

Proofpoint Encryption Guide Proofpoint Version 8.20.8

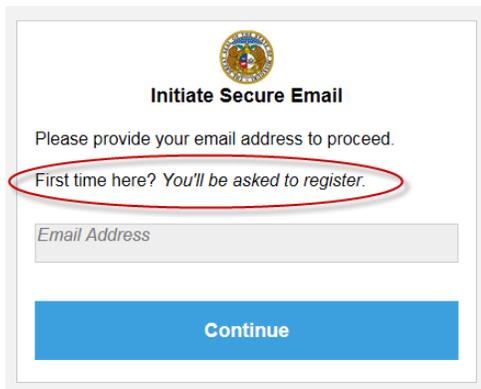
Proofpoint encryption is a type of email encryption between State of Missouri agencies using Proofpoint and an outside (external) recipient and vice versa. The internal (State) user must have a Proofpoint encryption license for an external person to send a Proofpoint encrypted email to them.

How to Send a Proofpoint Encrypted Email – External Sender

If an external sender needs to send an encrypted email to a State recipient, and that State recipient has a license to use Proofpoint email encryption, the external sender can use the following link to send an encrypted email from the State's Proofpoint system:

<https://mosecuremail.mo.gov/securereader/init.jsf?brand=907ede0c>

After clicking on the link, the sender will be prompted to enter their email address to proceed. The sender should enter their email address and click "Continue", as shown below.




Initiate Secure Email
Please provide your email address to proceed.
First time here? You'll be asked to register.
Email Address

Continue

The first time a sender initiates an encrypted message to the State using the Proofpoint email encryption system, they will be prompted to register in the Proofpoint email encryption system as shown below. This is a one-time registration process. The sender is prompted to type in their first name, last name, create a password, confirm the password, and then select two password reset questions and answers. The sender must complete this information to register to send an encrypted message. The sender should complete this information and select "Continue", as shown below.



Registration

Password Policy

- Passwords must be 8-20 characters long.
- At least one digit (0-9) is required.
- At least one symbol character is required.
- Both uppercase and lowercase characters are required.
- Your username may not appear in the password.

Create your account to read secure email.

Email Address: [REDACTED]@hotmail.com

First Name:

Last Name:

Password:

Confirm Password:

Question :

Answer:

Question 2:

Answer:

Continue

Note: The password must be 8 to 20 characters long, contain at least 1 number, 1 special character (special character such as: !@\$%^*()[]_ +=:.) and a combination of upper and lowercase letters. **Spaces are not allowed in passwords.** The sender should remember the password they enter on this screen because it will be needed for any subsequent encrypted messages they open.

After the sender has registered and selects “Continue”, an “Activation Request Sent” notice will appear on the screen informing the sender that an activation email has been sent to them. This email contains a URL that must be clicked to activate their Proofpoint email encryption account.



Activation Request Sent

A verification message was sent to your email address which contains a URL you must use to activate your account. Once active, you will be able to send your secure message.

If you do not receive this message within a few moments, please check your spam folder or other filtering tools you may be using as this activation message sometimes gets blocked.



email_digest@oa.mo.gov



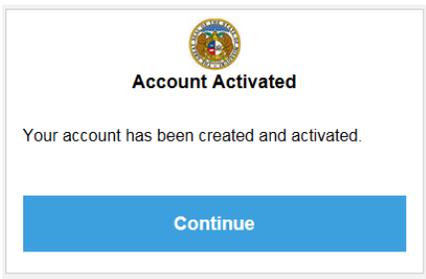
To: You

Thu 5/29/2025 2:32 PM

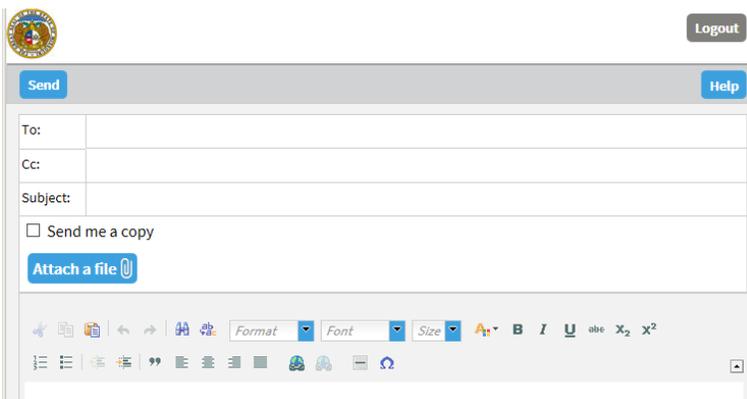
This is the URL to activate your account. Please click the following link to activate your account to send a secure message: <https://mosecuremail.mo.gov/securereader/activate?token=Ww6TrjWMNq72SAWPo3IS4&brand=907ede0c>. Note: This URL will only work once and will expire in 30 minutes. To restart the activation process, you must start over at the initiate URL.

