

Secure Email



TABLE OF CONTENTS

LEGAL REQUIREMENTS.....	2
TLS (Transport Layer Security).....	3
SENDING AN ENCRYPTED E-MAIL.....	4
READING AN ENCRYPTED E-MAIL	5
SAVING E-MAILS	9
SAVING ATTACHMENTS.....	9
READING BCC E-MAILS	10
ADDING EXTERNAL DOCUMENTS TO EMERGE.....	12
INFORMED CONSENT	13

LEGAL REQUIREMENTS

The WCB has an obligation to ensure that the information it collects is kept confidential and secure. This obligation stems from *The Workers Compensation Act (WCA)*, *The Freedom of Information and Protection of Privacy Act (FIPPA)* and *The Personal Health Information Act (PHIA)*.

All WCB employees sign a Pledge of Confidentiality when they commence their employment and are expected to adhere to the WCB's policies regarding confidentiality and e-mail.

The WCA states that information obtained by WCB employees in the course of their work must be kept confidential. Both FIPPA and PHIA also set out rules to protect individuals against the unauthorized use and disclosure of their personal information and personal health information. The WCB, as both a public body and trustee, is required to make reasonable security arrangements and implement safeguards to ensure that personal information and personal health information is protected. The rules in FIPPA and PHIA apply when information is shared by e-mail or other networked systems such as the Internet.

PHIA also specifically requires trustees, such as the WCB, to implement procedures to prevent the interception of information when it is being shared via electronic means.

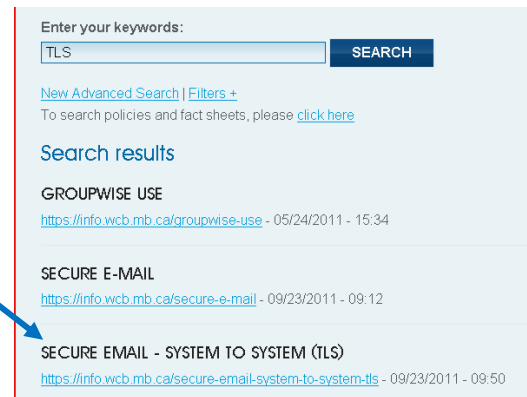
Secure E-Mail and TLS enabled e-mail are the procedures used by the WCB to ensure that personal information and personal health information is being transmitted in a secure manner.

TLS (Transport Layer Security)

TLS is a secure e-mail solution that provides encryption of e-mails between e-mail systems. If an organization is TLS enabled, any e-mails you send to that organization are automatically encrypted without having to use the Send Secure button.

A list of organizations that are TLS enabled is available on the WCB Intranet.

Enter TLS in the search field at the top of any intranet page; click the Search Button or press Enter; select the link under the heading *Secure E-mail - System to System (TLS)* from the search results.



Adding Other Organizations to the List

If you receive an e-mail with the following message at the bottom, it means the originating organization is TLS enabled:

"This message was received over a secure connection using TLS."

If the organization is not on our list, forward the e-mail to HelpDesk and ask them to add it to the TLS list on the Intranet. The more up-to-date the list, the less staff will need to use Send Secure.

Establishing New TLS Enabled Contacts

If an organization expresses interest in an alternative method for communicating securely, suggest they look into using TLS. The organization's IT department would need to investigate whether their computer systems have the capability.

SENDING AN ENCRYPTED E-MAIL

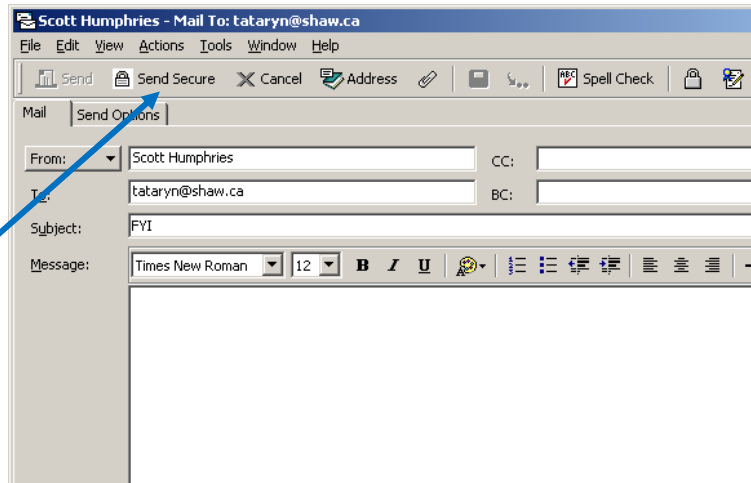
Sending an encrypted e-mail is as simple as clicking the **Send Secure** button; however, you should first advise the recipient that you will be sending an encrypted e-mail and provide them with the **External Encrypted E-Mail Instructions** document to assist them in completing a registration process. This document is located in *U:\General\Secure E-mail*.

