Northern Trust
Secure Email
User Guide

Version 1.0

Table of Contents

About Northern Trust Secure Email

How Does Encryption Work?

Northern Trust uses a secure method to facilitate e-mail communication called Secure E-Mail. From the evening of April 5, 2024 (9pm CDT onwards) Northern Trust will begin to upgrade its secure email solution to Microsoft Purview Message Encryption (Microsoft Purview). We are targeting completion by the end of June 2024.

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.

* Any reference to client(s) within this guide includes direct clients of Northern Trust but also all parties with whom we communicate e.g. vendors, consultants and the underlying investors of our asset manager clients.

How to Access Encrypted Emails From Northern Trust Using Microsoft Purview Message Encryption

Once Northern Trust is fully transitioned on to Microsoft Purview, 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 the event a client is not using Microsoft 365 email on MS Outlook or Outlook on the Web, clients 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.

The following sections provide additional details on the above two 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

   The following images illustrate the display of an encrypted email in the recipient's inbox within MS Outlook with a single and a double pane view. Since the recipient is using MS Outlook (configured with MS Exchange Online), the recipient does not have to take any additional step to decrypt this email.

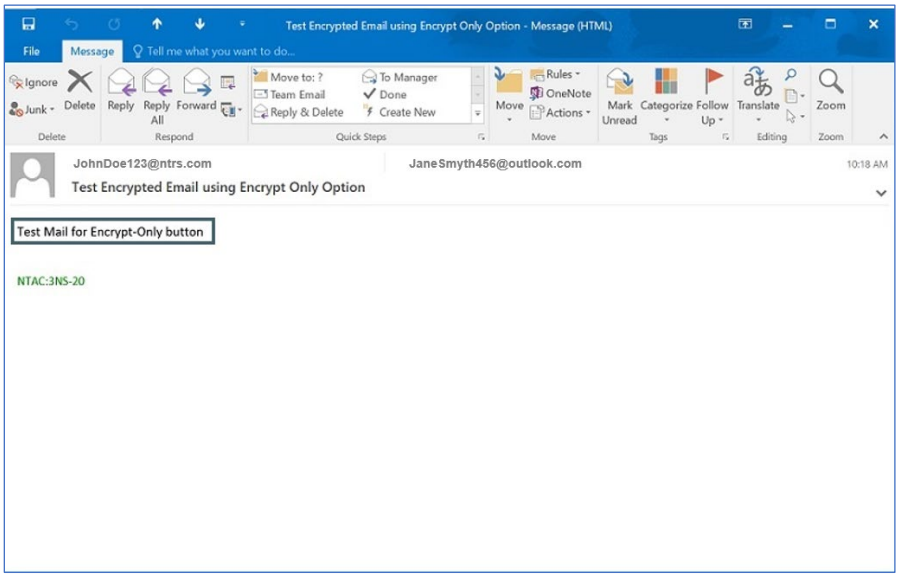

Figure 1 – Encrypted email viewed in single pane on MS Outlook

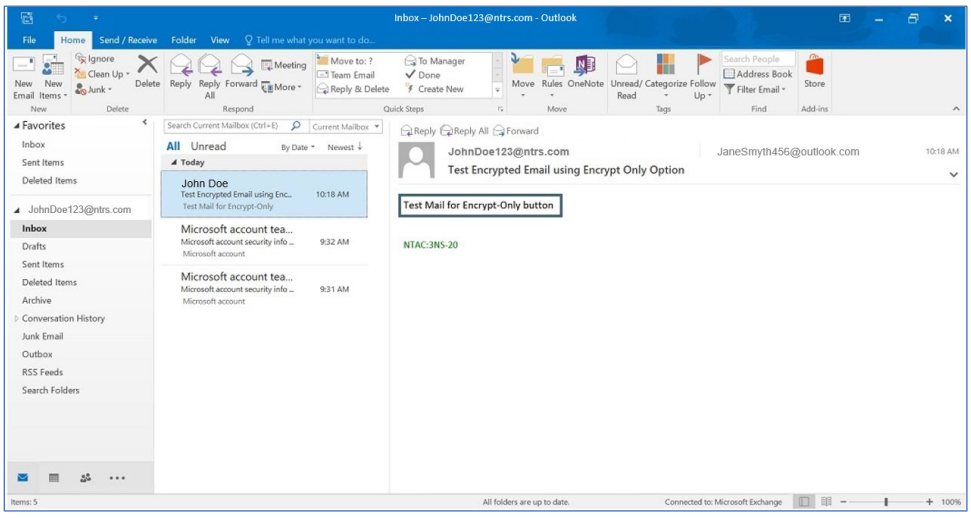

Figure 2 – Encrypted email viewed in double pane on MS Outlook

2. View encrypted email on MS Outlook configured on mobile device

   The below illustrates the display of an encrypted email in the recipient's inbox within the MS Outlook app on a mobile device. Since the recipient in this example is using MS Outlook (configured with MS Exchange Online), the recipient does not have to take any additional step to decrypt this email.