After clicking on the URL, the sender will receive an “Account Activated” message on the screen that says their account has been successfully activated. The sender should click “Continue”.

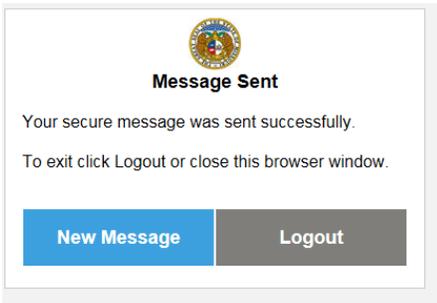
Note: If the sender receives an error or “Account Not Activated” message, the sender should start again by clicking on the <https://mosecuremail.mo.gov/securereader/init.jsf?brand=907ede0c> link. When a new registration message is received, the sender should follow the link in the NEW message to activate the account.



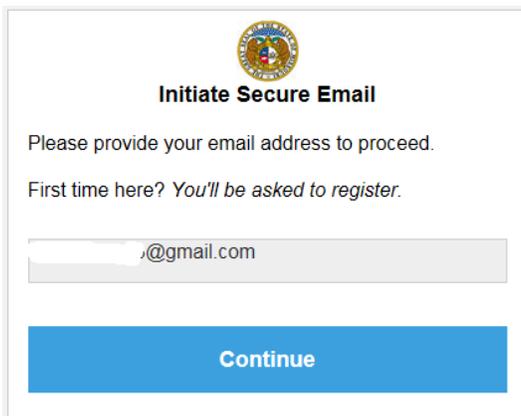
A window will appear that will allow the sender to compose and send an encrypted message. The sender needs to complete the “To” field, the “Subject” field and type in the text of the message, then press “Send”. **Note:** The sender can only add recipients who belong to an email domain that Proofpoint handles mail for, i.e. oa.mo.gov, dss.mo.gov, etc.



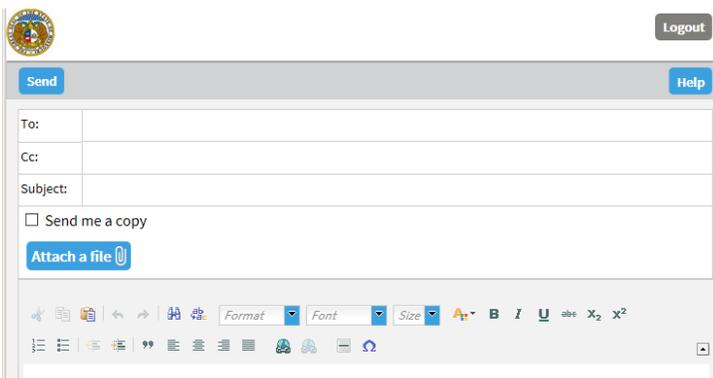
A message will appear on the screen informing the sender that their message was successfully sent. The sender can either click “New Message” to compose another encrypted email or click “Logout” to exit the window.



For any subsequent encrypted messages initiated by this same sender, the sender just needs to click on the URL, <https://mosecuremail.mo.gov/securereader/init.jsf?brand=907ede0c>. Instead of receiving the initial registration screen, the sender will see their email address already populated. The user should click "continue", and then enter their password and click "continue".