After you have advised the recipient of your intent, create your e-mail as usual in GroupWise.

Attach any documents you want to include.

Click the **Send Secure** button.

Our e-mail system will encrypt the e-mail and any attached files.



When the recipient opens your E-mail, a message similar to the one below will indicate the E-mail is secure and provide instructions for reading it.

To: tataryn@shaw.ca

Attachments: [securedoc.html](#)

You have received a secure message

Read your secure message by opening the attachment, [securedoc.html](#). You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser. To access from a mobile device, forward this message to mobile@res.cisco.com to receive a mobile login URL.

If you have concerns about the validity of this message, contact the sender directly.

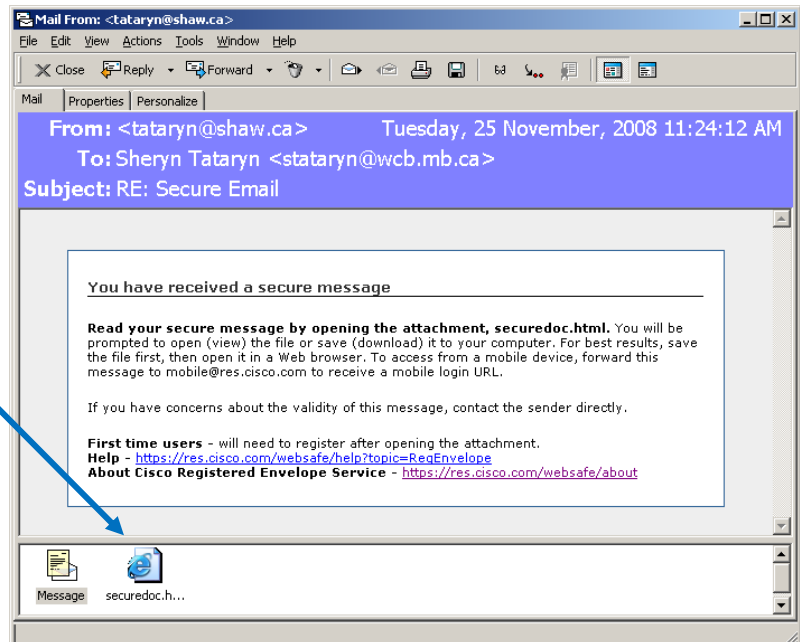
First time users - will need to register after opening the attachment.
Help - <https://res.cisco.com/websafe/help?topic=RegEnvelope>
About Cisco Registered Email Service - <https://res.cisco.com/websafe/about>

READING AN ENCRYPTED E-MAIL

If the recipient of an encrypted e-mail chooses to reply back to you, the reply will be encrypted and you will need to go through the registration process in order to read their reply. Once registered, you will be able to open future encrypted e-mails just by entering your password.

When you receive a Secure e-mail do the following:

