Northern Trust
Secure Email
Client User Guide

Version 3.0

NORTHERN
TRUST

Table of Contents

Northern Trust Secure Email

How Does Encryption Work?

Northern Trust uses a secure method to facilitate e-mail communication called Secure E-Mail. This secured approach is supported by Microsoft Purview Message Encryption. Encryption software minimizes the potential for unauthorized individuals to view information that is confidential or proprietary by converting an e-mail message and contents into an unreadable format. The message is decrypted on the receivers end by logging in, which converts the message to clear text so that it can be read.

Why Should You Use Secure Email?

Protecting client information is required by current privacy laws and banking regulations and is considered a good business practice. Electronic communication presents a unique set of trust issues, which business must address at the outset to minimize risk.

Using Microsoft Purview Message Encryption

Northern Trust clients will be able to access encrypted emails sent by Northern Trust in two ways:

Option 1 – Microsoft 365 Users

> Clients using Microsoft 365 email server and accessing their emails on MS Outlook or Outlook on the Web (OWA), will receive their email in MS Outlook (Desktop or Mobile) or OWA in clear text. In such a case, they do not have to take any additional step to decrypt the email.

Option 2 – Non-Microsoft 365 Users

> In case the client is not using Microsoft 365 email on MS Outlook or Outlook on the Web, client's will receive a message in their Inbox informing them about receipt of an encrypted email. In such cases, they will have to click on the link in email that will take the user to OME portal (O365 Message Encryption- https://outlook.office365.com). Clients will then follow instructions on Microsoft 365 portal to retrieve an encrypted email.

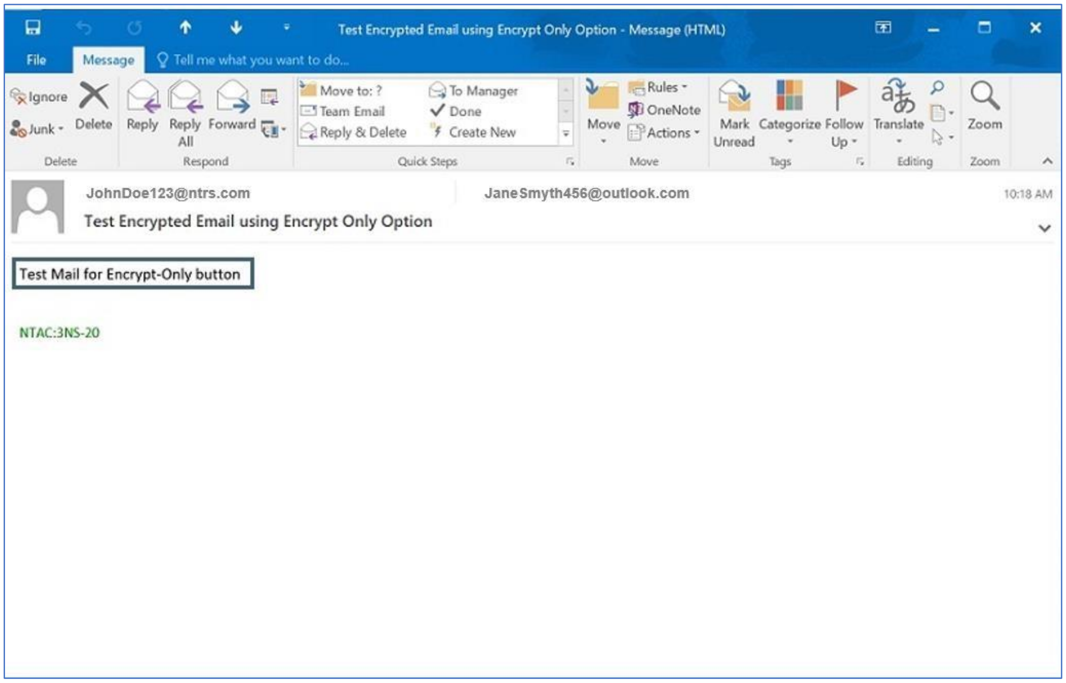
Following sections provide details on the above three scenarios:

Option 1 – Microsoft 365 Users

Clients using Microsoft 365 email server and accessing their emails on MS Outlook or Outlook on the Web (OWA), will receive their email in MS Outlook (Desktop or Mobile) or OWA in clear text. In such a case, they do not have to take any additional step to decrypt the email.

1. View Encrypted email on MS Outlook client

The following image illustrates the display of an encrypted email in the recipient's inbox within MS Outlook on Desktop app. Since the sender in this example is using MS Outlook (Configured with MS Exchange or O365), the recipient does not have to take any additional step to decrypt this email.



