
Proofpoint Email Encryption Manual

18 July 2014



Table of Contents

Table of Contents	2
Why did I Receive an Encrypted Email?	3
Registering to Open an Encrypted Email for the First Time	3
Opening an Encrypted Email (Subsequent Openings).....	5
Forwarding or Replying to Encrypted Messages.....	5
Closing an Encrypted Message.....	6
Initiating an Encrypted Message.....	6
Using Proof Point Encryption by Lpha.mopublic.org Email Addresses.....	7
Using the Proof Point Encryption Site for Non-mopublic.org Addresses and All Other Users.....	8

Why did I Receive an Encrypted Email?

The Department of Health and Senior Services uses Proofpoint email encryption to eliminate the risks in sharing Protected Health Information (PHI). Users can manually encrypt email messages using [encrypt] in the subject line. For those in the State of Missouri email system (mo.gov domain), Proofpoint automatically screens all outgoing messages (and attachments) for PHI and auto-encrypts the contents if sensitive information is suspected. This means that emails from DHSS staff may be encrypted by the sender or by the software. In some cases the software will auto-encrypt a message without PHI if it detects an eight or nine digit number in the body of the message or an attachment. Invoice numbers, confirmation numbers, or order numbers may be mistaken for Social Security numbers or DCNs by the software. If you receive an encrypted message from DHSS, simply decrypt the message to read.

Registering to Open an Encrypted Email for the First Time

When you open an encrypted email that was sent from the State using Proofpoint encryption, the email will appear as shown in Figure 1 below. It will instruct you to open the attachment called “SecureMessageAtt.html”.

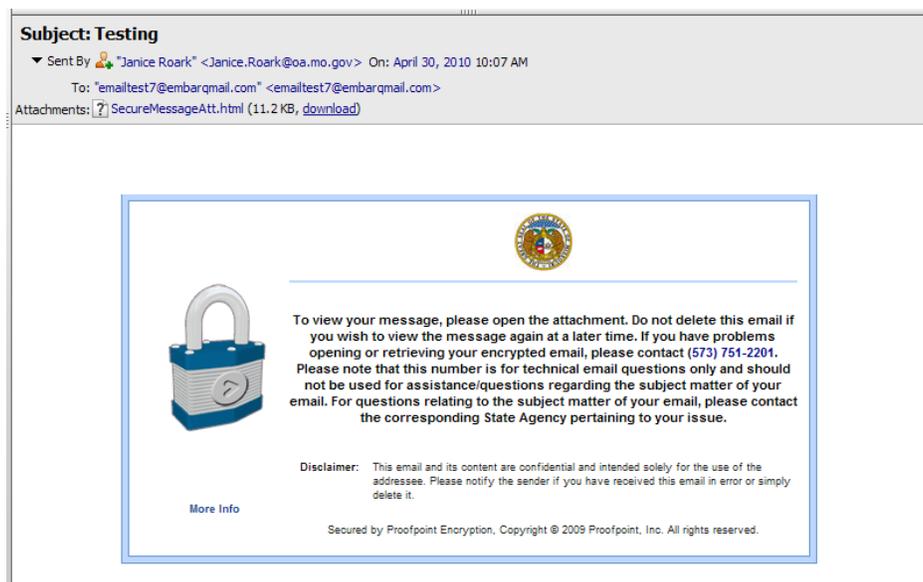


Figure 1: Encrypted Email Message – Email sent from the State to an Internet Address instructing the Recipient to open the “SecureMessageAtt.html” Attachment

When you open the attachment, SecureMessageAtt.html, you are prompted to click the button that says “Click to read message”, as shown in Figure 2 below.



Figure 2: Recipient is prompted to click the button that says “Click to read message”.

If this is the first time you have opened an encrypted message, you will be prompted to register in the Proofpoint email encryption system as shown in Figure 3 below. This is a one-time registration process. You will need to type in your first name, last name, create a password, confirm the password, and then select a password reset question and answer.

Note: The password below is a password you will create yourself. The password entered must be 7 to 20 characters long with one number character required. This password will be used for opening all subsequent encrypted messages.