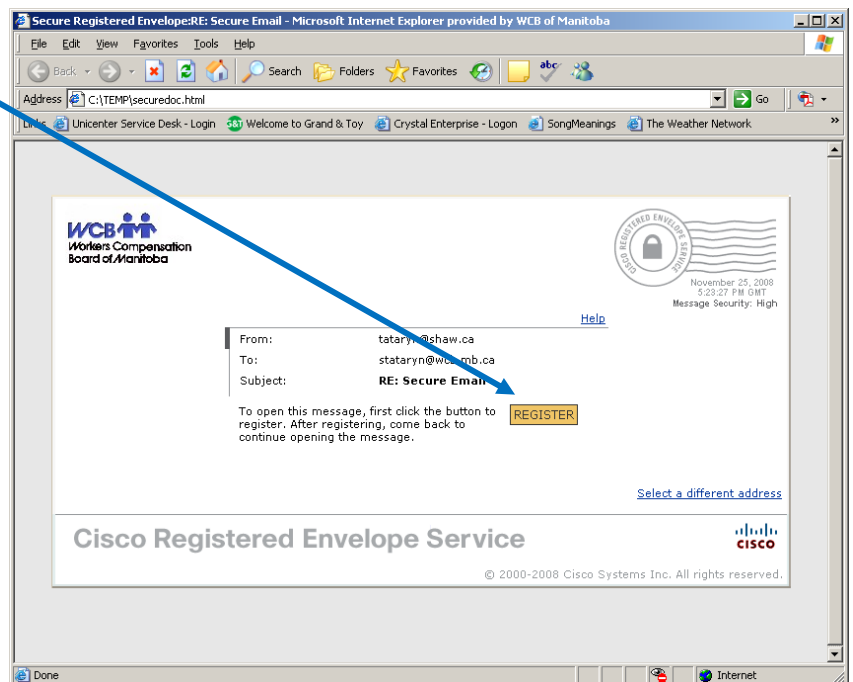
1. Right click on the attachment.
2. Select Open With
3. Click Ok to open with Internet Explorer.



If your E-mail address is not registered, a Register button will appear. This is a one time registration process.

Click the **Register** button.

Note: If the e-mail was sent to other people as well, you may need to select your e-mail address from a dropdown list.



The **New User Registration** screen displays.

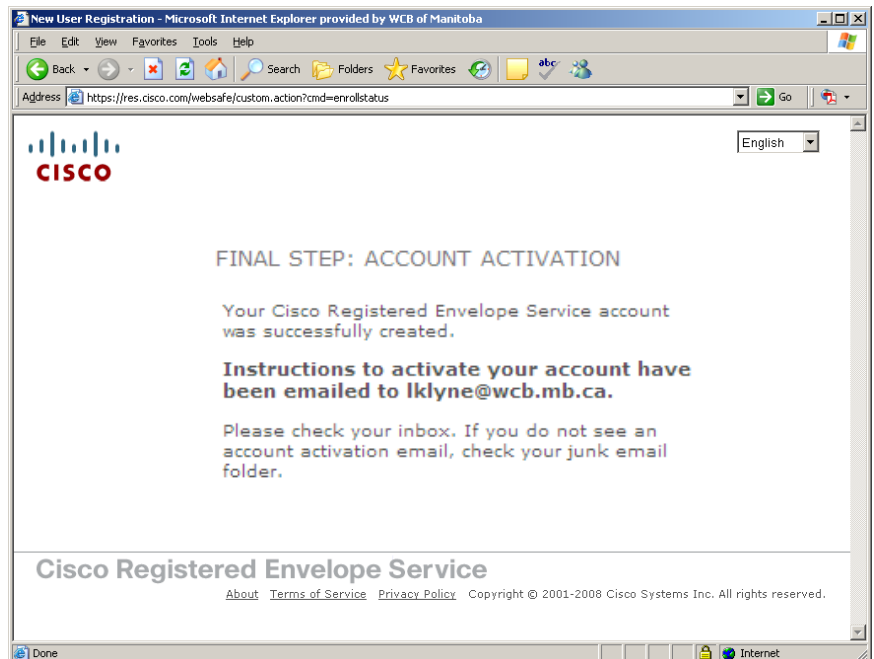
Complete the registration screen:

1. Choose a language.
2. Enter your first and last names.
3. Create a password.
4. Enter a short phrase as your Personal Security Phrase (e.g. My cat's name is Snow).
5. Select and answer 3 security questions.
6. Click the **Register** button.

The screenshot shows the 'NEW USER REGISTRATION' form. At the top, it says 'To assure future messages from this service are not accidentally filtered out of your email, please add "DoNotReply@res.cisco.com" to your Address Book or Safe Sender List.' and '* = required field'. The form is divided into several sections: 'Enter Personal Information' with fields for Email Address (lklyne@wcb.mb.ca), Language (English), First Name, and Last Name; 'Create a Password' with fields for Password and Confirm Password, and a Personal Security Phrase field with a checkbox to 'Enable my Personal Security Phrase'; and 'Select 3 Security Questions' with three sets of question, answer, and confirm answer fields. A 'Register' button is at the bottom right.