JohnDoe123@ntrs.com

JaneSmyth456@outlook.com

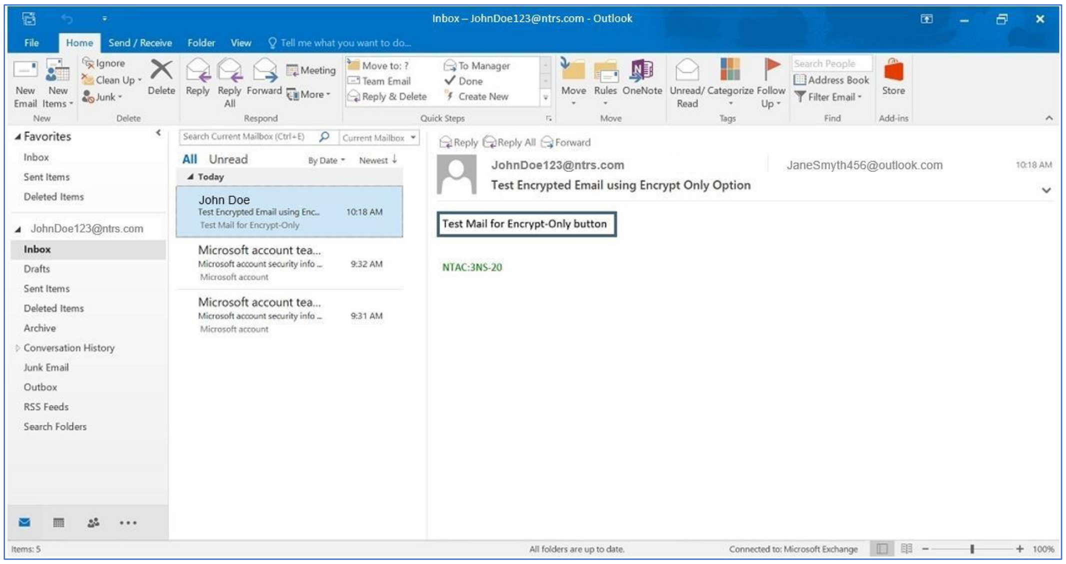
10:18 AM

Test Encrypted Email using Encrypt Only Option

Test Mail for Encrypt-Only button

NTAC:3NS-20

Figure 1 – Encrypted Email viewed in single pane on MS Outlook client



John Doe
Test Encrypted Email using Enc...
Test Mail for Encrypt-Only
10:18 AM

Microsoft account tea...
Microsoft account security info ...
Microsoft account
9:32 AM

Microsoft account tea...
Microsoft account security info ...
Microsoft account
9:31 AM

JohnDoe123@ntrs.com

JaneSmyth456@outlook.com

10:18 AM

Test Encrypted Email using Encrypt Only Option

Test Mail for Encrypt-Only button

NTAC:3NS-20

Items: 5

All folders are up to date.

Connected to: Microsoft Exchange

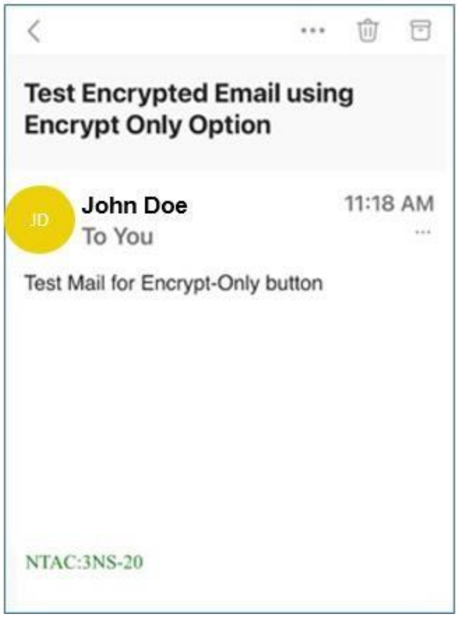
100%

Figure 2 – Encrypted Email viewed in double pane on MS Outlook client

2. View Encrypted email on MS Outlook configured on Mobile Device

The following image illustrates the display of an encrypted email in the recipient's inbox within

MS Outlook app on Mobile Device. Since the sender in this example is using MS Outlook (Configured with MS Exchange or O365), the recipient does not have to take any additional step to decrypt this email.



