ACADEMIC COMPUTING AND NETWORKING SERVICES
COLORADO STATE UNIVERSITY

OFFICE OF TELECOMMUNICATIONS
COLORADO STATE UNIVERSITY

INFORMATION SYSTEMS
COLORADO STATE UNIVERSITY

Encrypt with Microsoft 365 Message Encryption Service

To view the 2021 PDI Session, *Using Microsoft 365 email encryption,* please click here.

IMPORTANT NOTE: Before using the Microsoft email encryption service, you must register for DUO 2-Factor Authentication. Instructions are here, https://www.acns.colostate.edu/duo/, or contact your departmental IT for assistance.

The Microsoft Email Encryption Service allows a user to send encrypted messages and attachments to recipients inside and outside of the University. Email encryption is available **only** through the desktop client and web client. Email encryption is **not** available on mobile devices.

Encryption Options:

There are four email message protection options available.

1. **Encrypt:** Allows you to send encrypted messages to any recipient, whether they are inside the organization or not.
    *   If the recipient is another Microsoft 365 user and using Outlook, Outlook on the Web, or Outlook for mobile, they will be able to open the encrypted e-mail without any additional steps.
    *   If the recipient is outside of Microsoft 365, they will receive an e-mail with a link to the message, which is securely stored on the Microsoft 365 servers. If the recipient is an @gmail address, the recipient will need to sign-in with their Google account credentials. If any of the e-mail service, the recipient will need to sign in with a Microsoft account or one-time access code.
2. **Do Not Forward:** Allows to you send an encrypted message, and restricts the content and email from being forwarded, printed, or copied. *Be aware that with this option, a camera can still be used to capture the contents of the message.*
3. **Colorado State University – Confidential:** Grants read and modify permissions for the protected content - for recipients using CSU Office 365 only.
4. **Colorado State University - Confidential View Only**: Grants read-only permission for the protected content (cannot reply, forward, save, export) - for recipients using CSU Office 365 only.


Encryption Instructions:

How do I encrypt email using Outlook on Windows?

To send encrypted mail using Outlook for Windows, you must be using Outlook 2016 version 1804 or later. To check your version, click on File > Office Account. Under about Outlook, the version number must be at least 1804. If you are not using a supported version of Outlook, please contact your local IT support.

To encrypt a single message using Outlook on a Windows PC:

In an email message, choose Options, select Encrypt and pick the encryption that has the restrictions you want to enforce, such as Encrypt-Only or Do Not Forward.
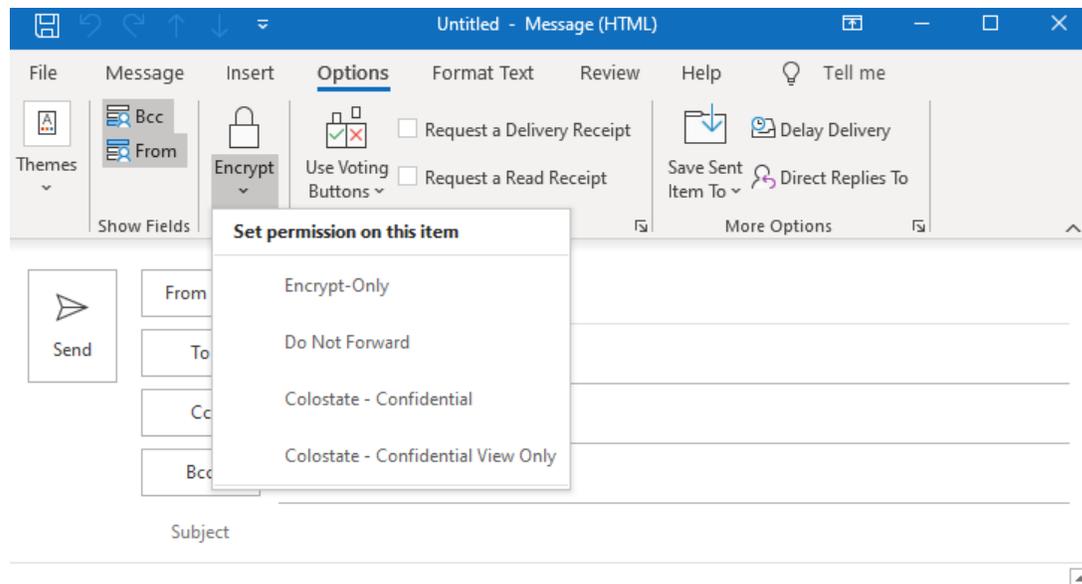

How do I send protected messages using the Office 365 portal?

