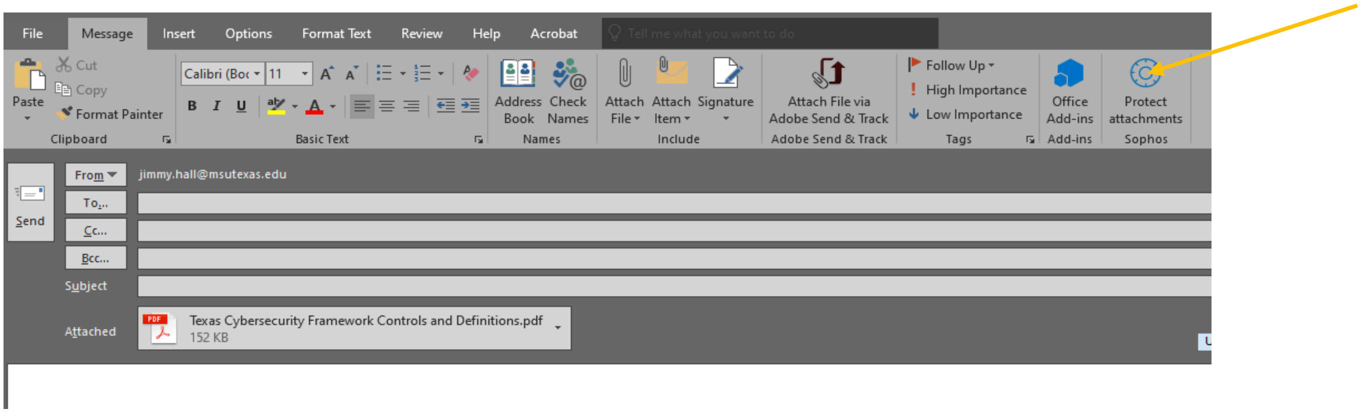
To create an encrypted message to an off-campus address you can follow the procedures below:

There are two ways to do this and this document covers both. **The BEST way** is to use the Sophos email encryption plugin that is installed when you have had IT setup desktop encryption on your office computer. Desktop encryption uses the Bitlocker technology built into Windows to encrypt the entire disk on your computer and uses the TPM or Trusted Platform Module in the computer to store the key. The key is also stored in the MSU Sophos management console to make sure we can assist you if you ever lose access to your key in stored in the TPM.

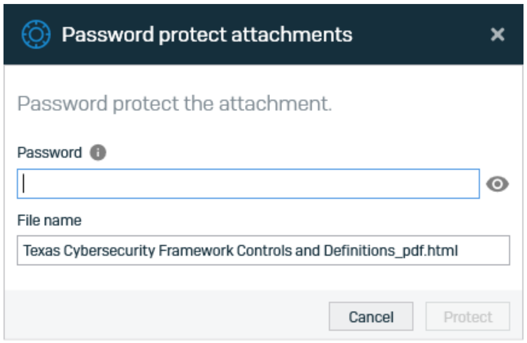
Once the Sophos plugin is installed in Outlook you can attach a file to an email as shown below and then click the Protect Attachments button to encrypt the file before it is sent.



From: jimmy.hall@msutexas.edu

Attached: Texas Cybersecurity Framework Controls and Definitions.pdf 152 KB

When you click the Protect attachments button you will see a window pop up asking for a password as shown below.