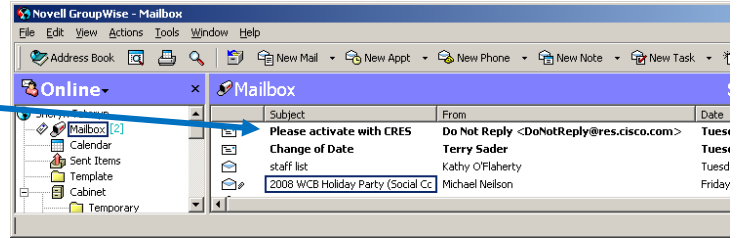
A window confirming you have created a *Cisco Registered Envelope Service* account will display.

Close this window.

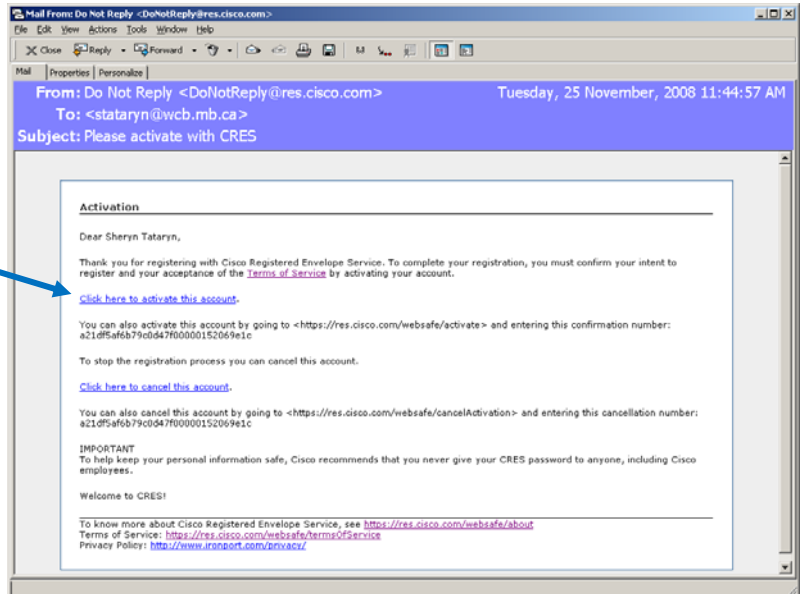


Within a few minutes you will receive an e-mail from **Do Not Reply**.

To activate your account, you need to first open this message.



Click the link as indicated to activate your account.



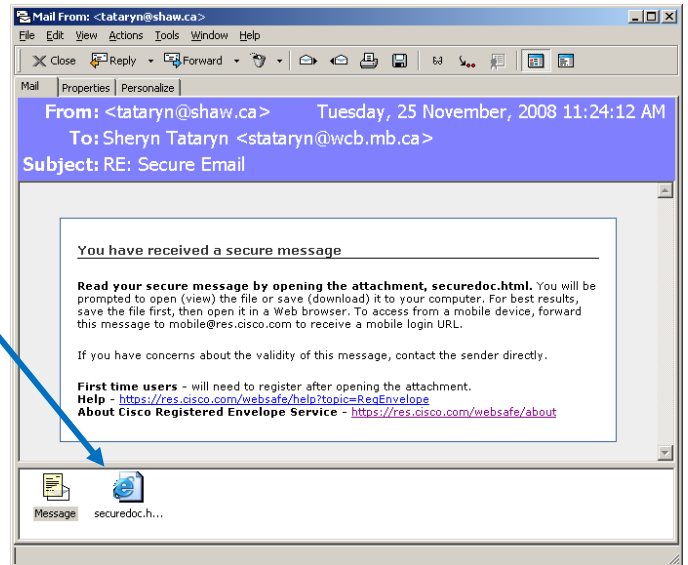
The confirmation screen will show that your account has been activated.

Close this window and return to the original secure e-mail.



Right click on the attachment again.

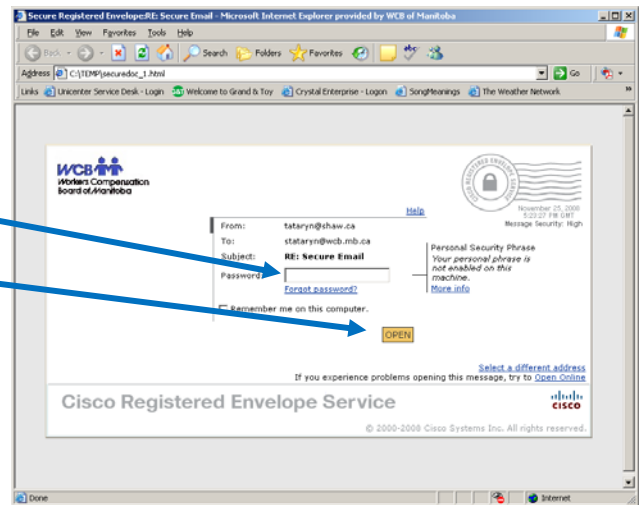
1. Select **Open With**
2. Click **Ok** to open with Internet Explorer.