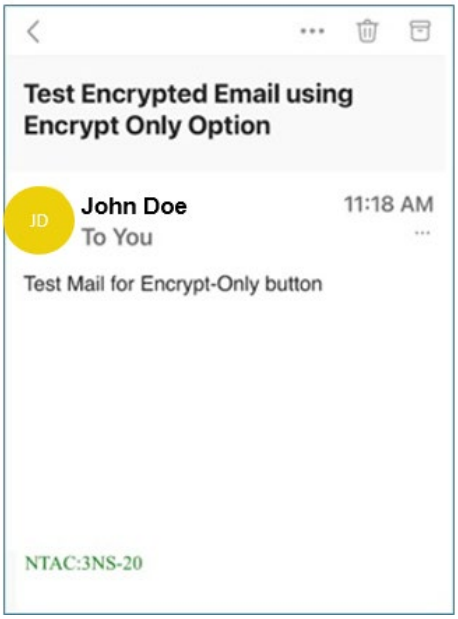

Figure 3 – Encrypted message received on mobile

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

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

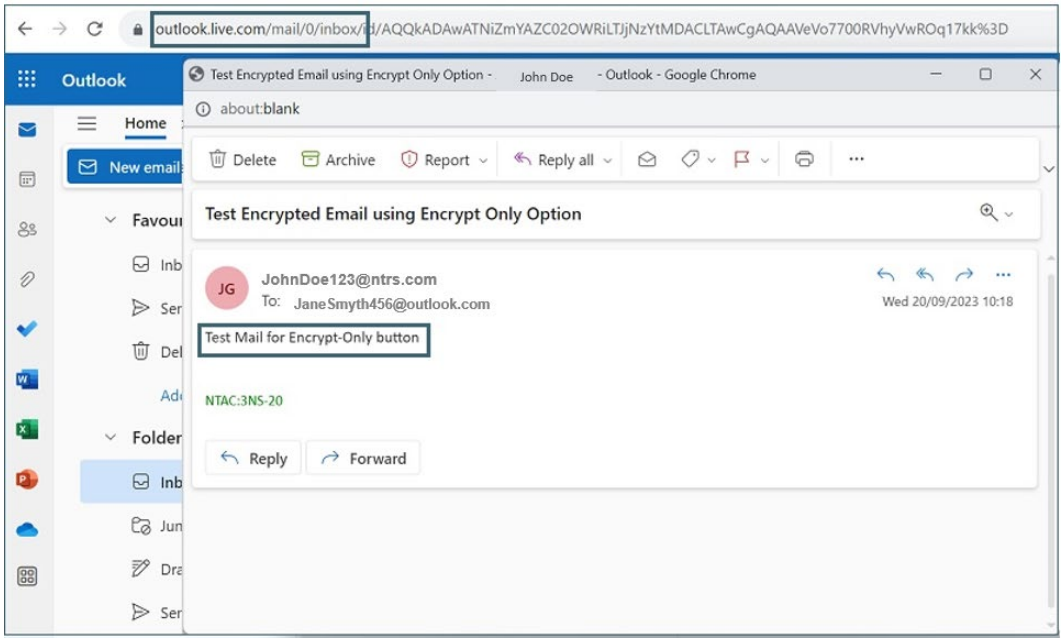

Figure 4 – Encrypted message received on OWA

Option 2 – Non-Microsoft 365 Users

This following is applicable to clients not using Microsoft 365 and instead receiving encrypted emails via other email platforms.

Clients who use email platforms other than Microsoft 365 such as 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. (If