FCC Information Technology

# Outlook/O365 Tip Sheet

### When and How Encrypt Your Emails in Outlook and Office 365

## The Importance of Email Security

With the rapid globalization of technology, the important of email and network security cannot be understated. At times, it may be necessary to add additional security to an email that may contain sensitive information or that may only be intended for certain recipients. In Outlook and Office 365, this additional levels of security are known as Permissions, and they may easily be applied to any email. By adding a Permission level to your email, you are applying specific criteria about who can open the email and what action they make take with the email. More information about Permissions may be found in the next section.

## Email Permission Levels at the FCC

There are currently five email permissions available at the Commission, each of which is described in detail below.

| Email Permission Level | Description |
|---|---|
| Unrestricted Access (default) | This is the default level of email security. This email is *unencrypted* and does not have any preventative security features. Emails that does not contain any of the sensitive data are safe to send with this permission level. |
| Encrypt - Only | This encrypts your email. Encryption cannot be removed, and the email may only be opened by the intended recipient. |
| Do Not Forward | This permission allows recipients to read this email message, but they may not forward, print, or copy content from the email.<br>***This does not encrypt your email message.*** |
| FCC – Confidential | This level of security allows you to send to recipients within the FCC (i.e. with an @fcc.gov email address). This email contains proprietary information intended for internal users only. This content can be modified but cannot be copied and printed.<br>***This does not encrypt your email message.*** |
| FCC – Confidential View Only | This level of security only allows you to send to recipients within the FCC (i.e. with an @fcc.gov email address). This email contains proprietary information intended for internal users only. This content cannot be modified.<br>***This does not encrypt your email message.*** |

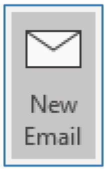
## When to Encrypt Your Emails

The following instances are all scenarios in which encryption of email helps to protect the security of your own information, as well as information relevant to the Commission. When in doubt, it is always good practice to err on the side of caution and encrypt your email.

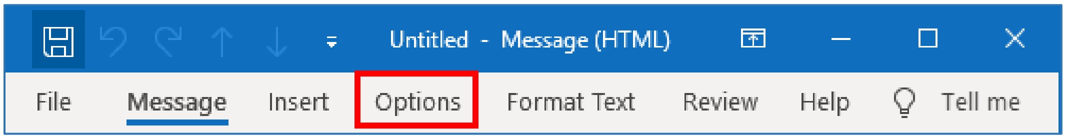
- Sending Personally Identifiable Information (PII), such as social security numbers, etc.
- Sending FCC IP Address(es) or information regarding FCC network architecture
- Sending FCC sensitive data/files
- Sending financial information
- Sending legal messages

## How to Apply Encryption Permissions to Emails in Outlook

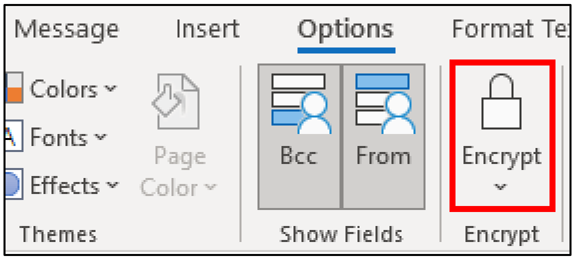
1. Click **New Email** in Outlook to start a new email that you would like to encrypt.



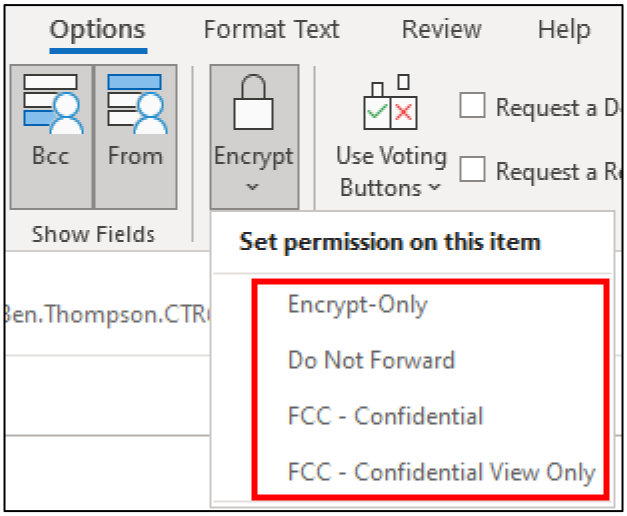
2. In your draft email, click the **Options** tab on the ribbon.



3. On the Options tab, click the **Permissions** button.

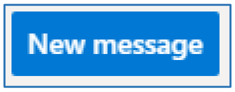


4. Select the level of security that you would like to apply to the email.

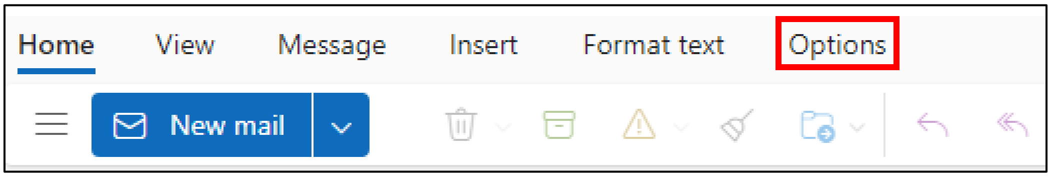


## How to Apply Permissions to Your Emails in Office 365

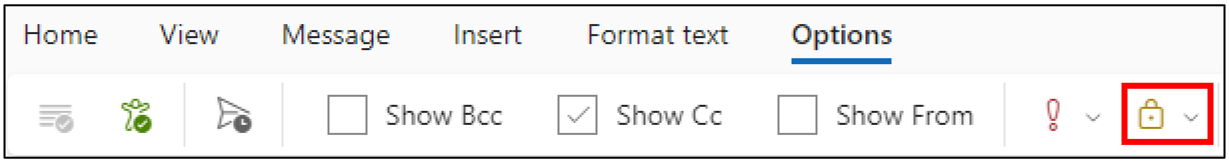
1. In Office 365, click **New Message** to start a new email that you would like to encrypt.



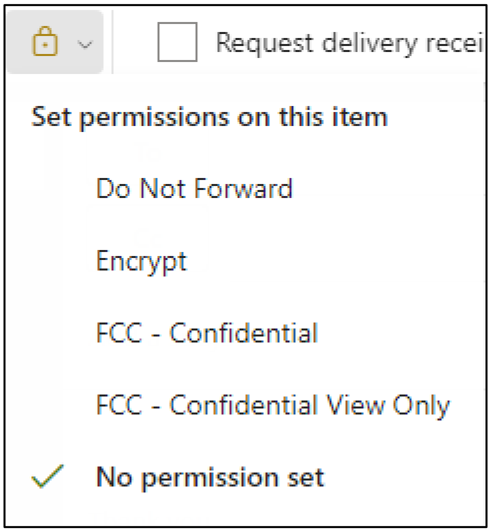
2. On the ribbon that appears above the draft message, select **Options**.



3. On the Options tab, select the **Lock** icon.



4. In the Lock menu, select the level of permissions you wish to apply to your email.


□ Request delivery recei
Set permissions on this item
Do Not Forward
Encrypt
FCC - Confidential
FCC - Confidential View Only
✓ No permission set