Test Encrypted Email using Encrypt Only Option

John Doe
To You
11:18 AM

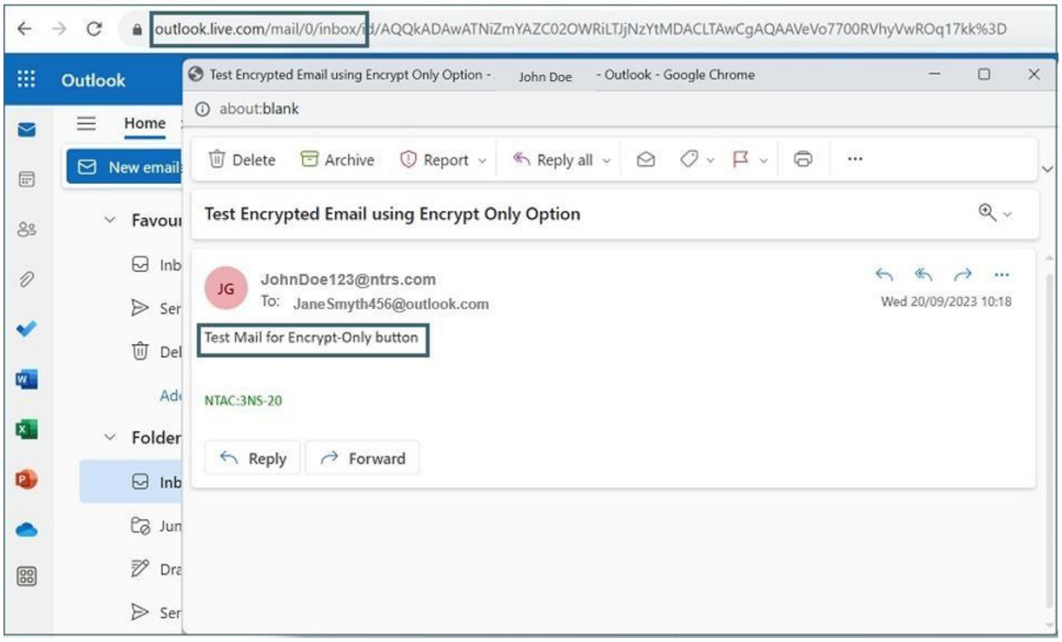
Test Mail for Encrypt-Only button

NTAC:3NS-20

Figure 3 – Encrypted message received on Mobile

3. Encrypted email on Outlook on the Web (OWA)

   The following image illustrates the display of an encrypted email in recipient's inbox within Outlook on the Web (OWA). Since the sender is using OWA in this example, the recipient does not have to take any additional step to decrypt this email.



outlook.live.com/mail/0/inbox/id/AQQkADAwATNiZmYAZC02OWRiLTJjNzYtMDACLTAwCgAQAAVeVo7700RVhyVwROq17kk%3D
Outlook
Test Encrypted Email using Encrypt Only Option - John Doe - Outlook - Google Chrome
about:blank
Home
New email
Favou
Inb
Ser
Del
Ad
Folder
Inb
Jun
Dra
Ser
Delete
Archive
Report
Reply all
Reply
Forward

Test Encrypted Email using Encrypt Only Option

JohnDoe123@ntrs.com
To: JaneSmyth456@outlook.com
Wed 20/09/2023 10:18

Test Mail for Encrypt-Only button

NTAC:3NS-20

Figure 4 – Encrypted message received on OWA

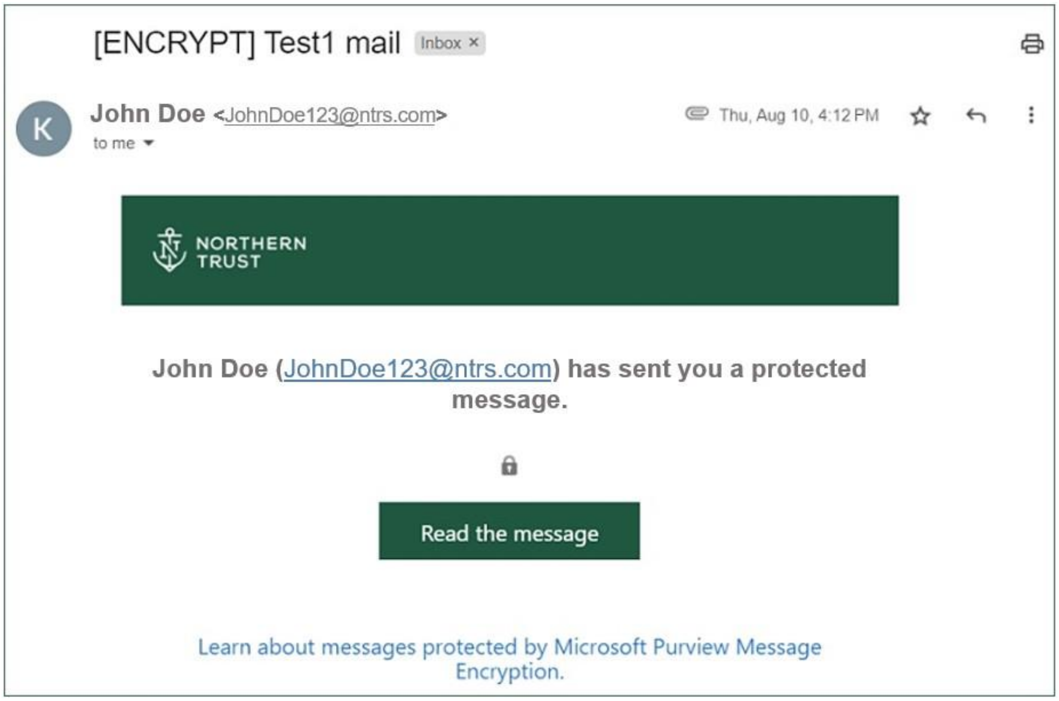
Option 2 – Non-Microsoft 365 Users

Encrypted emails received on external email clients (that are not hosted on Microsoft 365) such as OnPrem Microsoft Exchange, Gmail, and Yahoo, will receive a message in their Inbox informing them about receipt of an encrypted email. In such cases, the recipient will have to take the following steps:

1. Click on "Read the Message" available within the email body. This will take the recipient to the Microsoft 365 portal that will require authentication. Two authentication methods are available:
   a. The recipient may sign-in with their third-party login credentials to access email; or
   b. The recipient may request a "One Time Passcode" (OTP) that will be sent to their email address on file. Such OTPs are valid for 15 minutes.