the user wants to access an old email that has previously been decrypted they can search for it in their inbox and click on the link to access the secure mail). 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” – The 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 the OME portal (O365 Message Encryption - https://outlook.office365.com) for authentication.

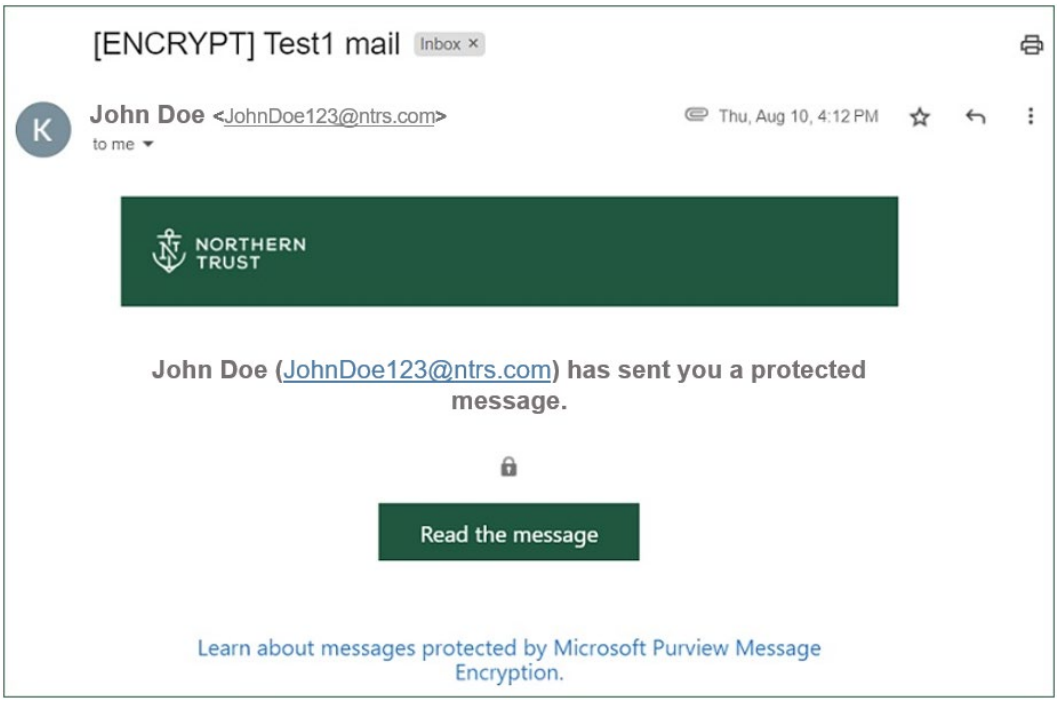

Figure 5 – Received secure email, click to view message

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:

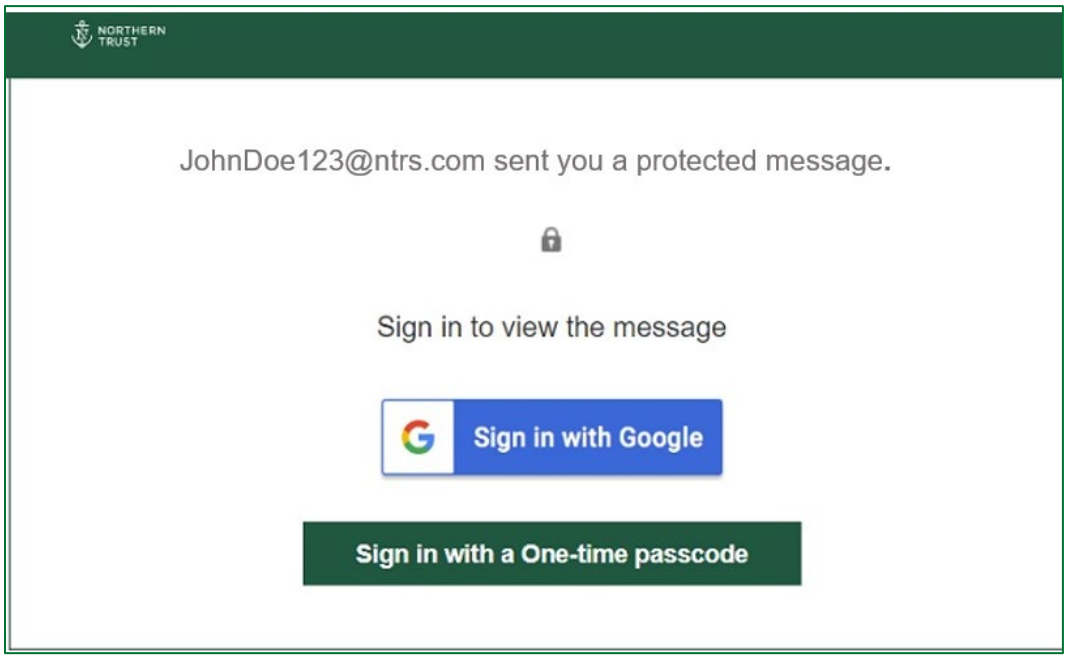

Figure 6 – Sign in with Google Account or One-time passcode

Email Service Provider Authentication

When the recipient clicks on “Sign in with Google”, they will either be presented with a 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 an example email that will be delivered to the recipient's inbox.

Figure 7 – One-time passcode received as mail in Gmail

Next, the recipient will be required to enter the OTP 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:

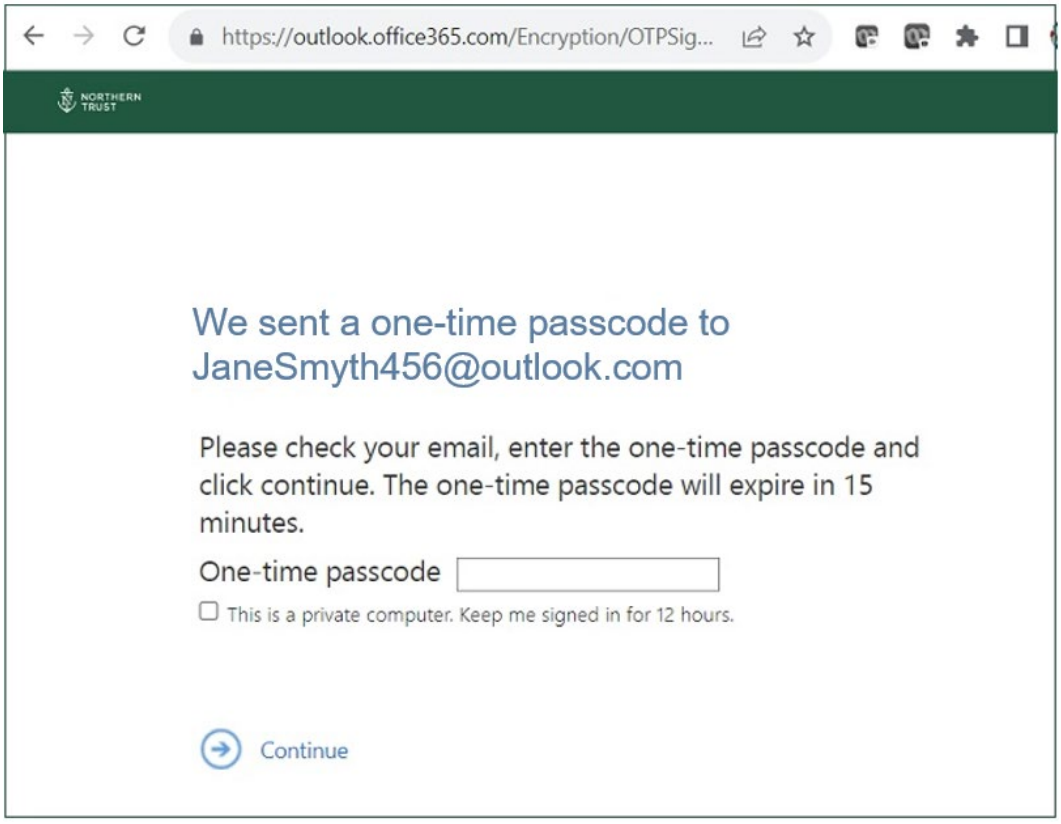

Figure 8 – Enter the One-time passcode received on Gmail

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 the display of a decrypted (readable format) message within the portal:

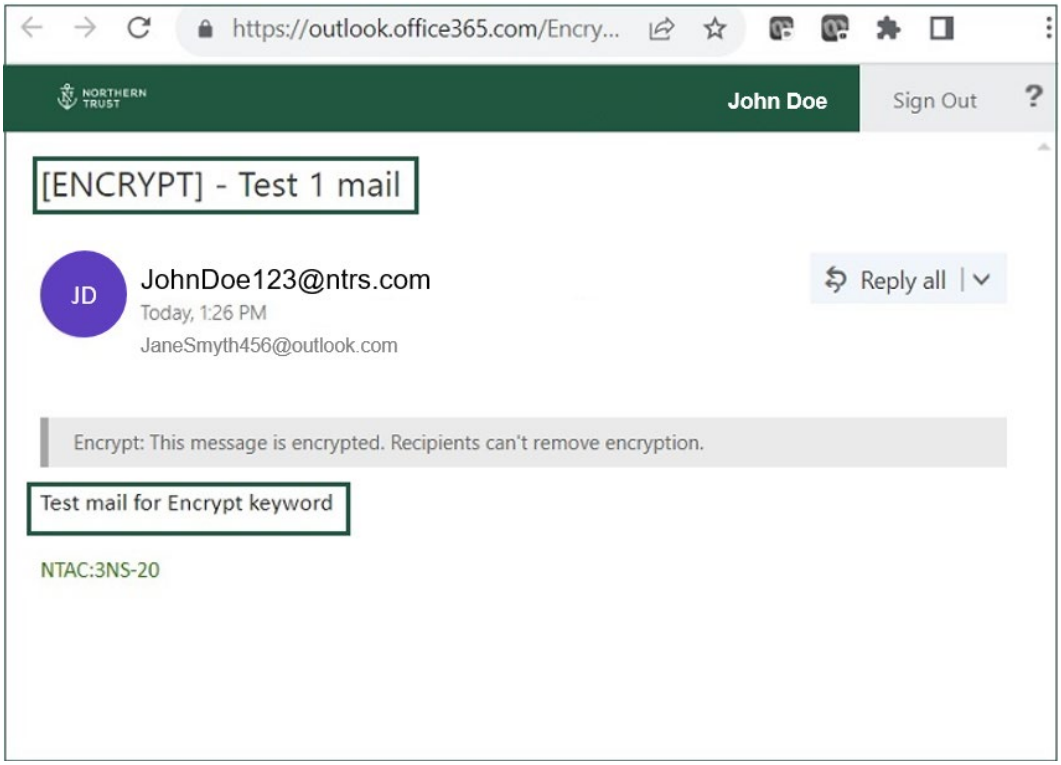

Figure 9 – Able to view encrypted message after verified with one-time passcode

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:

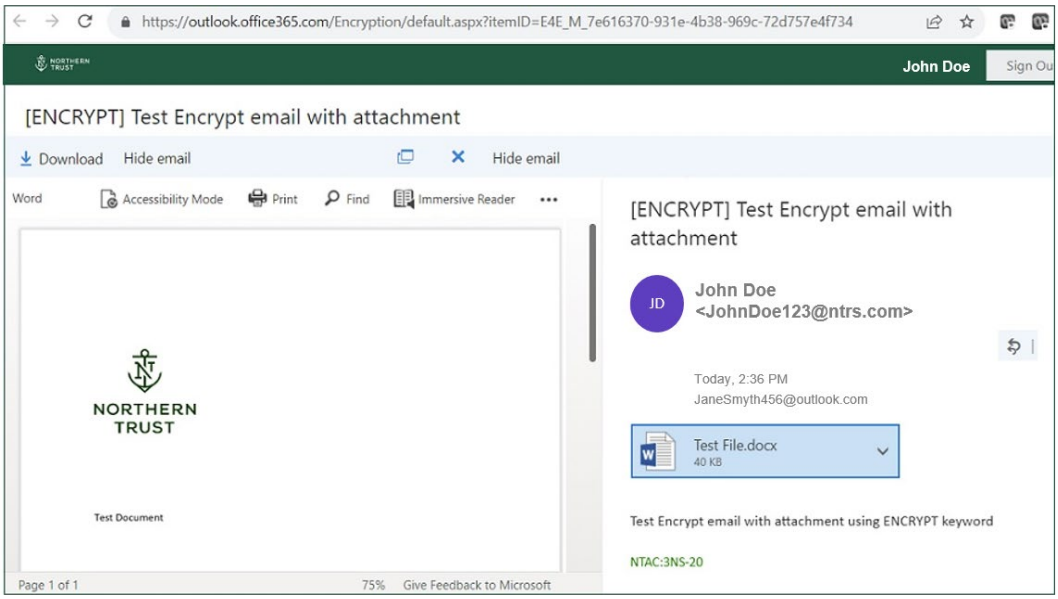

Figure 10 – Able to view encrypted attachment message after verified with One-Time Passcode

Note: if the recipient wishes to access their initial email at a later date, they should search for the original notification email in their inbox that they have an encrypted email waiting for them and click on the link to access the secure mail.

Frequently Asked Questions

1. How does Microsoft Purview Messaging Encryption work?

When a Northern Trust employee sends you a message, content of the email message is secured via encryption. You will receive an email message informing that you have received an encrypted email from Northern Trust that can be accessed by clicking on the link available in the email message. This link will open the Microsoft Portal to view encrypted email. To view encrypted messages, you can either request a one-time passcode or sign in using your personal email credentials within the Microsoft portal.

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 three months) from the day of receipt. We recommend downloading any email and/or documentation received as an attachment to avoid losing this over time. This is consistent with the retention period that was in place prior to Northern Trust transitioning over to Microsoft Purview Message Encryption.

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 application 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 Microsoft. 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. What is the experience for the 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.

10. 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.

11. 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.

12. How long do I have access to an email in the encrypted message portal?

You can sign into the encrypted message portal to retrieve mail within 90-days from initial receipt of the email, after which point the email is no-longer retained.

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

First, check the junk or spam folder in your email.

Next, check quarantine folder, often, messages containing a one-time pass code, especially the first ones your organization receives, end up in quarantine.

14. 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.


NORTHERN
TRUST