A screenshot of a registration form titled "Registration". At the top is a circular seal with an eagle and the text "UNITED STATES OF AMERICA". Below the seal is the text "Create your account to read secure email." The form contains the following fields: "Email Address:" with the value "emailtest7@embarqmail.com"; "First Name:" with the value "Test"; "Last Name:" with the value "User"; "Password:" with a masked field of 10 dots; "Confirm Password:" with a masked field of 10 dots; "Password Reset" section with a "Question:" dropdown menu showing "Your childhood best friend" and an "Answer:" text box with the value "Mary". At the bottom right is a "Continue" button with a right-pointing arrow.

Figure 3: Recipient is prompted to register in the Proofpoint encryption system by entering their first name, last name, password, confirm password, and password reset question/answer.

Opening an Encrypted Email (Subsequent Openings)

Once you have completed the password registration, you will only be prompted to enter your password as shown in Figure 4 below.



Figure 4: Recipient is prompted to enter their password for any subsequent encrypted messages they receive after the initial registration.

After entering your password, you can view the encrypted message as shown in Figure 5 below.

Forwarding or Replying to Encrypted Messages

After logging in and decrypting a message, you may reply or forward the encrypted message. Click the “Reply” button or “Forward” button located inside the encrypted message under the Missouri State Seal. This will ensure that your reply and/or forward of the message remains encrypted.

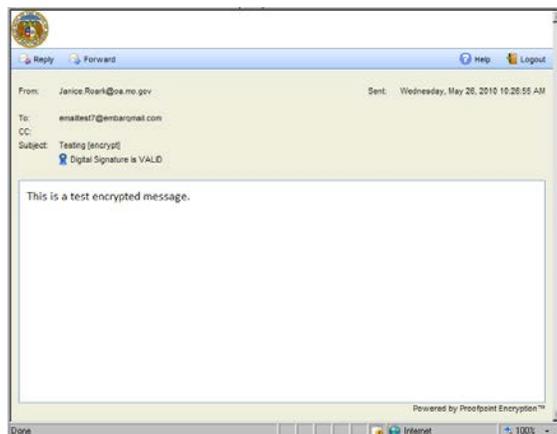


Figure 5: The contents of the encrypted message.

NOTE: You can only forward the encrypted email to users who are in the same email domain as the sender or recipient. You will receive an error if forwarding the message to anyone else.

Closing an Encrypted Message

When you are finished, click “Logout” found in the upper right hand corner of the message to ensure proper closure. When you click “Logout”, a message will appear on the screen as shown in Figure 6 below.



Figure 6: Logged Out message

Initiating an Encrypted Message

The State of Missouri’s Proof Point system provides options for initiating an encrypted message based on the sender’s email domain. The options are described in the table below.

	mopublic.org domains	Other domains
Encryption of original messages to any email recipient using [encrypt] in the subject line	✓	
Encryption of original messages to State of Missouri domains only (does not include mopublic.org) using securemail.mo.gov/securereader/init.jsf?brand=fbab8553	✓	✓

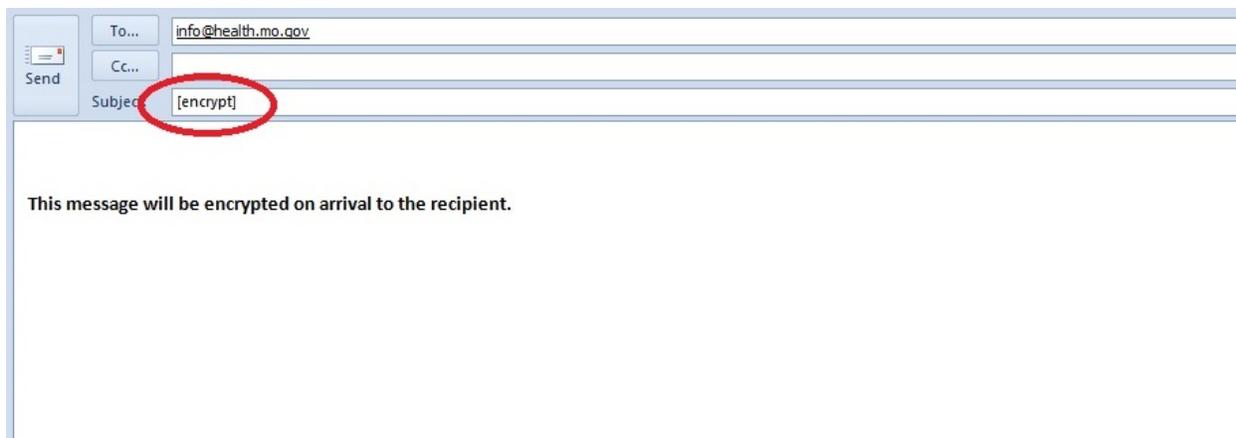
LPHAs using the mopublic.org email domain are able to initiate encrypted emails to any email recipient under the DHSS' Proofpoint license by typing [encrypt] in square brackets in the subject line of a new message.