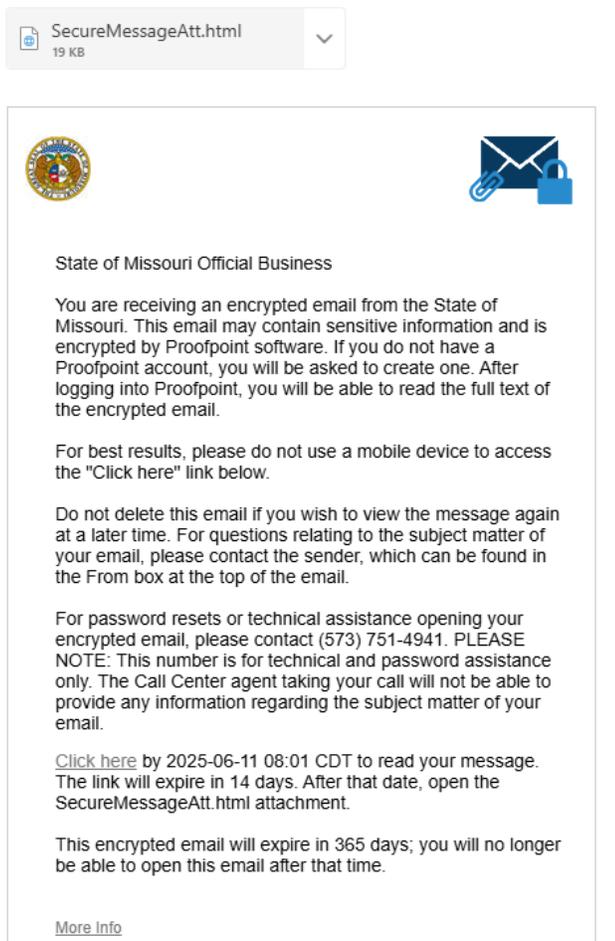
A window will appear that will allow the sender to compose and send an encrypted message.



How to open a Proofpoint encrypted email – External Recipient:

When an external recipient opens an encrypted email that was sent from the State using Proofpoint encryption, the email will appear as shown below. It will instruct the recipient to view their message by clicking on the “Click here” link.

Note: *If the link does not work they can open the attachment called “SecureMessageAtt.html” or save the attachment to their machine and then open it.*



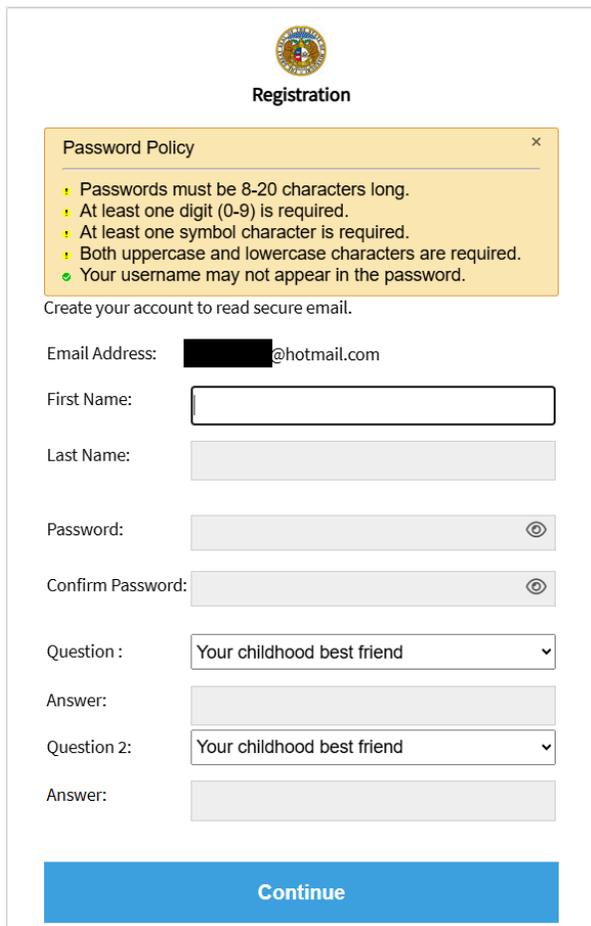
First Time Using Proofpoint Encryption to Open an Encrypted Message:

If this is the first time the recipient has opened an encrypted message that was sent from the State using the Proofpoint email encryption system, when the recipient clicks the button to read message, they will be prompted to register in the Proofpoint email encryption system as shown below. This is a one-time registration process.

The recipient is prompted to type in their first name, last name, create a password, confirm the password, and then select two password reset questions and answers. The recipient must complete this information to view the encrypted message.