The following section illustrates the above-mentioned steps:

Step "a" - Image below illustrates the receipt of email within the recipient's inbox informing them about the receipt of an encrypted email. The recipient will have to click on the link "Read the Message" that will take the recipient to OME portal (O365 Message Encryption - https://outlook.office365.com) for authentication.



[ENCRYPT] Test1 mail

John Doe <JohnDoe123@ntrs.com>

to me

Thu, Aug 10, 4:12 PM

John Doe (JohnDoe123@ntrs.com) has sent you a protected message.

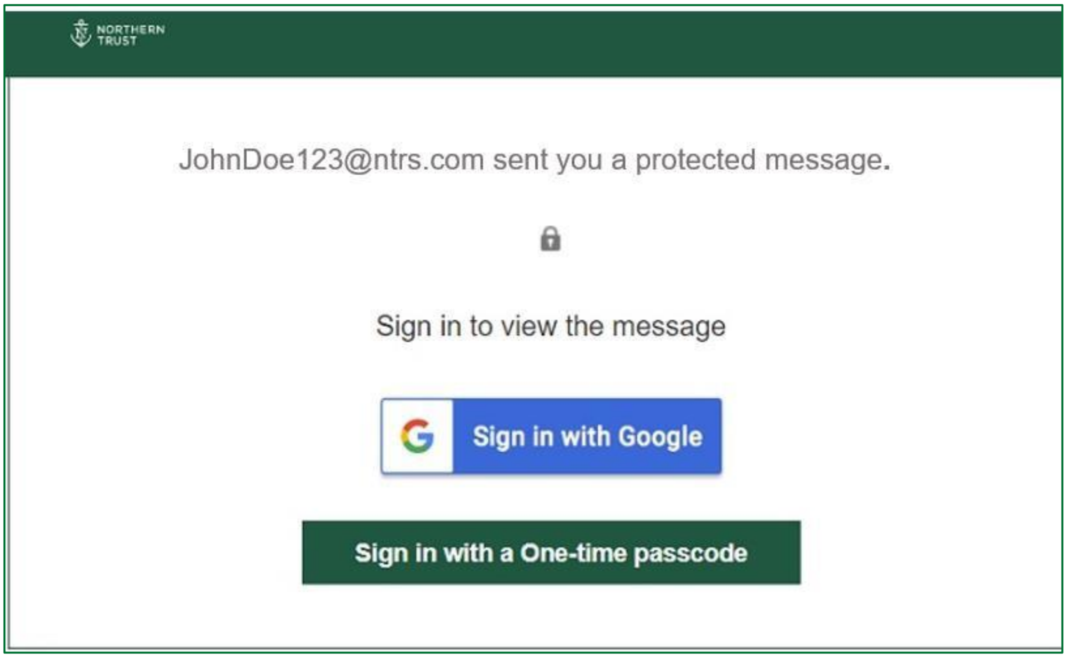
Learn about messages protected by Microsoft Purview Message Encryption.

Figure 5 – Received Secure Email, click to view message

Step "b" – The recipient is presented with two options to view the email.

- Authenticate via email hosting service provider credentials e.g., if the email is sent to “Gmail,” then “Sign in with Google” will appear. If the email is sent to a Yahoo address, then “Sign in with Yahoo” will appear.
- Request a “One Time Passcode” (OTP) that will be sent to the recipient’s email address in an encrypted email.

The following image illustrates the two options mentioned above:



JohnDoe123@ntrs.com sent you a protected message.