LPHAs using other email domains (not including mopublic.org) are not able to initiate original encrypted emails under DHSS' Proofpoint license using [encrypt] in the subject line.

All users (regardless of email domain) may initiate an encrypted message to a State of Missouri email address. This is initiated by logging into the Proofpoint encryption site at: securemail.mo.gov/securereader/init.jsf?brand=fbab8553.

Using Proofpoint Encryption by Lpha.mopublic.org Email Addresses

1. To initiate a secure message to a State of Missouri email address, open a new message window in your email program.
2. Enter the recipient's email address in the "To" section. Type [encrypt] in the subject line.
3. Please note that to successfully encrypt a message, you must use square brackets [], not curly brackets or braces. You may include a subject after [encrypt], but no PHI should be included in the subject line since Proofpoint can only encrypt the body of messages.



4. Enter the body text of your message and click send to complete the process.

Using the Proofpoint Encryption Site for Non-mopublic.org Addresses and All Other Users

1. Open an Internet browser and go to the link:

<https://securemail.mo.gov/securereader/init.jsf?brand=fbab8553>

You will be prompted to enter your email address to proceed, as show in Figure 1 below. Enter your email address and click “Continue”.



Figure 1: A sender clicks on the URL to initiate an encrypted email to the State and is prompted to enter their email address.

2. The first time you initiate an encrypted message to the State, you will be prompted to register in the Proofpoint email encryption system as shown in Figure 2 below. If you have already registered in Proofpoint to decrypt a message, please use the same password to log in to the Proofpoint site. Continue with step 6.

If you need to register, you are then prompted to type in your first name, last name, create a password, confirm the password, and then select a password reset question and answer.

Note: The password is a password you will create yourself. The password entered must be 7 to 20 characters long, with one number character required.

Figure 2: Registering on the Proof Point site.

- After you have registered and selected “Continue”, an “Activation Request Sent” notice, as shown in Figure 3 below, will appear on the screen informing you that an activation email has been sent. This email contains a URL that must be clicked to activate your Proofpoint email encryption account.

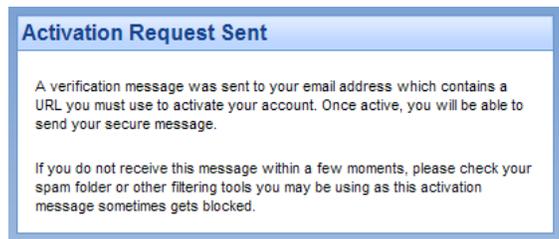


Figure 3: The sender will receive an Activation Request Sent notice on the screen

- Next, go into your email account and open the Proofpoint Encryption Registration message. Click on the securemail.mo.gov URL within the registration message as shown in Figure 4.

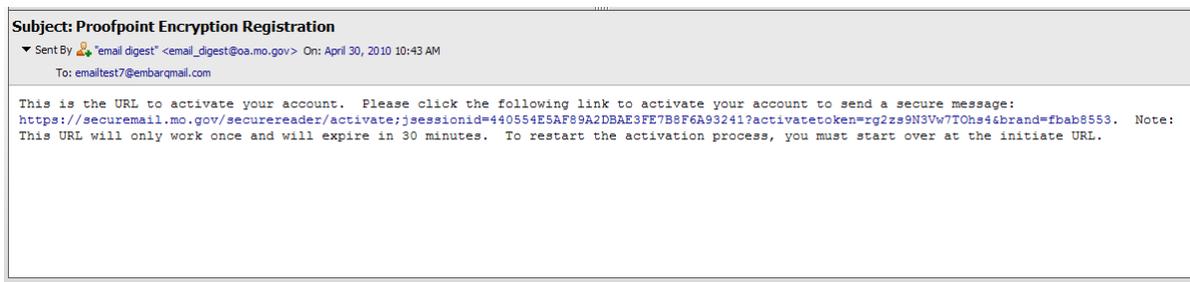


Figure 4

- You will receive an “Account Activated” message on the screen that says your account has been successfully activated as shown in Figure 5.

