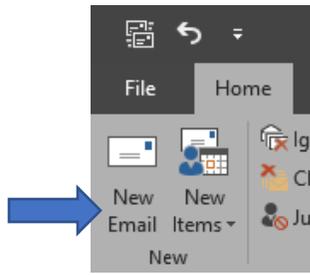


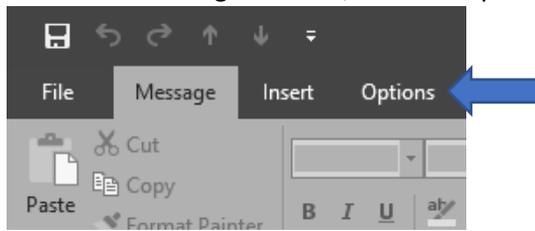
Sending an Encrypted Email Using Outlook

Encrypting an email is a more secure way to send emails containing confidential information. Emails that contain sensitive information, such as Personally Identifiable, health or financial information, should always be encrypted before being sent. In order to encrypt your emails that are sent from the Outlook web portal, you can follow the steps below.

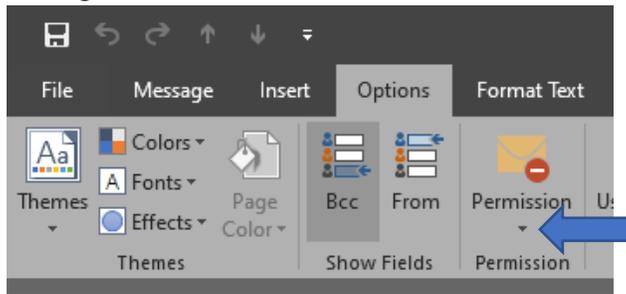
1. In Outlook, click New Email.



2. In the new message window, click the Options tab.



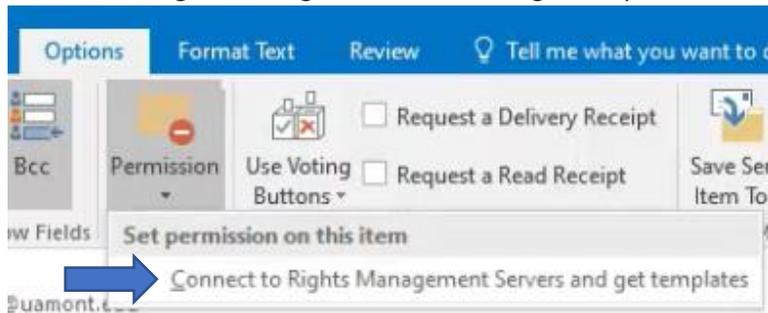
3. If using Office 2019, click the arrow on the Permissions icon.



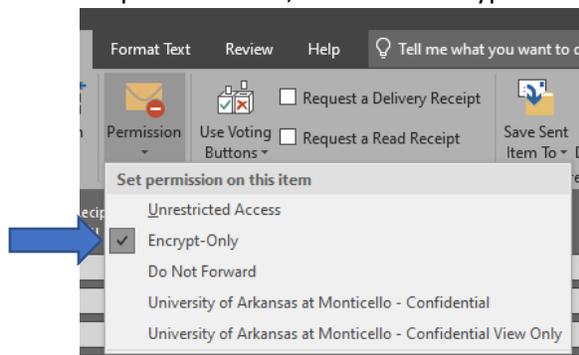
4. If using Microsoft 365 Apps for Enterprise, click on the arrow under the Encrypt icon.



5. If you haven't already, you will need to connect to the Rights Management Server. Click 'Connect to Rights Management Server and get templates' to do so.



6. Click on the arrow under the Permissions (or the Encrypt) icon again, and from the resulting drop-down menu, select the encryption level.



7. Finish composing your email, and click send.

In addition to encrypting an email, you can prevent an email, and any included attachments, from being forwarded by your intended recipient(s) by selecting the 'Do Not Forward' option. By selecting Do Not Forward, your message will be encrypted, and the recipient(s) will be prevented from forwarding the email message to others; they will be able to reply to your email, just not forward it on to others.

If your email contains an attachment, it will be encrypted, too. Microsoft file formats, such as Word and Excel files, will be protected and remain encrypted even if they are downloaded from the email. Non-Microsoft file formats, such as PDF documents and images files, however, will not be protected once downloaded, and will be able to be shared by the recipient.

To enable the Do Not Forward feature, follow the steps outlined above, then choose 'Do Not Forward' in the drop-down.