Now that your E-mail address has been registered, the Cisco Registered Envelope Service screen will display.

Enter the password you created.

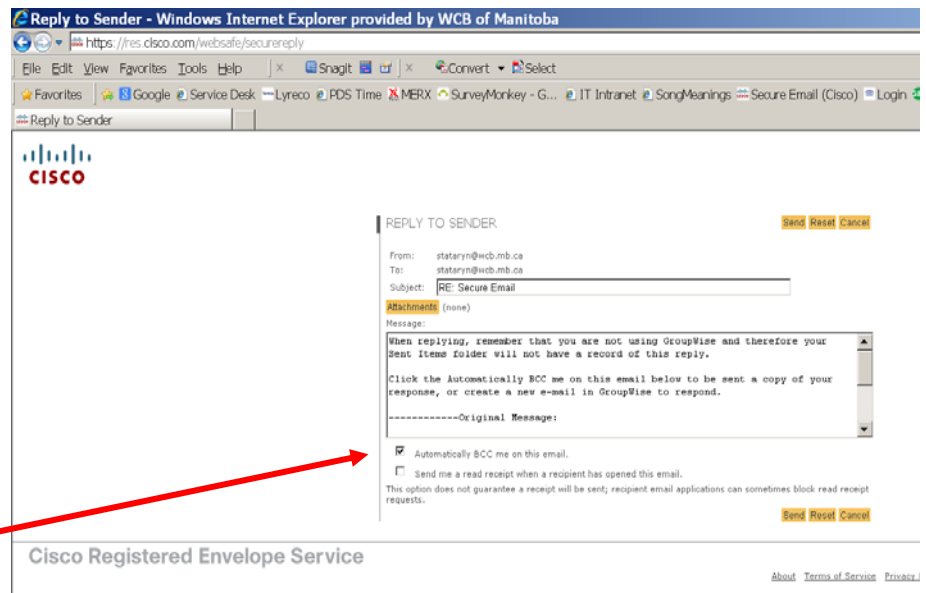
Click **Open** or press **Enter**.



The e-mail content will display and any attachments that may have been included will be listed.

IMPORTANT: When you reply to a secure e-mail, you are not using GroupWise so there is no record in your Sent Items folder.

If you need a record of your reply, check the *Automatically BCC me on this e-mail* checkbox.

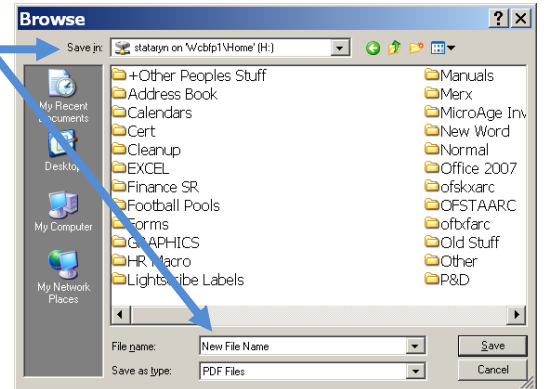
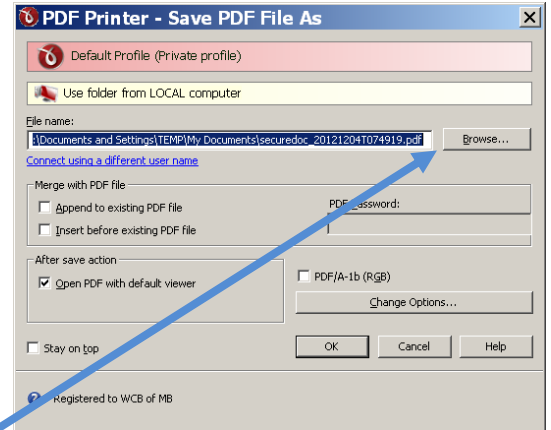


It is very important to follow the correct steps when reading these BCC messages. Please make sure you read the **Reading BCC E-mails** section on page 10.