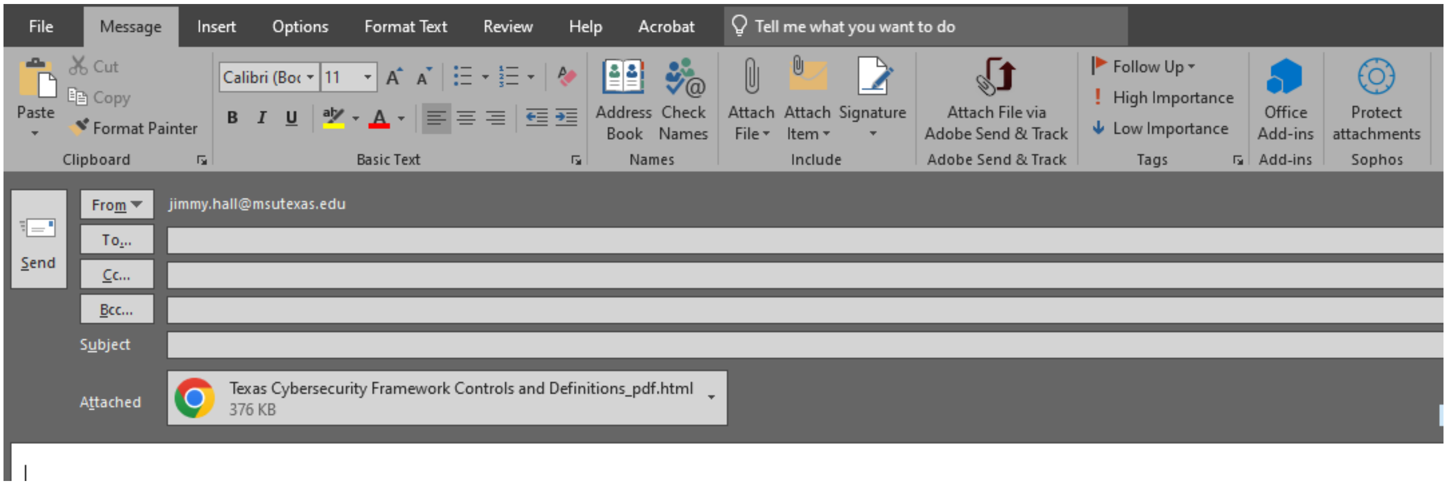


Password protect the attachment.

Password

File name: Texas Cybersecurity Framework Controls and Definitions_pdf.html

Once you enter the password and click the Protect button the attachment will be encrypted and you will notice that the attachment type changes.

