Outlook - Email: Digital Signatures

Secure messages by using a digital signature

Digitally sign a single message

1. In the message, on the **Options** tab, in the **Permission** group, click **Sign Message**.
    - If you don't see the **Sign Message** button, do the following:
        - In the message, click **Options**.
        - In the **More Options** group, click the dialog box launcher in the lower-right corner.
        - Click **Security Settings**, and then select the **Add digital signature to this message** check box.
        - Click **OK**, and then click **Close**.
    - If you don't see the **Sign Message** button, you might not have a digital ID configured to digitally sign messages, and you need to do the following to install a digital signature.
        - On the **File** menu, click **Options** > **Trust Center**.
        - Under **Microsoft Outlook Trust Center**, click **Trust Center Settings** > **Email Security**
        - Click **Import/Export** to import a digital ID from a file on your computer, or click **Get digital IDs** to find a list of services that issue digital IDs for your use.
2. Compose your message, and then send it.

Digitally sign all messages

1. On the **File** tab, click **Options** >**Trust Center**.
2. Under **Microsoft Outlook Trust Center**, click **Trust Center Settings**.
3. On the **Email Security** tab, under **Encrypted Mail**, select the **Add digital signature to outgoing messages** check box.
4. If available, you can select one of the following options:
    - If you want recipients who don't have S/MIME security to be able to read the message, select the **Send clear text signed message when sending signed messages** check box. By default, this check box is selected.
    - To verify that your digitally signed message was received unaltered by the intended recipients, select the **Request S/MIME receipt for all S/MIME signed messages** check box. You can request notification telling you who opened the message and when it was opened, When you send a message that uses an S/MIME return receipt request, this verification information is returned as a message sent to your **Inbox**.
5. To change additional settings, such as choosing between multiple certificates to use, click **Settings**.
6. Click **OK** on each open dialog box.

Verify the digital signature on a signed email message

When someone checks your identification to make sure that you are who you say that you are, it’s important that they match the identification photo with your face. Similarly, when you receive a message in Microsoft Outlook that contains a digital signature, it’s important to verify that the signer is who you think that the person is.

1. Open the digitally signed message.
2. Look at the **Signed By** status line to check the email address of the person who signed the message. It isn’t enough to check the email address in the **From** line — you want to verify who actually signed the message, not only who sent the message.

   Important: If the email address in the **From** line doesn’t match the email address in the **Signed By** status line, the **Signed by** line is the one that you should use to determine who actually sent the message.
3. To check whether the signature is valid, click 🎖 on the **Signed By** status line. Then, to see more information about the digital signature, click **Details**.

   Notes:

   - If a digital signature isn’t valid, there can be many causes. For example, the sender's certificate may have expired, it may have been revoked by the certificate authority (CA), or the server that verifies the certificate might be unavailable. Notify the message sender of the problem.
   - If a delegate sent the message on behalf of another person, then the delegate's name is listed as the sender.

Encrypt email messages

When you need to protect the privacy of an email message, encrypt it. Encrypting an email message in Outlook means it's converted from readable plain text into scrambled cipher text. Only the recipient who has the private key that matches the public key used to encrypt the message can decipher the message for reading. Any recipient without the corresponding private key, however, sees indecipherable text. Outlook supports two encryption options:

1. **S/MIME encryption** - To use S/MIME encryption, the sender and recipient must have a mail application that supports the S/MIME standard. Outlook supports the S/MIME standard
2. **Microsoft 365 Message Encryption** (Information Rights Management) - To use Microsoft 365 Message Encryption, the sender must have Microsoft 365 Message Encryption, which is included in the Office 365 Enterprise E3 license.

New Encrypt button and updates to email encryption

With the new Office update, email encryption in Outlook got better.

- The **Permissions** button

is replaced with the **Encrypt** button

.
- The new Encrypt button contains both encryption options (S/MIME and IRM). The S/MIME option is only visible if you have S/MIME certificate configured in Outlook.

Encrypting with S/MIME

Before you start this procedure, you must first have added a certificate to the keychain on your computer. Once you have your signing certificate set up on your computer, you'll need to configure it in Outlook.

1. Under the **File** menu, select **Options** > **Trust Center** > **Trust Center Settings**.
2. In the left pane, select **Email Security**.
3. Under **Encrypted email**, choose Settings.
4. Under **Certificates and Algorithms**, click **Choose** and select the **S/MIME certificate**.
5. Choose OK
6. If you are an Office Insider with Microsoft 365 subscription, here's what is new to you:

In an email message, choose **Options**, select **Encrypt** and pick **Encrypt with S/MIME** option from the drop down,

You'll see an **Encrypt with S/MIME** if you have an S/MIME certificate installed on your computer.

For **Outlook 2019 and Outlook 2016**,

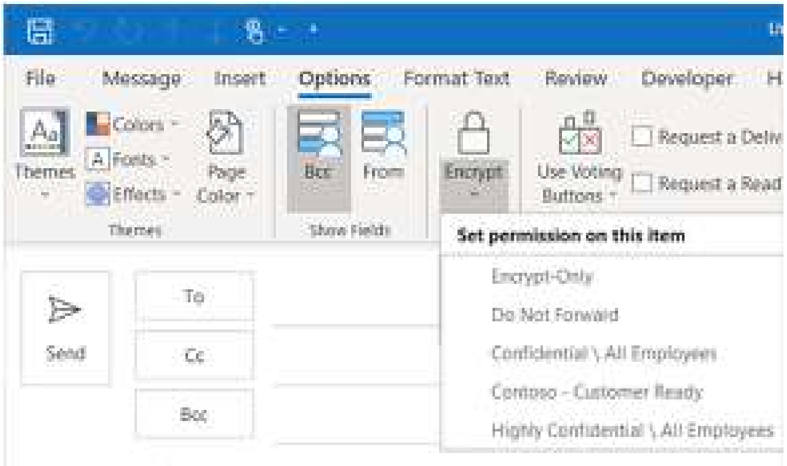
In an email message, choose **Options**, select **Permissions**.

7. Finish composing your email and then choose **Send**.

Encrypt with Microsoft 365 Message Encryption

- If you are a Microsoft 365 subscriber, here is what is new to you:

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**.



Outlook - Email: Digital Signatures

Note: Microsoft 365 Message Encryption is part of the Office 365 Enterprise E3 license. Additionally, the Encrypt-Only feature (the option under the Encrypt button) is only enabled for subscribers (Microsoft 365 Apps for enterprise users) that also use Exchange Online.

- **For Outlook 2019 and 2016**,

In an email message, select **Options** > **Permissions** and pick the encryption option that has the restrictions you'd like to enforce, such as Do Not Forward.

Encrypt a single message

1. In message that you are composing, click **File** > **Properties**.
2. Click **Security Settings**, and then select the **Encrypt message contents and attachments** check box.
3. Compose your message, and then click **Send**.

Encrypt all outgoing messages

When you choose to encrypt all outgoing messages by default, you can write and send messages the same as with any other messages, but all potential recipients must have your digital ID to decode or view your messages.

1. On the **File** tab. choose **Options** >**Trust Center** > **Trust Center Settings**.
2. On the **Email Security** tab, under **Encrypted email**, select the **Encrypt contents and attachments for outgoing messages** check box.
3. To change additional settings, such as choosing a specific certificate to use, click **Settings**.

For more information, please refer to the Microsoft training resource page HERE