SAVING E-MAILS

The preferred method for saving a Secure E-Mail and preserving the original content, is to print it to a PDF file. PDF files can be added as external documents to Emerge and Optimal or attached to e-mails and forwarded to other parties. To print to PDF, follow the steps below:

1. Click the **File** menu and select **Print**.
2. From the list of available printers select **PDF printer** and click **Print**.
3. On the **PDF Printer** dialogue box, click the **Browse...** button.
4. Select a location to save the file and enter a name for the file.
5. Click Save.
6. The PDF file will display once it has been created.



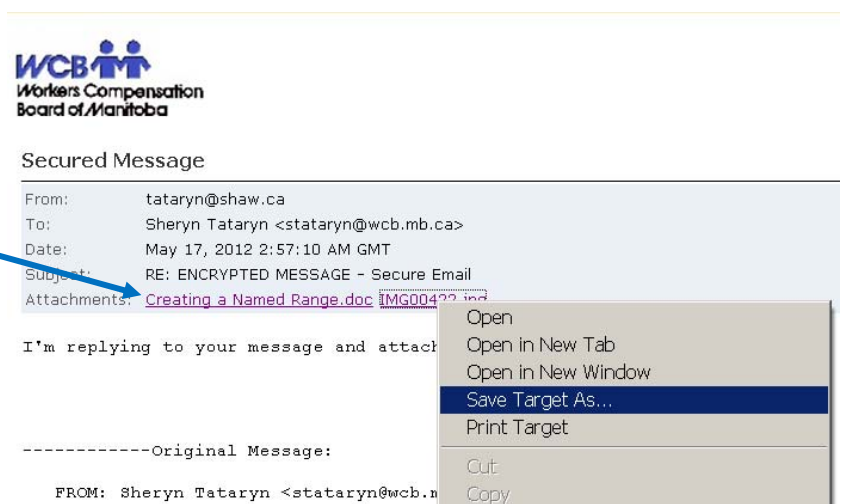
SAVING ATTACHMENTS

To save an attachment, right-click on the attachment link and choose **Save Target As...**

When the *Save As* window appears, select a location to save the file and enter a name in the **File Name** text box.

Click Save.

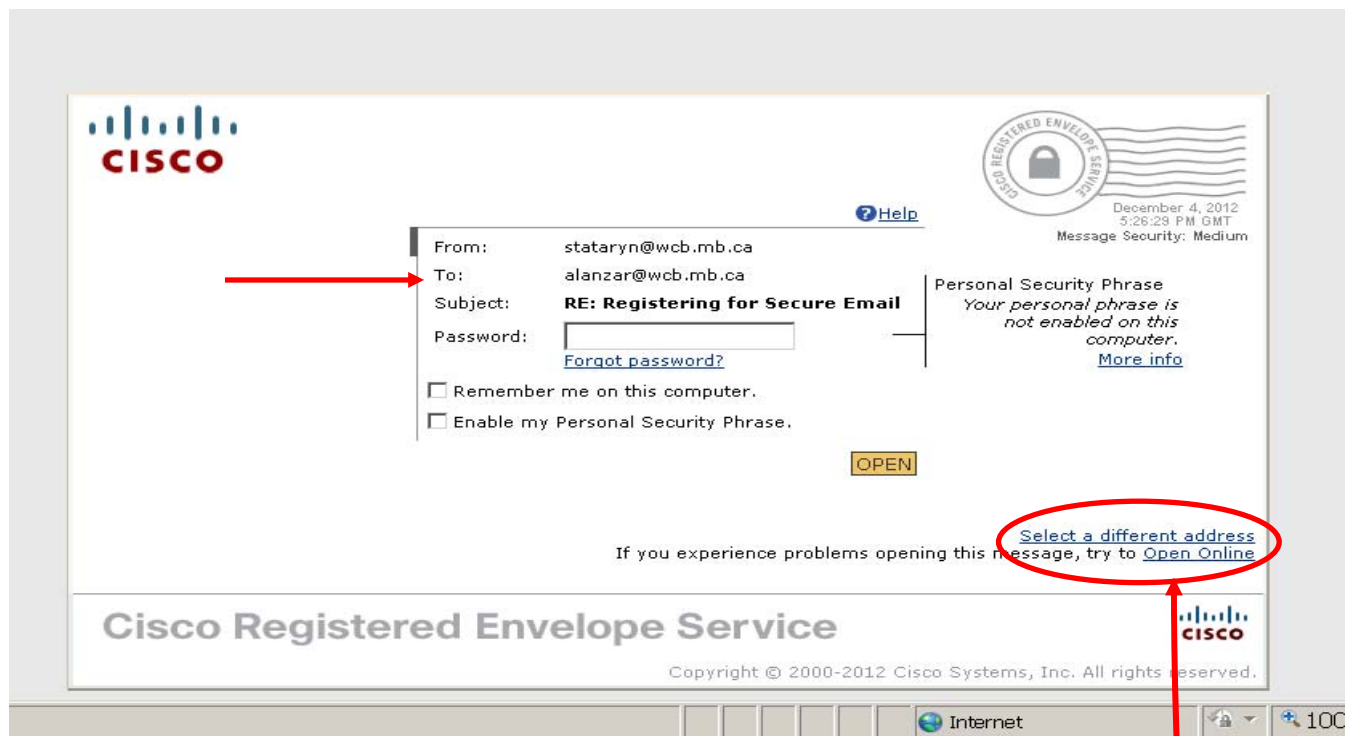
Repeat the process for each attachment.