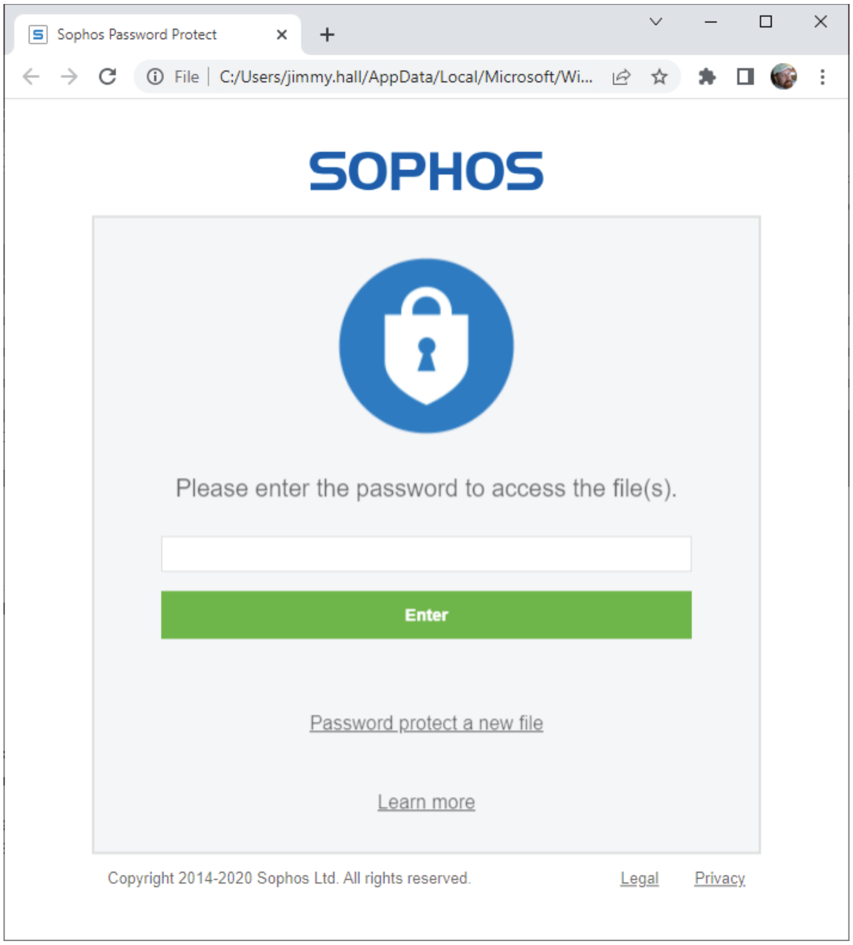


From: jimmy.hall@msutexas.edu

Attached: Texas Cybersecurity Framework Controls and Definitions_pdf.html 376 KB

Complete the email addressing and send as you normally would. You should send the password in a separate email or by txt message to the recipient but never in the same email.