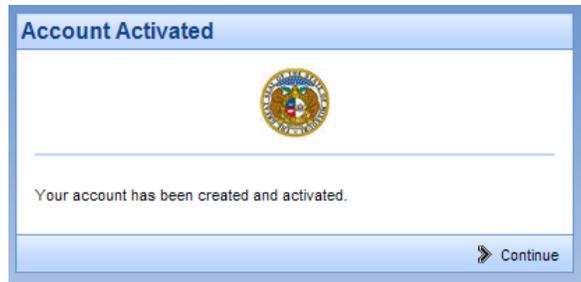


Figure 5

6. After you click “Continue”, a window will appear that will allow you to compose and send an encrypted message, as shown in Figure 6 below. Complete the “To” field, the “Subject” field and type in the text of the message, then press “Send”.



Figure 6

7. A message, as shown in Figure 7 below, will appear on the screen informing you that your message was successfully sent. You can either click “New Message” to compose another encrypted email, or click “Logout” to exit the window.

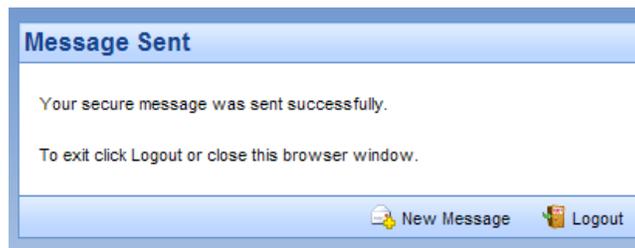


Figure 7

8. To initiate any subsequent encrypted messages, click on the URL, <https://securemail.mo.gov/securereader/init.jsf?brand=fbab8553>. Instead of receiving the initial registration screen as show in Step 2, you will be prompted to type in your password as shown in Figure 8 below.

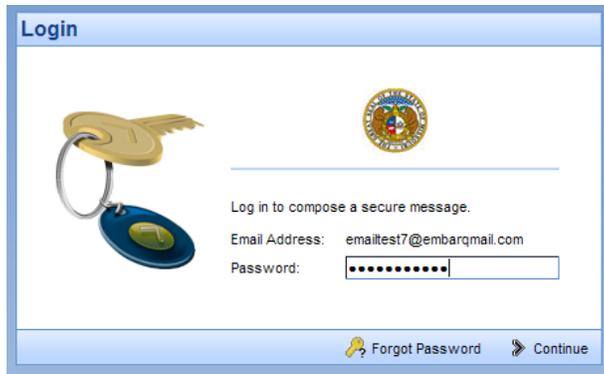


Figure 8

9. A window will appear that will allow you to compose and send an encrypted message, as shown in Figure 9 below. Complete the “To” field, the” Subject” field and type in the text of the message, then press “Send”.

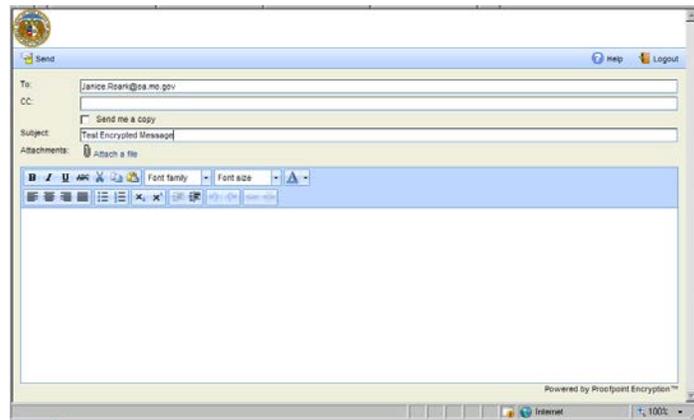


Figure 9

Note: You can only add recipients who belong to State of Missouri email domain