1. Go to https://portal.office.com and sign in.
2. Click on the Outlook icon to access your email
3. Click "New message" to compose a new email.
4. Click "Encrypt", and then "Change Permissions" to select an encryption option. The "Encrypt" option should suffice in most cases.
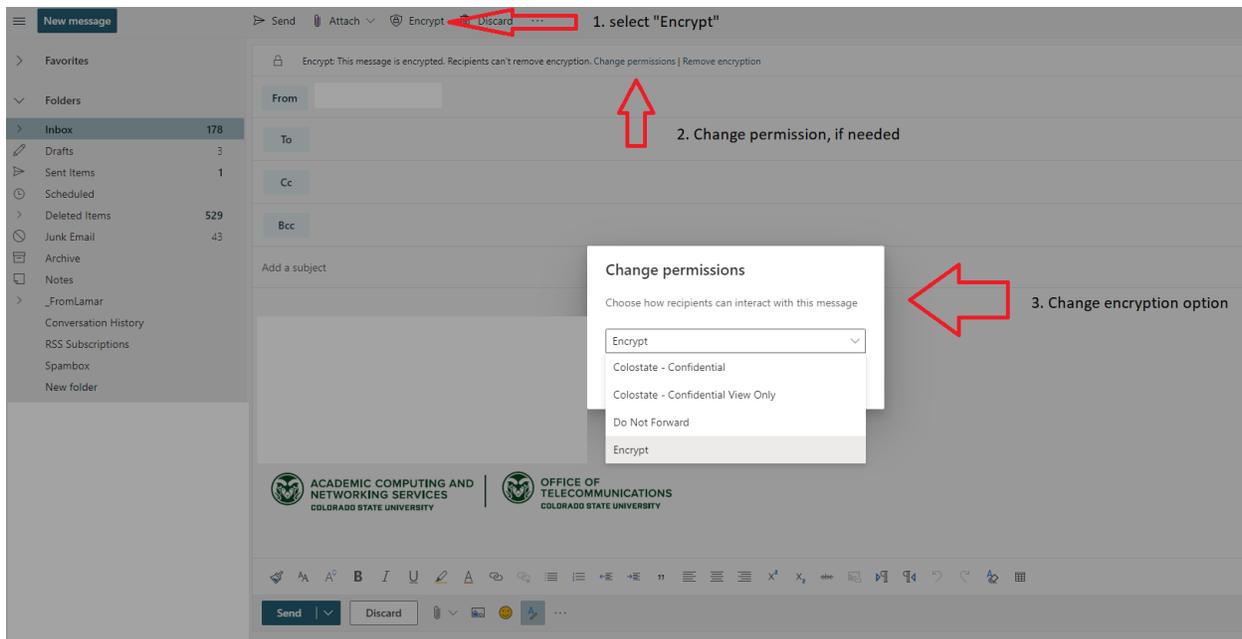
How do I send protected messages using the Office for Mac?

When composing a message, click on the options tab in the ribbon, and click the Permissions button.
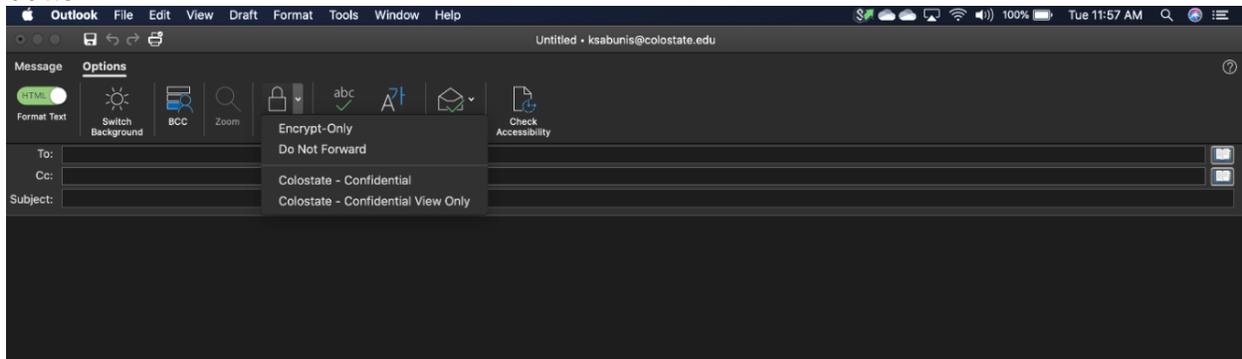
## How do I know a message I receive is protected?

