

How to Encrypt Emails in Outlook For Secure Communication

TechRounder PDF Edition

Live article: <https://www.techrounder.com/how-to/how-to-encrypt-emails-in-outlook-for-secure-communication/>

By Vipin PG | Published March 29, 2025 | Updated March 29, 2025 | Format: Guide | 4 min read

Quick answer

Email security is more important than ever, especially when it comes to protecting personal or business-sensitive information. For users of Microsoft Outlook, encryption is a built-in feature that helps keep your messages safe from unauthorized access, both while they're in transit and at rest.

Email security is more important than ever, especially when it comes to protecting personal or business-sensitive information. For users of Microsoft Outlook, encryption is a built-in feature that helps keep your messages safe from unauthorized access, both while they're in transit and at rest. In this article, we'll break down everything you need to know about encrypting emails in Outlook, including how it works, the available encryption types, setup instructions, and practical tips for secure usage.

What is Email Encryption in Outlook?

Email encryption is a process that transforms readable content (known as plaintext) into coded text (called ciphertext). Only the intended recipient with the proper access or decryption key can view the original message. This ensures your data remains confidential and protected from cyber threats. In Outlook, encryption plays an important role in:

- Preventing unauthorized access
- Securing data during transmission
- Meeting compliance regulations
- Reducing the risk of data breaches

How Email Encryption Works

When you send an encrypted email in Outlook:

- The message is transformed using cryptographic algorithms.
- It remains encrypted both while being sent and after arriving in the recipient's inbox.
- Only recipients with the right permissions or tools can decrypt and read it.
- In some cases, replies in the email thread will also remain encrypted.

Available Email Encryption Methods in Outlook

Outlook provides multiple encryption options based on your account type and organization settings. Below are the most commonly used:

1. S/MIME Encryption (Secure/Multipurpose Internet Mail Extensions)

- Requires a digital certificate (digital ID) for both sender and recipient.
- Offers end-to-end encryption and the option to digitally sign emails.
- Commonly used in enterprise environments.

- Supports improve security by verifying sender identity.

2. Microsoft Purview Message Encryption (Previously Office 365 Message Encryption)

- Integrated with Microsoft 365 for eligible subscriptions.
- Does not require additional software.
- Encrypted messages can be accessed by recipients without Outlook or Microsoft accounts using one-time passcodes.
- Allows restrictions such as "Do Not Forward."

Levels of Encryption Protection

Outlook gives users control over how much protection an email message should have. Here are the common protection levels:

Protection Type: Encrypt-Only | Description: Encrypts content and attachments; replies stay encrypted.

Protection Type: Do Not Forward | Description: Adds encryption and blocks forwarding, printing, or copying.

Protection Type: Custom Rules (Org-Specific) | Description: Used by organizations to limit sharing or access within internal users.

Requirements Before You Start

Depending on the encryption type, you may need:

- A Microsoft 365 subscription (for Purview encryption).
- A digital certificate from a Certificate Authority (for S/MIME).
- Proper configuration through Outlook settings or IT admin support.

Account Type: Work/School (M365) | Supports Encryption: ? | Digital Signature: ? | IRM (Rights Management): ? | Sensitivity Labels: ?

Account Type: Personal (M365) | Supports Encryption: ? | Digital Signature: ? | IRM (Rights Management): ? | Sensitivity Labels: ?

Account Type: Free Outlook/Personal Email | Supports Encryption: ? | Digital Signature: ? | IRM (Rights Management): ? | Sensitivity Labels: ?

How to Encrypt Emails in Outlook

For Individual Emails

? In New Outlook Interface:

1. Create a new message.
2. Go to the Options tab.
3. Click Encrypt.
4. Choose either Encrypt-Only or Do Not Forward.
5. Compose and send your email.

? In Classic Outlook Interface:

1. Start a new email.
2. In the ribbon, select Options > Permissions > Encrypt.
3. Select the encryption type.
4. Send your email.

To Encrypt All Outgoing Emails Automatically

? New Outlook:

- Go to Settings > Mail > S/MIME.
- Enable Encrypt contents and attachments for all messages I send.

? Classic Outlook:

- Navigate to File > Options > Trust Center > Trust Center Settings > Email Security.
- Tick the box for Encrypt contents and attachments for outgoing messages.

Setting Up S/MIME Encryption

If you opt for S/MIME, follow these steps:

Step 1: Get a Digital Certificate

- Obtain it from a Certificate Authority (e.g., Comodo, DigiCert) or your IT team.

Step 2: Install and Configure

- In Outlook, go to:
 - File > Options > Trust Center > Trust Center Settings > Email Security
 - Import your certificate under Import/Export
 - Under Settings, choose your certificate for signing and encryption

How Recipients View Encrypted Messages

The recipient's experience depends on how they're accessing your email:

Recipient Type: Same Organization (Outlook) | How They View It: Can open directly without extra steps

Recipient Type: External (with Microsoft 365) | How They View It: Can open in Outlook apps/web without issues

Recipient Type: External (Other Email Providers) | How They View It: Will receive a link to view the message securely after verification

For those outside your organization, the recipient can verify their identity via:

- Microsoft/Google login
- One-time passcode sent to their email

Troubleshooting Common Issues

Issue: Rights Management not available | Solution: Ensure M365 plan supports encryption; check admin settings

Issue: Certificate errors | Solution: Reinstall or renew the certificate; validate the date and trust

Issue: Recipient can't open message | Solution: Provide instructions or use Microsoft Purview for better compatibility

Issue: Missing features in new Outlook | Solution: Switch to classic Outlook temporarily or contact IT for activation

Email Encryption Best Practices

? Security Tips

- Use strong passwords and enable 2FA.
- Double-check recipient addresses to avoid sending sensitive data to the wrong contact.

- Secure your digital certificate with a password and store it safely.

? For Organizations

- Define clear encryption policies for sensitive communications.
- Educate employees on how and when to use encryption.
- Regularly audit encryption usage and update certificates.
- Consider alternative secure communication methods for file transfers like OneDrive, SharePoint, or secure messaging platforms.

Conclusion

Email encryption in Outlook is a powerful feature that adds an extra layer of protection to your communication. Whether you're securing internal business messages or sharing sensitive personal information, understanding how encryption works and using it consistently helps ensure data confidentiality and compliance. From S/MIME to Microsoft Purview encryption, Outlook offers tools that suit both enterprise and individual needs. As cyber threats grow more advanced, enabling and managing encryption is no longer optional, it's essential.