READING BCC E-MAILS

When you blind copy yourself on a reply you are sending through CISCO, the copy you get will be addressed to the person you sent the reply to.

It is very important that you don't enter your password at this point or you risk locking up the recipient's Cisco account.



(Example above - stataryn@wcb.mb.ca used the BCC feature on an email to alanzar@wcb.mb.ca.)

Before entering your password, you need to change the To: address to your own.

1. Click the Select a different address link in the bottom right corner.

The following screen appears.

CISCO

CISCO REGISTERED ENVELOPE SERVICE
December 4, 2012
5:26:29 PM GMT
Message Security: Medium

[? Help](#)

From: stataryn@wcb.mb.ca
To: - Select One -
Subject: **RE: Registering for Secure Email**

SUBMIT

[My address is not listed](#)

Cisco Registered Envelope Service

Copyright © 2000-2012 Cisco Systems, Inc. All rights reserved.

Your address won't be included on the To: drop down list because it is a blind copy of the original e-mail.

1. Click the [My address is not listed](#) link.

CISCO

CISCO REGISTERED ENVELOPE SERVICE
December 4, 2012
5:26:29 PM GMT
Message Security: Medium

[? Help](#)

From: stataryn@wcb.mb.ca
To: Address not listed
Your address:
Subject: **RE: Registering for Secure Email**

SUBMIT

[My address is not listed](#)