The recipient can double click the received attachment and will be prompted for the password in order to decrypt.


Sophos Password Protect
File
C:/Users/jimmy.hall/AppData/Local/Microsoft/Wi...
SOPHOS
Enter
Password protect a new file
Learn more
Legal
Privacy

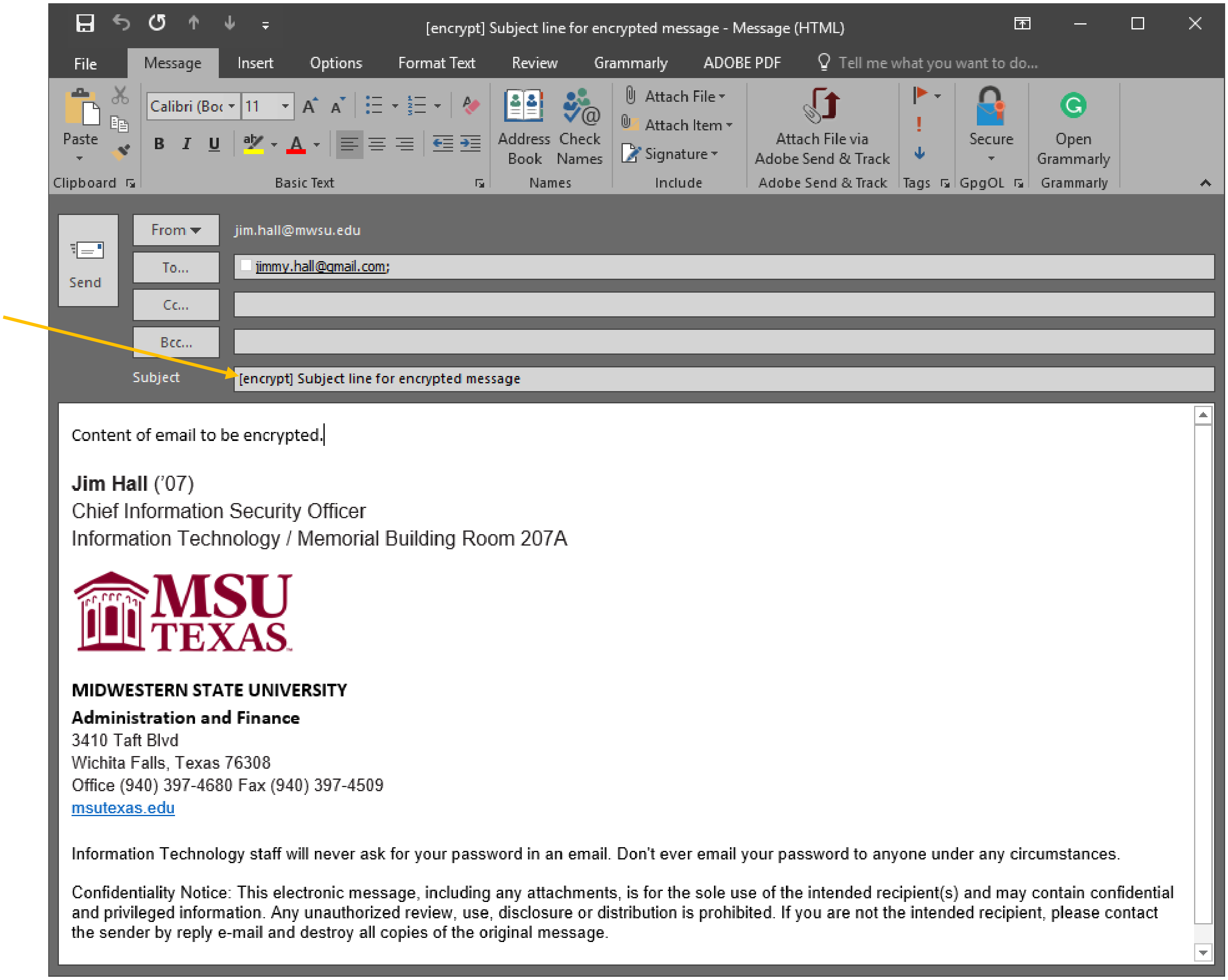
Please enter the password to access the file(s).