When you receive a protected message, the message in your inbox will likely have a padlock, see red arrow in image below, depending on the client you are using. All client options will display a header at the top of the message that indicates the message is protected, and with the policy it has been protected with, see red arrows in image below.
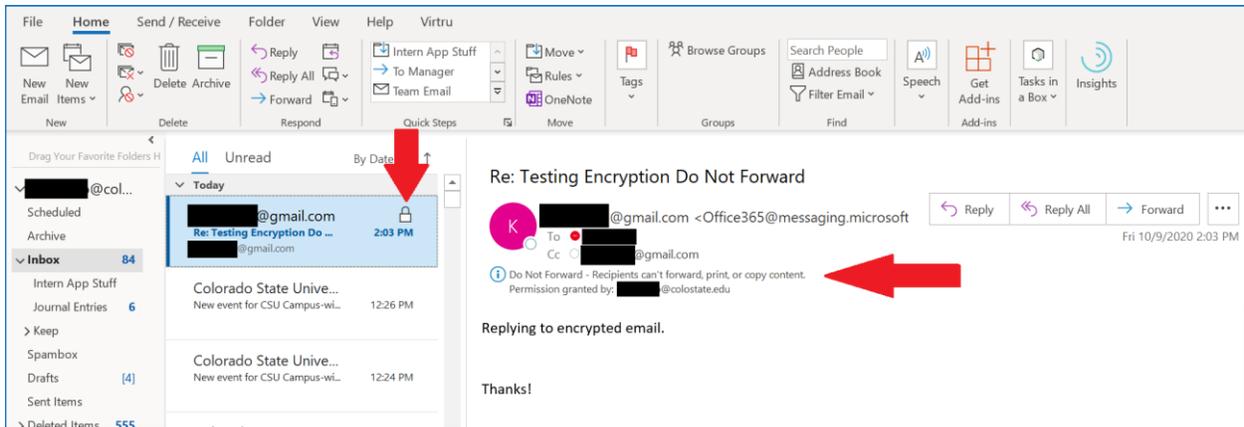
How does an external user open a protected message?

If you send a protected message to an external user, (that is, someone outside of CSU Office 365) they will receive a message from you like normal. The message however will have all the content removed and will only have a link with instructions on how to open the message. They will need to authenticate with a Microsoft account or request a one-time access code. The access code will be e-mailed to the address you sent the original e-mail to. If you sent the message to a @gmail.com or @yahoo.com account, the user can use their Gmail or Yahoo credentials.