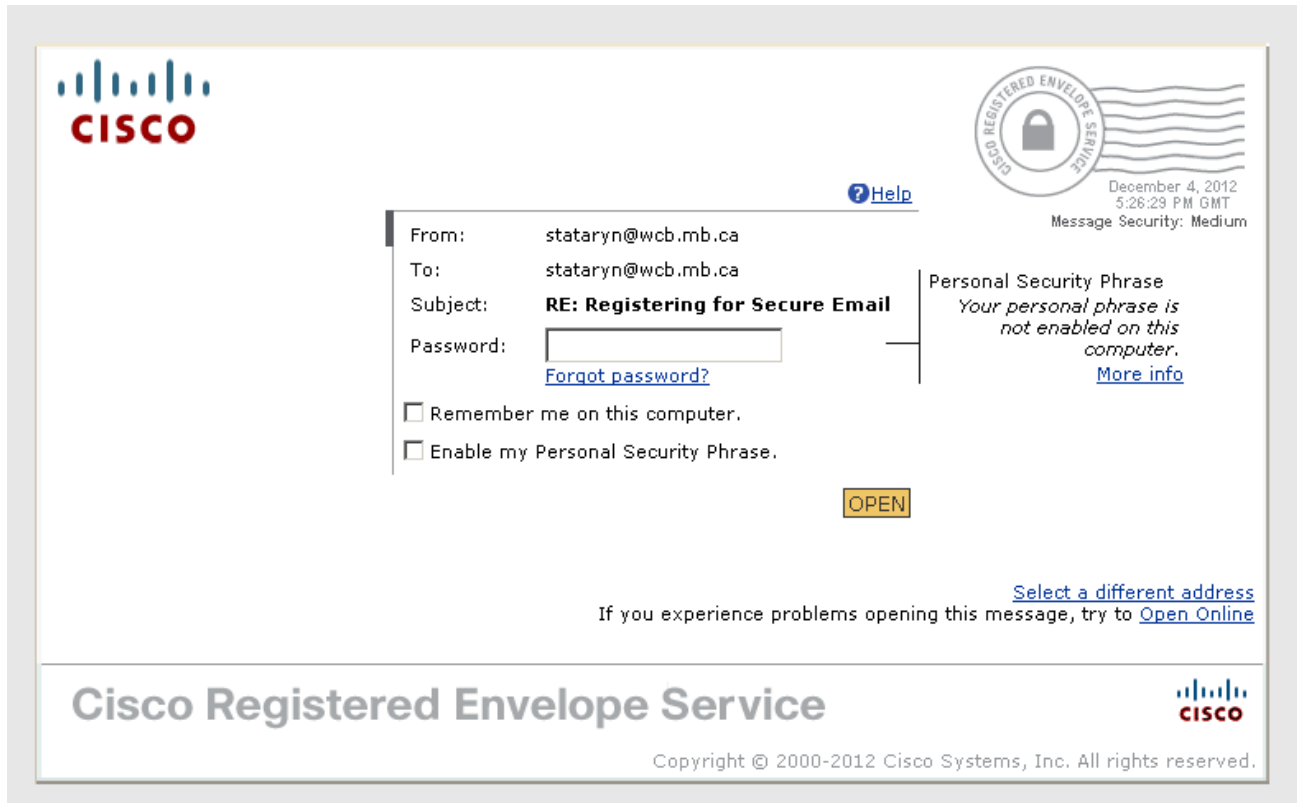
Cisco Registered Envelope Service



Copyright © 2000-2012 Cisco Systems, Inc. All rights reserved.

2. Enter your e-mail address and press **Enter** or click **Submit**.

Your address will now appear in the **To:** area.

3. Enter your password to open the BCC message you received.



[? Help](#)

December 4, 2012
5:26:29 PM GMT
Message Security: Medium


From: stataryn@wcb.mb.ca
To: stataryn@wcb.mb.ca
Subject: **RE: Registering for Secure Email**
Password:
[Forgot password?](#)

Personal Security Phrase
Your personal phrase is not enabled on this computer.
[More info](#)

Remember me on this computer.
 Enable my Personal Security Phrase.

OPEN

[Select a different address](#)
If you experience problems opening this message, try to [Open Online](#)

Cisco Registered Envelope Service 

Copyright © 2000-2012 Cisco Systems, Inc. All rights reserved.

ADDING EXTERNAL DOCUMENTS TO EMERGE

1. On any page that displays the **New Document** button, click the button.
2. On the Create Document page, click the **Add External Document** button.
3. On the Add External Document page, click the **Browse** button and locate the file you want to add.
4. Ensure that the other attributes are correct and appropriate.
5. To put the external document in the claim folder, click the **Add Document** button.

INFORMED CONSENT

If a worker is unwilling to participate in secure e-mail , you must have their consent prior to e-mailing confidential, personal or personal health information. The consent must be either written or sent via e-mail and must be stored as a business record.

To obtain informed consent, do the following:

1. Send an e-mail to the worker with the following scripted text:

The WCB has requested you to communicate via encrypted (secured) e-mail. By advising the WCB you want to communicate using unencrypted (unsecured) e-mail instead of secured e-mail you are expressly authorizing the WCB to use unsecured e-mail to communicate with you for all purposes. You acknowledge that unsecured e-mail communication may allow third parties to intercept and read your confidential, personal and/or personal health information and the WCB cannot protect any information sent via unsecured e-mail. The WCB shall in no way be liable for any such violation of your confidential, personal and/or personal health information, including any direct or indirect damages arising therefrom. Should you later decide you want the WCB to communicate with you via secure e-mail or not communicate via e-mail at all, you must advise the WCB in writing before such change can be implemented.

2. Advise them that if they still want you to communicate via unencrypted E-mail to reply back and indicate their consent.
3. Once you receive their e-mail, it must be stored as a business record. If it is claim related, it must be saved to the electronic claim file. See section **Saving E-Mails**.

IMPORTANT: When adding a consent e-mail to Emerge using Add External Document, the document description should indicate "**Worker Consent to Unencrypted E-mailing**".