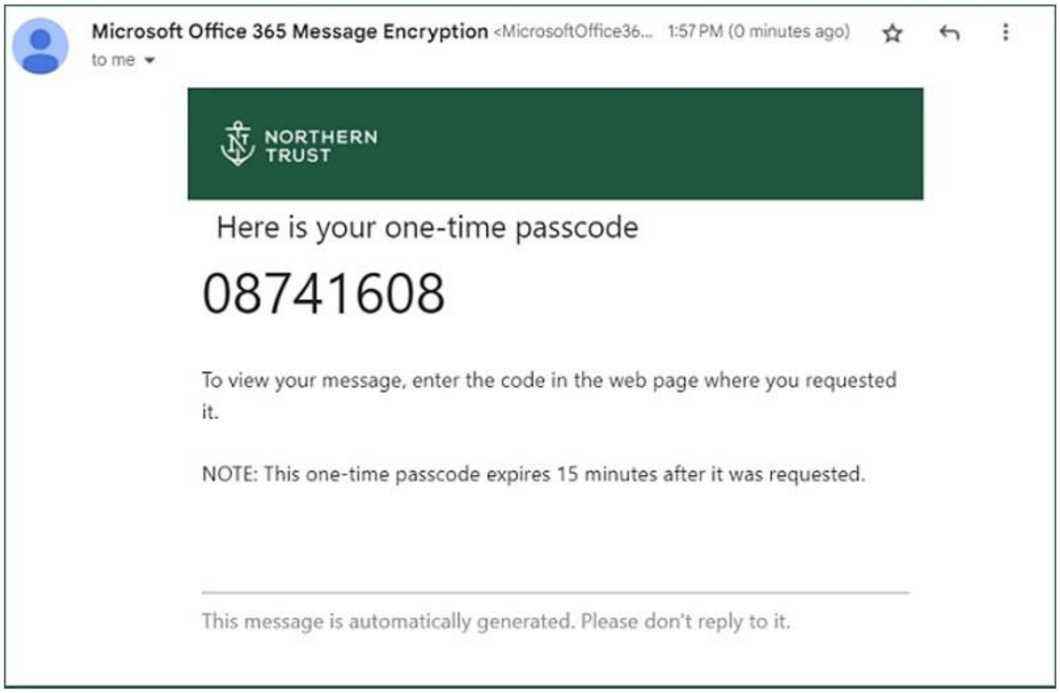
Sign in to view the message

Figure 6 – Sign in with Google Account or One-Time Passcode

Email Service Provider Authentication
When the recipient clicks on “Sign in with Google”, they will either be presented Google Authentication screen or if the recipient is already signed into Google account, email contents will be displayed to the user in clear text.

One Time Password Authentication
If the recipient requests a One-Time Passcode, an email will be sent to the recipient’s email address with the One Time Passcode, which will be valid for 15 minutes.

The following image illustrates the content of email that will be delivered to the recipient’s inbox.



Microsoft Office 365 Message Encryption <MicrosoftOffice36... 1:57 PM (0 minutes ago)

to me

NORTHERN TRUST

Here is your one-time passcode

08741608

To view your message, enter the code in the web page where you requested it.

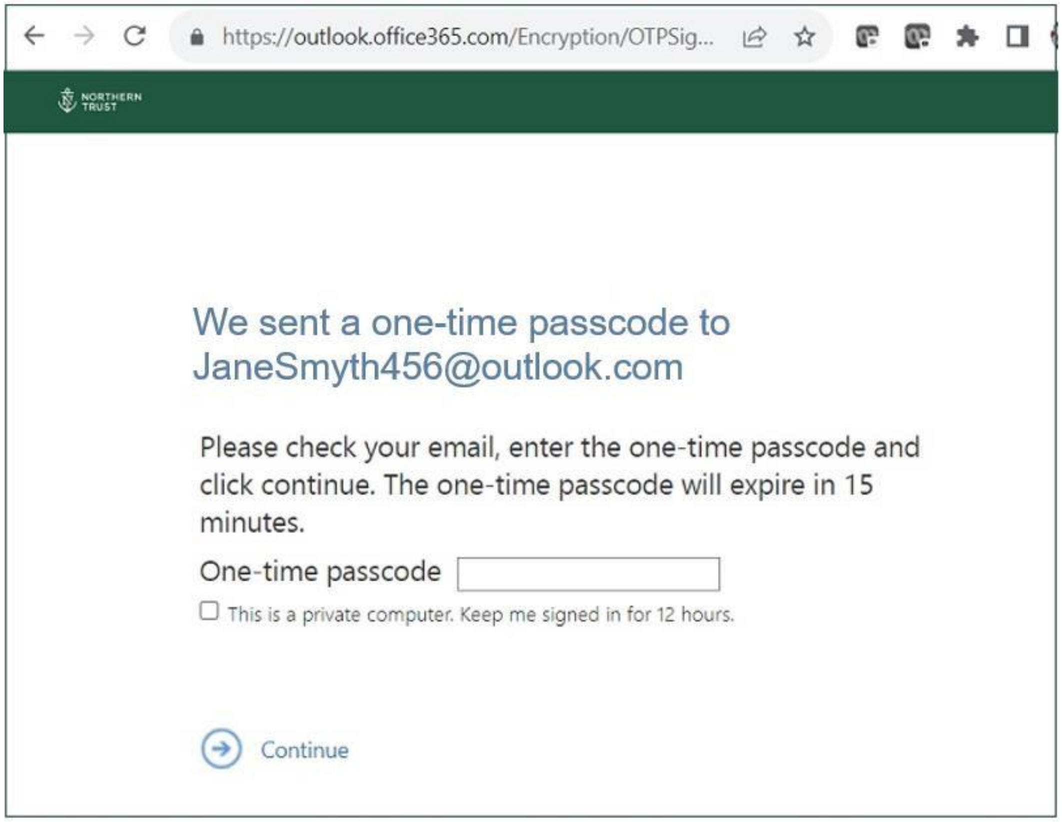
NOTE: This one-time passcode expires 15 minutes after it was requested.