The following screenshots demonstrates the process for a gmail account receiving a onetime passcode for an encrypted message from a CSU email.
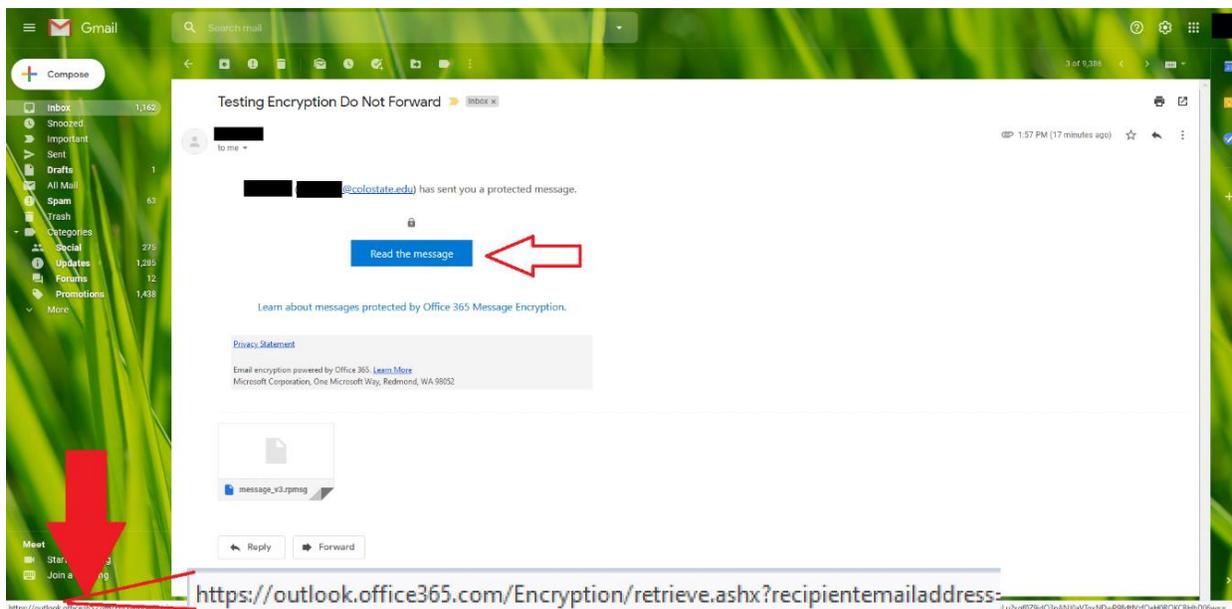
The user can authenticate with a one-time passcode.
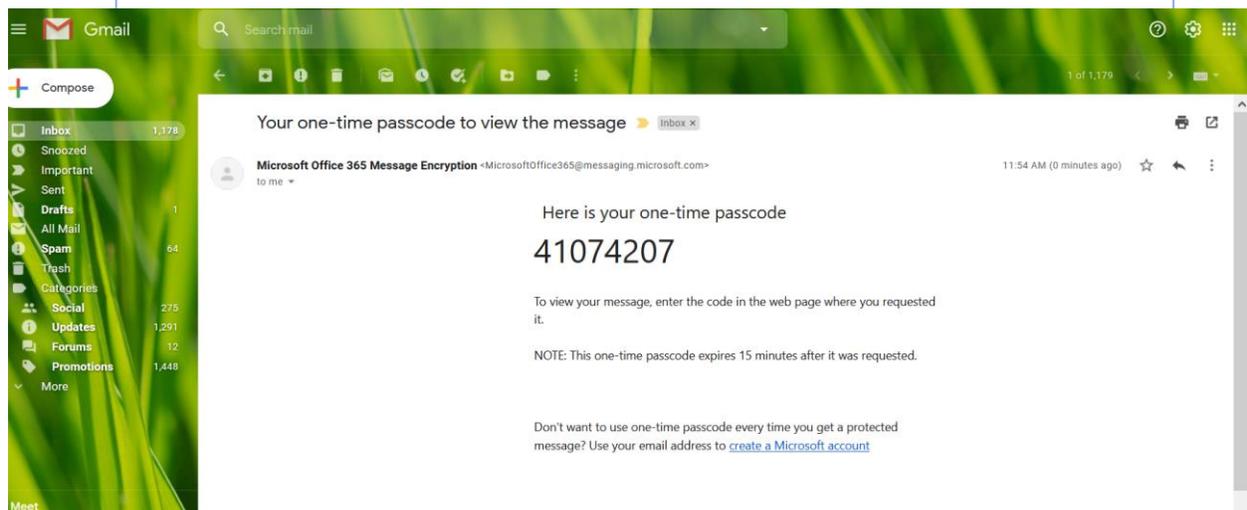
We sent a one-time passcode to ████████@gmail.com.

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.

→ Continue

Didn't receive the one-time passcode? Check your spam folder or get another one-time passcode.

Encrypted Email, notice the grayed box indicates the email is encrypted.

Testing Features

P   ████████████@colostate.edu>   ↩ Reply all | ⌄
     Today, 11:47 AM
     ████████@gmail.com ⌄

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

Stuff and things.

Kind Regards,

██████████

Colorado State University
Academic Computing and Networking Services
Cy███████████rnship Manager
P: 970-491-5190
E:████████@colostate.edu

Do Not Forward Email, notice the forwarding option is grayed out.

Testing Encryption Do Not Forward

P   ████████ < ████████@colostate.edu>   ↩ Reply all | ⌄
     Today, 1:57 PM   Reply
     ████@gmail.com ⌄   Reply all
   Forward
> Do Not Forward: Recipients can't forward, print, or copy content.   Print

Testing Encryption Do Not forward.

Frequently Asked Questions:

1. How do I access email encryption?
   a. You can access Microsoft email encryption through the desktop or cloud versions of Microsoft 365. See above, how to send an encrypted email.

