

Contents

What is Email Encryption?	1
Why encrypt?	1
How does an email get encrypted?	2
What if the SecureEmail button is missing?	2
Can I send attachments?	2
What does the recipient see?	2
What if the recipient does not receive my email?	2
What if the recipient is getting a "System Unavailable" error?	2
How do I know if an email I sent was encrypted, received, or read?	2
What happens if the recipient's organization strips HTML attachments?	3
Is there a way to encrypt meeting requests with sensitive documents attached?	3
Can a Mobile Device receive, open, and reply to encrypted email?	3
Who can access or monitor encrypted emails?	3
What happens if I send an encrypted email to the wrong email address?	3
Can I send encrypted email to listserv lists?	3
What support does Cisco provide for email encryption?	3

What is Email Encryption?

An encrypted email allows only the sender and receiver to read the email and attachments. Direct replies to encrypted emails are also encrypted. DOR uses Cisco's Registered Envelope Service (CRES).

Why should I encrypt email?

Regular email is sent as clear text that can potentially compromise privacy if intercepted. By comparison, encrypted email is secure and only users on the system can send and receive secure messages and attachments. This means that the sender and recipient can communicate about private information while following state and federal privacy laws.

How do I send an encrypted email?

You have two options:

1. Using the **SecureEmail** button in Outlook. This button works like an on/off switch. Click once to encrypt mail; click a second time to turn it off. When **[Send Secure]** is at the start of the Subject line it means encryption is turned on.
2. Manually typing **[Send Secure]**, including the square brackets, as the first thing in the email subject line. This also will work with email sent through Outlook Web Access (OWA).

Note: Please refer to [Secure Encrypted Email](#) for complete instructions

What if the SecureEmail button is missing?

As a first step, try closing and reopening Outlook. If the button is still missing and you need to send an email, manually type **[Send Secure]** in the Subject line, as mentioned above. Then contact the [Service Desk](#) (608-266-8653) to let them know the button is gone.

Can I send attachments?

Yes, attachments as large as 15MB can be included in your encrypted email. Some email systems may reject a message it considers too large. If you have multiple large attachments, you may want to send them in separate messages, or by a different route (Globalscape, mailing a Flash Drive, etc.).

What does the recipient see?

The recipient gets a secure email message with instructions on how to open the email. The instructions will take the recipient through the steps to register (the first time) and open the encrypted email.

To better understand the recipient's experience and to assist them with questions, please review the document [Secure Encrypted Email](#) found on DORIS. If you have additional questions, please contact the Service Desk (608-266-8653).

What if the recipient does not receive my email?

Double-check that you have the correct email address for the recipient. If so, advise them to check the **Junk Email** folder for your email. If they are part of an organization, they can ask their IT or Security team to see if the email is being **Quarantined**.

If they still can't find the email, you can ask if they have a different email address that you can use instead.

What if the recipient is getting a "System Unavailable" error?

First, double-check that they are saving the HTML attachment before trying to open it, as instructed in [Cisco's Recipient Guide](#). If it still isn't working, they can **Forward** the email to mobile@res.cisco.com which will provide them with a login link instead of using the attachment.

If it still doesn't work, they will need to contact [Cisco Support](#) for further assistance.

How do I know if an email I sent was encrypted, received, or read?

You can go to your Sent Mail to look for your message. Encrypted email will have **[Send Secure]** in the Subject line. Additionally, encrypted messages generate a "read receipt" when the recipient opens the initial email that contains the link to the email. The "read receipt" confirms that the email was received, but not that the encrypted content was read.

What happens if the recipient's organization strips HTML attachments?

The recipient will need to contact their organization's support or [Cisco Support](#) for further assistance.

Is there a way to encrypt meeting requests with sensitive documents attached?

Meeting requests in Outlook do not have the "SecureEmail" button on the toolbar so you will need to manually type **[Send Secure]** at the beginning of the Subject line.

Can a Mobile Device receive, open, and reply to encrypted email?

Yes, a mobile device can send a secure message, but you will need to manually type **[Send Secure]** at the beginning of the Subject line. You can open a secure message on a mobile device by forwarding the encrypted email to mobile@res.cisco.com. You'll then receive a new email with a link that you can use to log in.

Who can access or monitor encrypted emails?

In addition to the specified recipients, DOR Security teams monitor encrypted email and can access them if there is a security breach.

What happens if I send an encrypted email to the wrong email address?

Contact the Service Desk immediately to have the message blocked. Provide them with:

1. Your name and email address.
2. The recipient's email address.
3. The Subject line of the email.
4. The Date and Time that the email was sent.

Even if the email has been read by the recipient, further access can be blocked.

Can I send encrypted email to listserv lists?

No. The list members would be instructed to go to CRES to open the message, and they would not be able to open the encrypted email because their email address would not be listed in the **To:** field.

What support does Cisco provide for email encryption?

1. Cisco's Secure Email Encryption Recipient Guide:
https://www.cisco.com/c/en/us/td/docs/security/email_encryption/CRES/recipient_guide/b_Recipient/b_Recipient_chapter_011.html
2. Cisco's 24/7 Email and Web Chat Support: <https://res.cisco.com/websafe/help?topic=ContactSupport>