This message is automatically generated. Please don't reply to it.

Figure 7 – One-Time Passcode received as mail in Gmail

Next, the recipient will be required to enter the OPT delivered to their Inbox in the OME portal (O365 Message Encryption **-** https://outlook.office365.com) to access the encrypted email.

The following image illustrates the web page where the recipient will enter the OTP to access this email:



https://outlook.office365.com/Encryption/OTPSig...

We sent a one-time passcode to JaneSmyth456@outlook.com

Please check your email, enter the one-time passcode and click continue. The one-time passcode will expire in 15 minutes.

One-time passcode

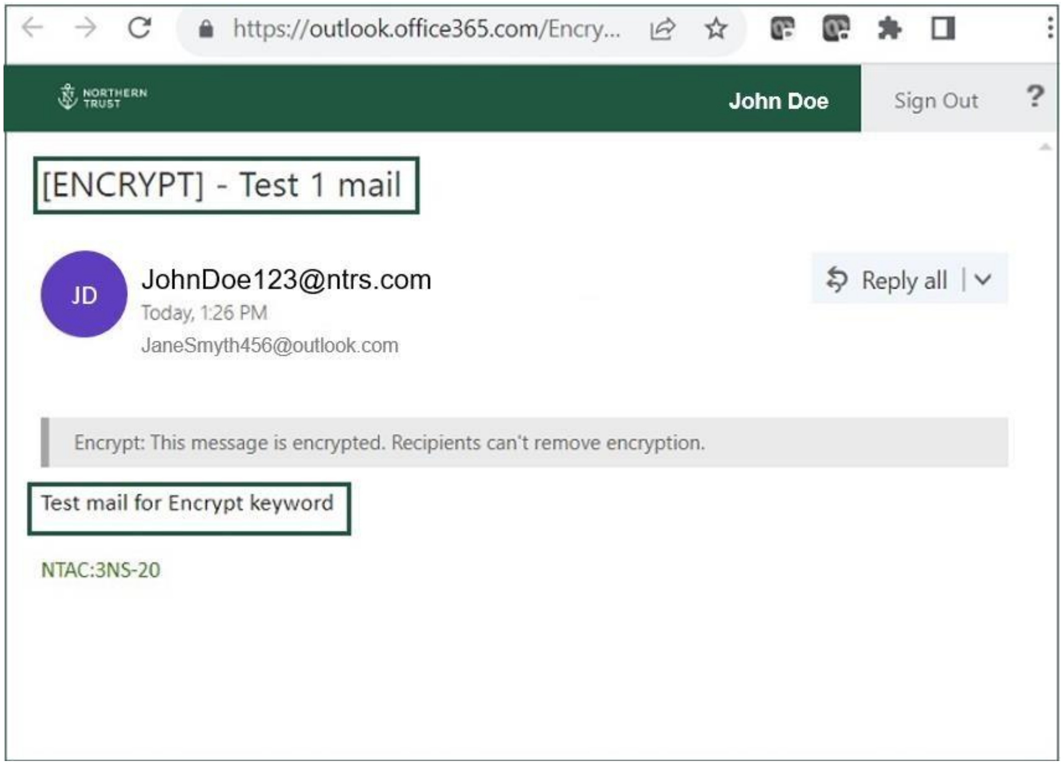
□ This is a private computer. Keep me signed in for 12 hours.

Figure 8 – Enter the One-Time Passcode received on Gmail

Decrypted Email Message

After the recipient is successfully authenticated via their Service Provider authentication or One Time Passcode, the decrypted email message will be displayed within the OME portal (O365 Message Encryption **-** https://outlook.office365.com).

The following image illustrates display of decrypted message within the portal:



[ENCRYPT] - Test 1 mail

JD

JohnDoe123@ntrs.com

Today, 1:26 PM

JaneSmyth456@outlook.com

Encrypt: This message is encrypted. Recipients can't remove encryption.