Copyright 2014-2020 Sophos Ltd. All rights reserved.

Once the password is successfully typed in, click the Enter button to complete the decryption of the attachment.

Another way to encrypt messages to off-campus users is shown below. Do not use this if the content cannot reside in sent items unencrypted.

Create your message just as you normally would, but the subject line must begin with [encrypt] as shown below. You can use any normal subject line text after [encrypt] that you wish to use.   Please make certain that there is a space between [encrypt] and your subject line text.



[encrypt] Subject line for encrypted message - Message (HTML)

From: jim.hall@mwsu.edu

To...: jimmy.hall@gmail.com;

Subject: [encrypt] Subject line for encrypted message

Content of email to be encrypted.

Jim Hall ('07)
Chief Information Security Officer
Information Technology / Memorial Building Room 207A

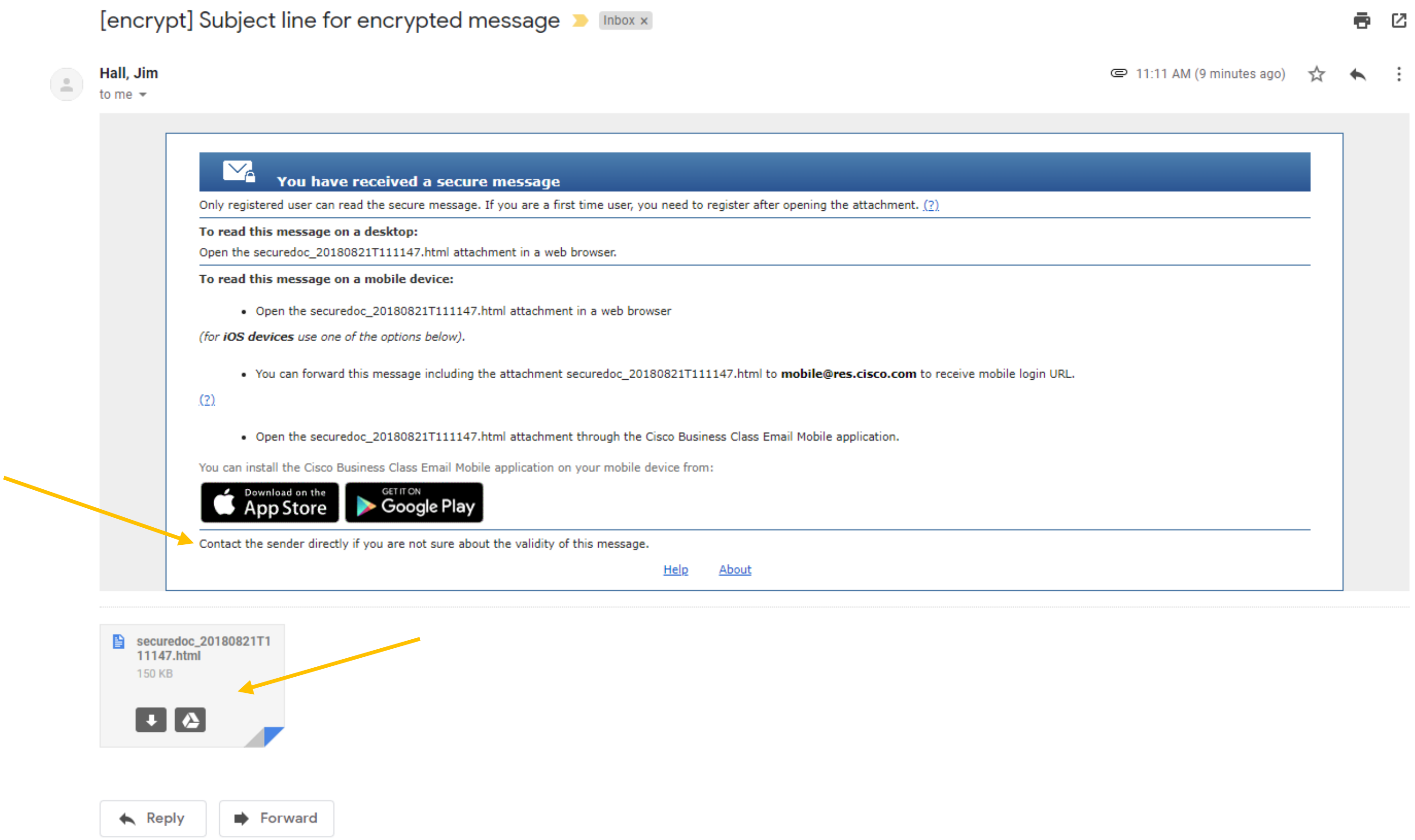
MSU TEXAS

MIDWESTERN STATE UNIVERSITY
Administration and Finance
3410 Taft Blvd
Wichita Falls, Texas 76308
Office (940) 397-4680 Fax (940) 397-4509
msutexas.edu

Information Technology staff will never ask for your password in an email. Don't ever email your password to anyone under any circumstances.

Confidentiality Notice: This electronic message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

The message recipient will get an email similar to the one shown below:



[encrypt] Subject line for encrypted message

You have received a secure message

Only registered user can read the secure message. If you are a first time user, you need to register after opening the attachment. (?)

To read this message on a desktop:

Open the securedoc_20180821T111147.html attachment in a web browser.

To read this message on a mobile device:

- Open the securedoc_20180821T111147.html attachment in a web browser

*(for **iOS devices** use one of the options below).*

- You can forward this message including the attachment securedoc_20180821T111147.html to **mobile@res.cisco.com** to receive mobile login URL.

(?)

- Open the securedoc_20180821T111147.html attachment through the Cisco Business Class Email Mobile application.