2. Does email encryption work on mobile devices?
   a. The option is not available for mobile devices.

3. Can I encrypt an email to which I am replying?

a. Yes. When using the desktop client, the process is the same as when encrypting the original email. Click reply, select **Options>Encryption**. When using the web client, first reply to the email, then click the on the ellipsis (the 3 dots "...") to the to access the encryption option, see screenshots below.
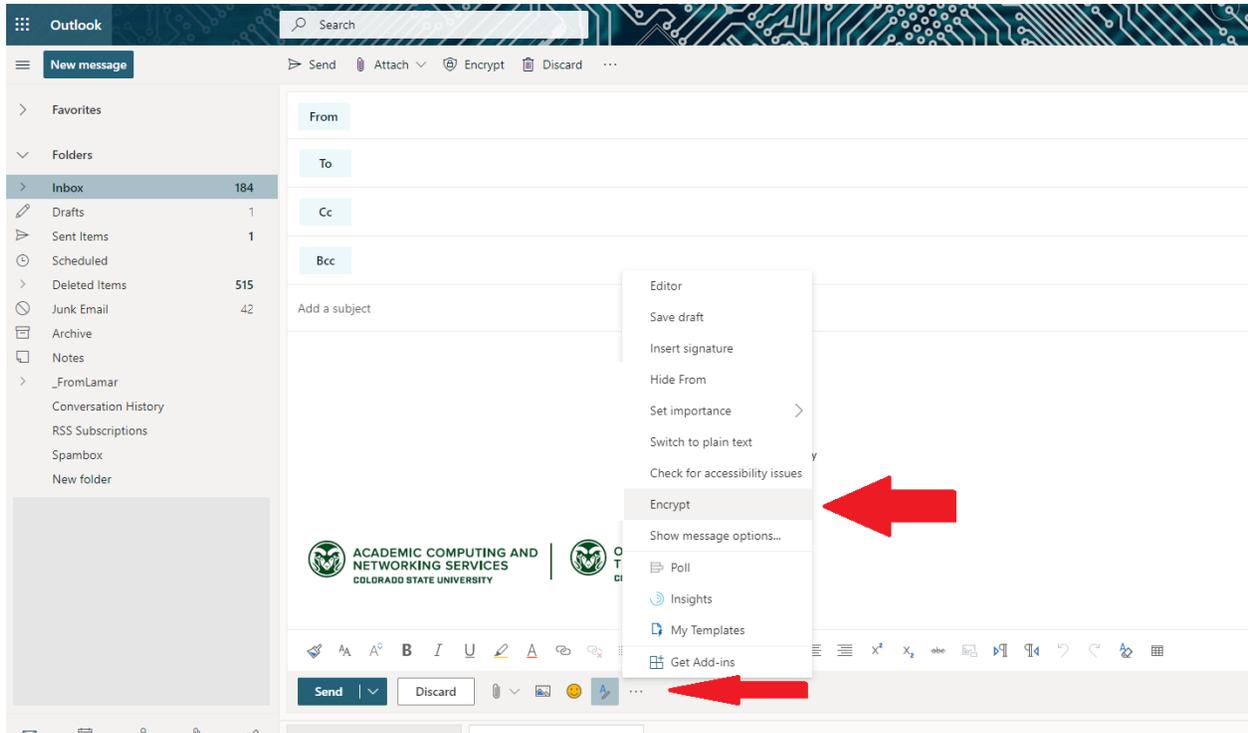
4. Why do I have to register for DUO to use encryption?
   a. DUO is important to verify that you are the owner and user of the devices and applications that you are accessing. This is an essential component to ensure that end to end encryption is taking place, meaning the emails that send are encrypted from the time you invoke encryption until the message is decrypted by the receiver.

5. I received an internal server error after I attempted to authenticate with DUO.
   a. Close Outlook and relaunch the service. You may need to authenticate again. If this did not work, contact your IT liaison.

6. I received a "Connect to rights management servers and get templates" message. See image.
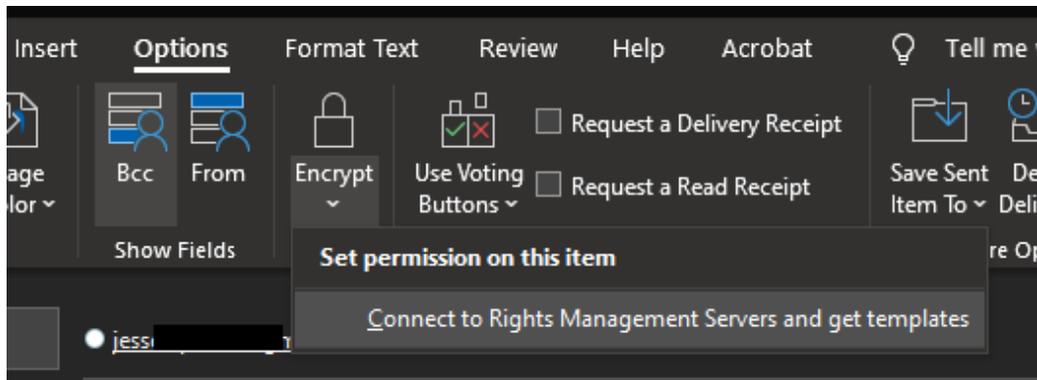
  a. Follow up with your IT liaison.

7. I received any other error message.
  a. Follow up with your IT Liaison.