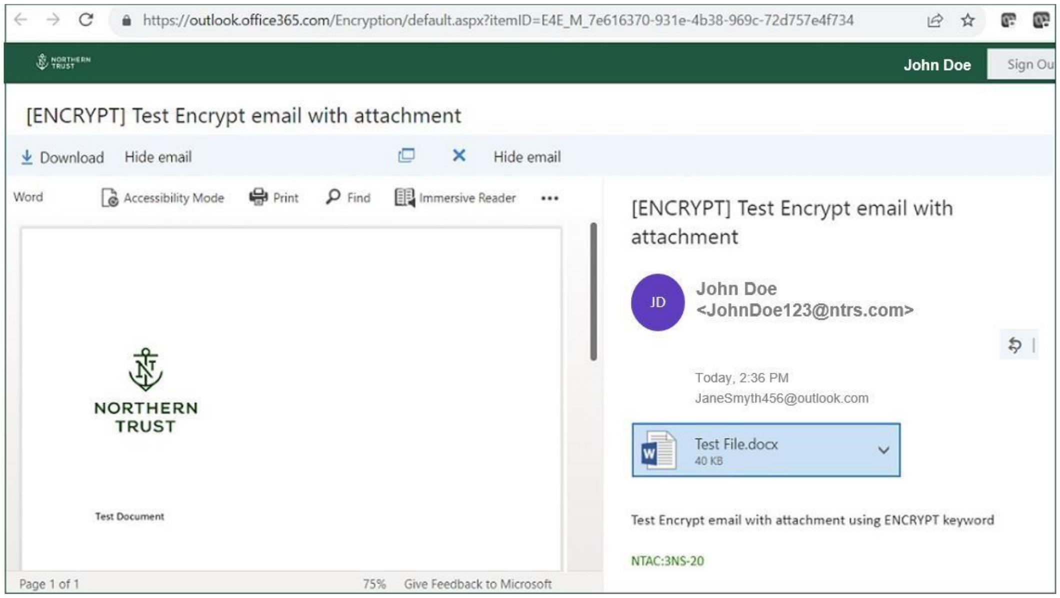
Test mail for Encrypt keyword

NTAC:3NS-20

Figure 9 – Able to view encrypted message after verified with One-Time Passcode

Any attachment in email will also be accessible to the recipient within their portal for viewing or to download.

The following image illustrates the option to view attachments in an encrypted email:



[ENCRYPT] Test Encrypt email with attachment

[ENCRYPT] Test Encrypt email with attachment

JD

John Doe <JohnDoe123@ntrs.com>

Today, 2:36 PM

JaneSmyth456@outlook.com

Test File.docx
40 KB

Test Encrypt email with attachment using ENCRYPT keyword

NTAC:3NS-20

Figure 10 – Able to view encrypted attachment message after verified with One-Time Passcode

Frequently Asked Questions

1. **How does Microsoft Purview Messaging Encryption work?**

   When a Northern Trust Partner sends you a message that matches a rule, encryption is applied automatically. To view encrypted messages, in another email application than Outlook or Outlook on the Web, you will either request get a one-time passcode or sign in using your personal email credentials.

2. **What happens when you encrypt a message?**

   Encryption converts data into a scrambled text, so only the authorized recipient can access and decrypt the message.

3. **Is there an email retention policy?**

   Please note that encrypted e-mails are retained for a period of 90-days (about 3 months) from the day of receipt.

   We recommend downloading any documentation received as an attachment to avoid losing this over time.

4. **What email applications are supported to read and reply to protected emails?**

   Microsoft 365 users can read and respond from Outlook for Windows and Mac (2013 and 2016), Outlook on the web, and Outlook mobile (Android and iOS). You can also use the iOS native mail client if your organization allows it. If you are not a Microsoft 365 user, you can read and reply to encrypted messages on the web through your web browser.

5. **What email applications support encrypt-only protected emails?**

   Microsoft 365 users can use Outlook for PC versions 2019 and Microsoft 365 to create mail protected with the encrypt-only policy. That means messages that have the new encrypt-only policy applied can be read directly in Outlook on the web, in Outlook for iOS and Android, and now Outlook for PC versions 2019 and Microsoft 365.

6. **Is there a size limit for messages you can send with OME (Office 365 Message Encryption)?**

   Yes. The maximum message size you can send with Microsoft Purview Message Encryption, including attachments, is 25 MB.

7. **What type of messages does the encrypted message portal support?**

   The encrypted message portal only supports mail. The portal does not support other message types such as calendar or voice mail.

8. **What file types are supported as attachments in protected emails? Do attachments inherit the protection policies and permissions associated with protected emails?**

   You can attach any file type to a protected mail. Protection policies are applied only to a subset of the file formats mentioned in File types supported by the Azure Information Protection client. Microsoft Purview Message Encryption only supports the following Office files extensions:

   Docx, docm, dotx, dotm, pptx, pptm, potx, potm, ppsx, ppsm, thmx, xlsx, xlsm, xlsb, xltx, xltm, xlam, xps

   Microsoft Purview Message Encryption does not support the 97-2003 versions of the following Office programs: Word (.doc), Excel (.xls), and PowerPoint (.ppt).

9. **Supported recipient type?**

   Email encryption is intended for sending emails to external recipients.

10. **Experience for email recipient?**

    Internal and external recipients receive email in Outlook for Windows, Outlook for Mac, Outlook on the web, Outlook for Android, and Outlook for iOS, or through a web portal, regardless of whether or not they are in the same organization or in any organization. The encrypted message portal requires no separate download.

