email. Office 365 will then automatically encrypt your message. The recipient will then need to authenticate themselves to decrypt and read the email. Note that only the user to whom the message is sent will be able to open the message.

Section 4: When to Use Email Encryption

Email encryption should be used whenever you send emails that include PII. This applies to both internal and external communications. By doing so, we not only ensure legal compliance but also build trust with our clients and partners, reinforcing our commitment to rigorous data security and privacy standards.

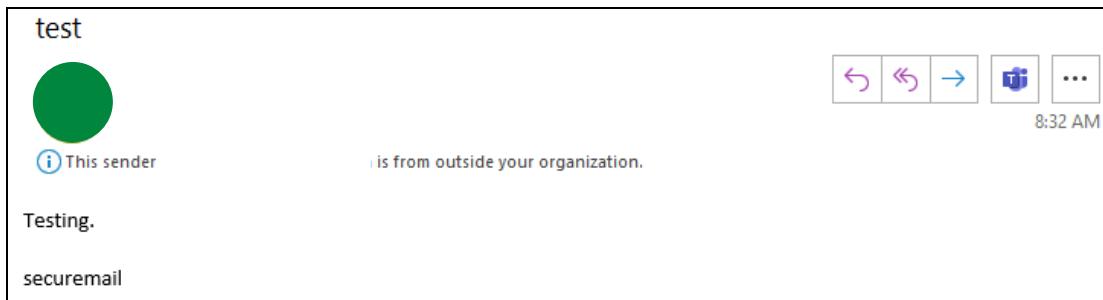
VIEW & REPLY TO AN ENCRYPTED MESSAGE USING OUTLOOK

If you are in a Microsoft 365 organization, you can read encrypted messages in Outlook 365 (For PC/Mac and OWA).:

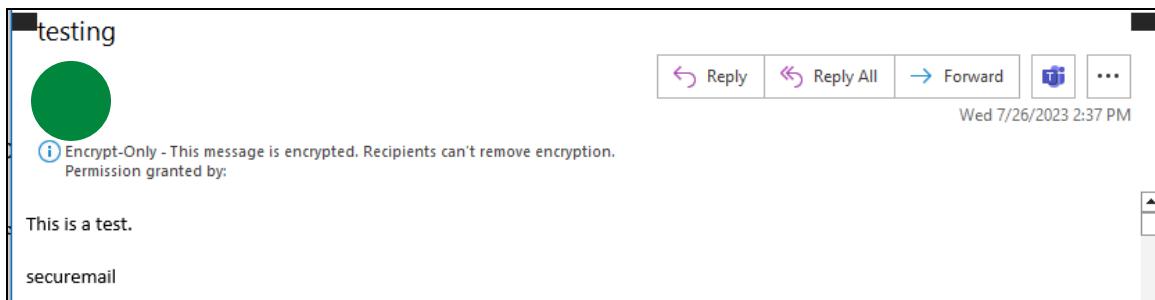


This lock icon will show in the email preview.

Whether receiving a message from inside or outside the organization,



Open the attached Outlook item to view the encrypted message:



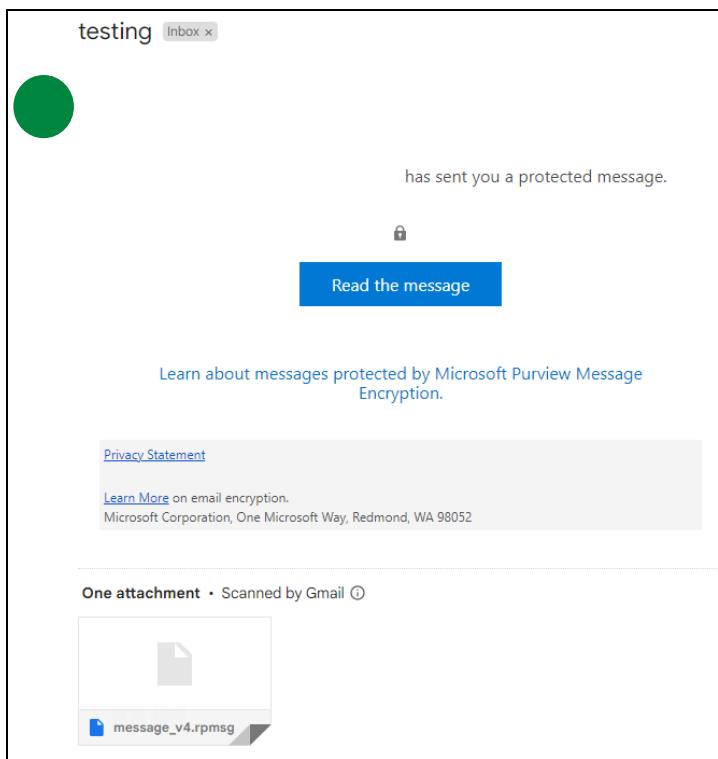
To reply to an encrypted message

1. Choose **Reply** or **Reply All**.
2. On the page that appears, type a reply and choose **Send**. An encrypted copy of your reply message is sent to you.

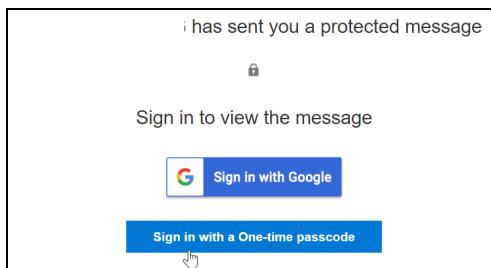
VIEW & REPLY TO AN ENCRYPTED MESSAGE WITHOUT MICROSOFT 365

If you're not using Outlook with Microsoft 365, your encrypted message will contain a link in the message body.

For example, in Gmail:



1. Select Read the message.
2. Select how you'd like to sign in to read the message. If your email provider is Google, Yahoo, or Microsoft, you can select Sign in with Google, Yahoo, or Microsoft respectively. Otherwise, select sign in with a one-time passcode.



3. Once you receive the passcode in an email message, make a note of the passcode, then return to the web page where you requested the passcode, enter the passcode, and select CONTINUE.

Tip: Each passcode expires after 15 minutes. If that happens, or if you can't open the message for any reason, start over by opening the attachment again and following the steps.