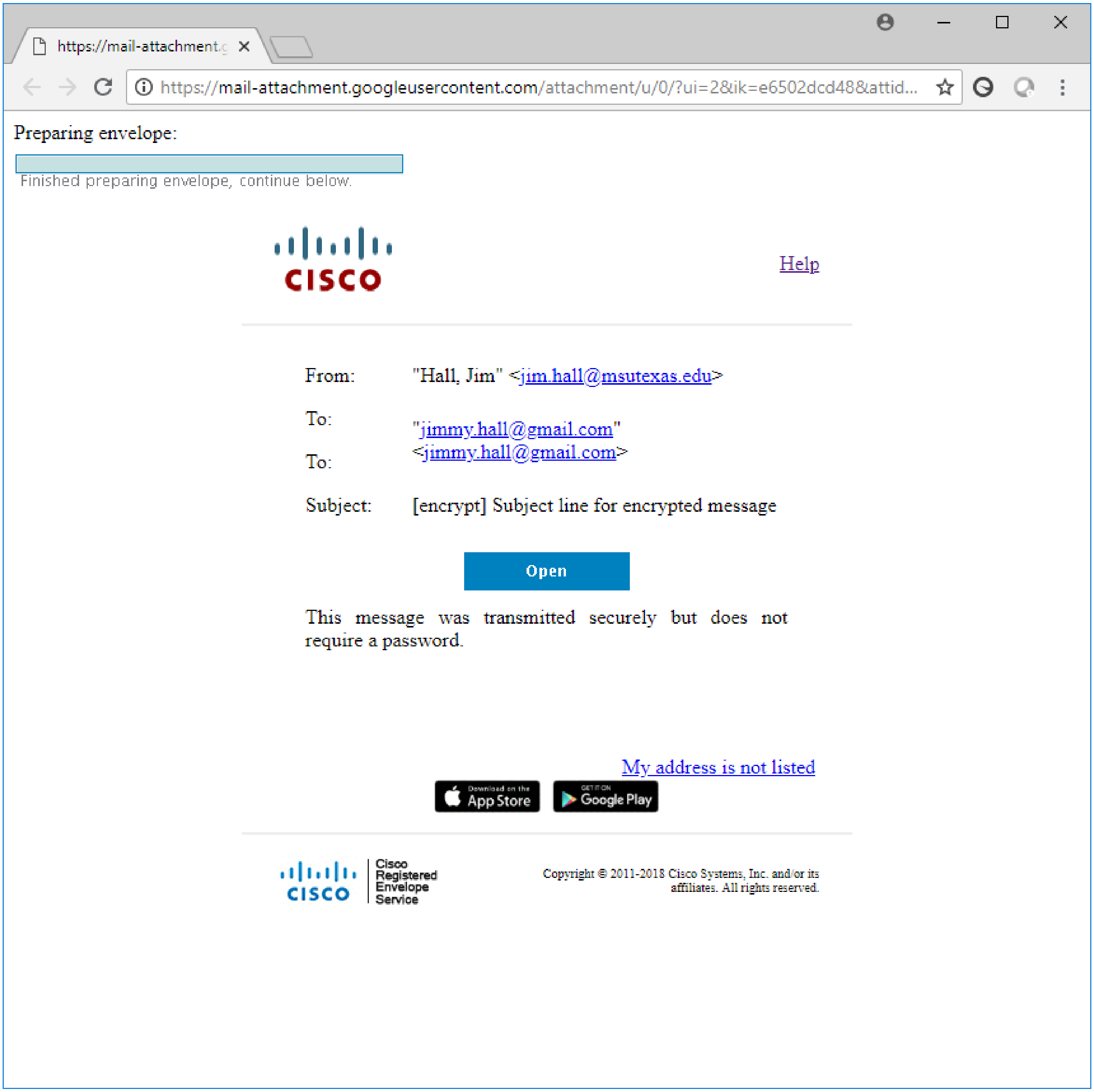
You can install the Cisco Business Class Email Mobile application on your mobile device from:

Contact the sender directly if you are not sure about the validity of this message.

Help About

To open the message double-click the attachment. Notice that we instruct the recipient to contact the sender directly if unsure of the validity of the message.

When you open the attachment you will see a browser screen similar to the one below.


https://mail-attachment.g
https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=e6502dcd48&attid...
Help
Open
App Store
Google Play

Preparing envelope:

Finished preparing envelope, continue below.

From: "Hall, Jim" <jim.hall@msutexas.edu>

To: "jimmy.hall@gmail.com" <jimmy.hall@gmail.com>

To:

Subject: [encrypt] Subject line for encrypted message

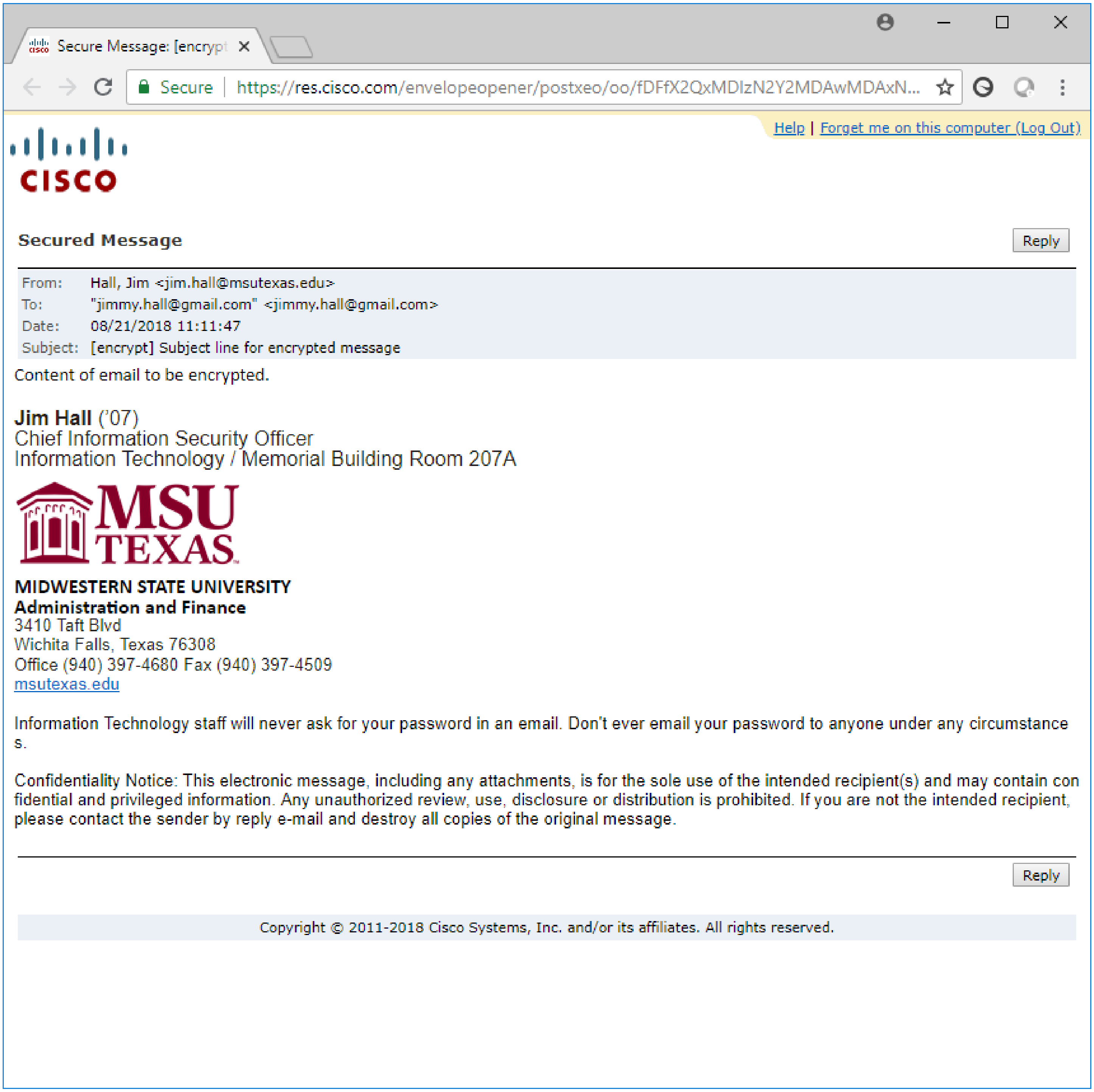
This message was transmitted securely but does not require a password.

My address is not listed

Cisco Registered Envelope Service

Copyright © 2011-2018 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

The encrypted message is displayed once the Open button has been clicked.


Secure Message: [encrypt
Secure
https://res.cisco.com/envelopeopener/postxeo/oo/fDFfX2QxMDIzN2Y2MDAwMDAxN...
Help | Forget me on this computer (Log Out)
cisco
Reply

Secured Message

From: Hall, Jim <jim.hall@msutexas.edu>
To: "jimmy.hall@gmail.com" <jimmy.hall@gmail.com>
Date: 08/21/2018 11:11:47
Subject: [encrypt] Subject line for encrypted message

Content of email to be encrypted.

Jim Hall ('07)
Chief Information Security Officer
Information Technology / Memorial Building Room 207A

MSU TEXAS

MIDWESTERN STATE UNIVERSITY
Administration and Finance
3410 Taft Blvd
Wichita Falls, Texas 76308
Office (940) 397-4680 Fax (940) 397-4509
msutexas.edu

Information Technology staff will never ask for your password in an email. Don't ever email your password to anyone under any circumstances.

Confidentiality Notice: This electronic message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

Copyright © 2011-2018 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

The user can click the Reply button on the encrypted message and the process will work the same way in reverse for the reply with the original sender receiving the encrypted message.