11. **Are PDF file attachments supported?**

    Encryption allows you to protect sensitive PDF documents attached to emails. When you send an email, the Office 365 service encrypts PDF file attachments for Outlook on the web, Outlook for Mac, Outlook for iOS, and Outlook for Android. You can encrypt PDFs you send without any more steps.

12. **Does the encrypted message portal support preview of encrypted attachments in protected emails?**

    The encrypted message portal supports preview of any encrypted attachment copies added to the encrypted mail. The support file types include Word, Excel, PowerPoint, and PDF files.

13. **Can I send as a shared mailbox and encrypt emails?**

    When someone sends an email message that matches an encryption mail flow rule, the message is encrypted before it's sent.

14. **Can I open encrypted messages sent to a shared mailbox?**

    Yes! You can open encrypted messages for a shared mailbox. When the mail is sent from the same organization, you can open the mail when you're signed into a supported Outlook client. If the mail is sent from an external organization, you need to use Outlook on the web.

    Users can open protected mails in a shared mailbox where the shared mailbox received a protected mail as part of a distribution group.

Users can view attachments that inherit protection from email when they use Outlook for Windows, Outlook for Mac, Outlook for Android, Outlook for iOS, and Outlook on the web.

15. How long do I have access to the mail in the encrypted message portal?

You can sign into the encrypted message portal to retrieve mail as long as the sender's organization is active and the mail hasn't been configured to expire.

16. What about encryption for data at rest?

"Data at rest" refers to data that isn't actively in transit. In Microsoft 365, email data at rest is encrypted using BitLocker Drive Encryption. BitLocker encrypts the hard drives in Microsoft datacenters to provide enhanced protection against unauthorized access.

17. What do I do if I don't receive the one-time pass code after I requested it?

Please check your Junk Email or Quarantine to determine if the message was blocked. If the message is not in either location, please try a different device and request the code again (for example if you are on your phone, please use your computer and try again). If none of these are successful, please coordinate with your email provider to ensure that emails from MicrosoftOffice365@messaging.microsoft.com are allowed to be delivered.

18. I receive a One Time Passcode but the website is not accepting it?

The One Time Passcode is only valid as long as you are on the OTP screen. If you need to leave the OTP screen at any time while you are waiting for the code then the code will reset. Please ensure that you wait for the newest OTP code and enter that code.

19. I logged in “successfully” to the message but it is saying that I do not have permission to read the email. What to do?

This usually indicates a challenge with how the message was sent. Please reach out to your contact indicating that you do not have permissions to the message and ask for the message to be resent.

20. I have Office 365 and I am connecting on my Mac or Windows Outlook client and I am getting errors opening the message?

If you are having challenges accessing the email in your desktop application, please connect to your web email (https://outlook.office.com) and view the email from your browser. The browser will automatically decrypt the message and will allow you to access the email.

21. I am using a Hotmail or Windows Live Account and am not getting the One Time Passcode (OTP) prompt and instead am getting a login screen?

Please login to your Hotmail or Live account and that will replace the need for the OTP. Once you are logged in, please return to the message that previously had the link. When you are connected to the browser, the message will no longer have the link and instead will automatically decrypt the message.

22. I have Gmail and am using the Gmail mobile client on iOS. I am stuck in a loop getting the One Time Passcode because I need to leave the login screen to get the code and then the code resets. How to avoid getting stuck in this loop?

This is a known bug with the Gmail mobile client when using the Safari browser. If prompted, please use an alternate browser for the OTP authentication process. Otherwise, please use an alternate mail app – a browser, your desktop/laptop, or the native iOS mail app – and you will be able to process the OTP properly or use "Sign in with Google" option to access encrypted email.

23. I am clicking on the link for the encrypted email and I am receiving the error "This message might have been moved or deleted". In most cases, I did not receive a login prompt and immediately received this error.

This error appears when you are logged into your browser with an account different from the one that received the email. For example, if you have two Microsoft LiveIDs or two Office 365 email accounts this error can appear if your browser is trying to login with the "other" account. To resolve, please copy the link from the email and try opening it again in an In-Private / Incognito window. You will be prompted to authenticate with the correct account and then receive access to the email.

Further Investigation Required

My question is not listed above, what information can I provide to assist with troubleshooting?

Answer: We apologize for the inconvenience. Please provide the following information to your **Business Relationship Manager** to help troubleshoot:

1) What device are you using (Windows, Mac, iOS, Android)?
2) What application are you using (Outlook app, Chrome, Edge, Safari, Firefox, native iOS mail app, etc)?
3) What step in the process is failing (for example "I can get to the OTP screen but the OTP code is not arriving")?
4) If you are receiving an error, what error are you receiving. If possible, please provide a screen shot of the error.
5) Have you tried using a different device and do you get the same results or is this a device specific error?
6) Please make sure to forward or screen shot the original email as well so we know the sender, recipient, subject and date/time the email was sent.