Note: *The password must be 8 to 20 characters long, contain at least 1 number, 1 special character (special character such as: !@\$%^*()[]_ +=:;) and a combination of upper and lowercase letters. Spaces are not allowed in*

passwords. The sender should remember the password they enter on this screen because it will be needed for any subsequent encrypted messages they open.

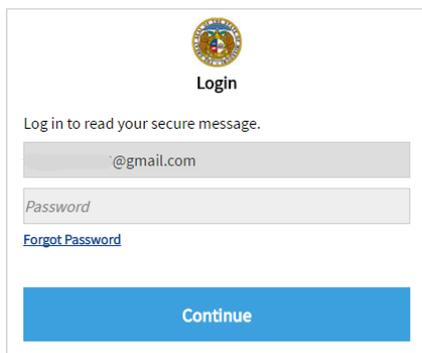


The registration form features a logo at the top center. Below it, a yellow popup window titled "Password Policy" lists five requirements: 8-20 characters, at least one digit, at least one symbol, both uppercase and lowercase characters, and the username cannot be in the password. The form itself asks for an email address (partially filled with a redacted name and "@hotmail.com"), first and last names, password and confirm password (with visibility toggles), and two security questions (both set to "Your childhood best friend") with corresponding answer fields. A blue "Continue" button is at the bottom.

Once the user is registered this first time the message will open.

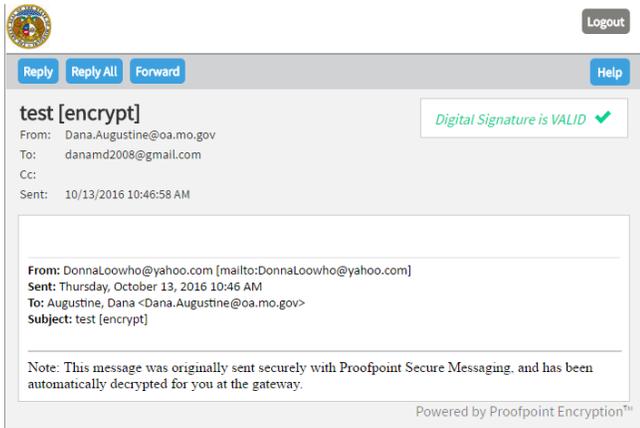
If Previously Registered:

For any subsequent encrypted email messages, the recipient receives after they have completed the one-time enrollment in the Proofpoint encryption system, the recipient will only be prompted to enter their password, as shown below.

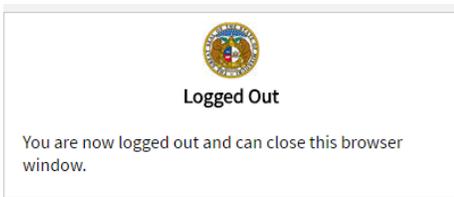


The login form features the same logo at the top. Below it, the text "Login" is centered. Underneath, it says "Log in to read your secure message." followed by an input field for an email address (partially filled with "@gmail.com"), a "Password" input field, and a blue link for "Forgot Password". A blue "Continue" button is at the bottom.

After registering and/or entering their password, the recipient can view the encrypted message as shown below. If the recipient needs to reply or forward the encrypted message, the recipient should click the “Reply” button or “Forward” button located inside the encrypted message under the Missouri State Seal. This will ensure that the reply and/or forward to the message is also encrypted.



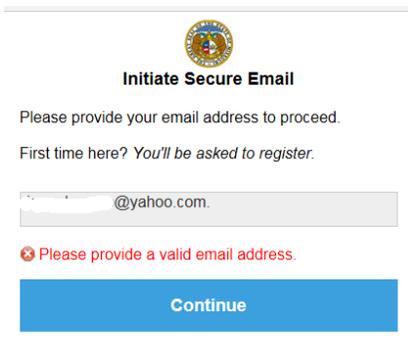
When finished, the recipient should click “Logout” found in the upper right-hand corner of the message. When the user clicks “Logout”, a “Logged Out” message appears on the screen.



Additional Information:

Login ID Case Sensitivity:

The login ID is case sensitive. If the email address is saved in Proofpoint in all lower-case letters it must be entered in all lowercase letters when you try to log in to send an email. If the ID is entered differently than it is reflected in Proofpoint, they will get an error regarding entering a valid Email address.



Active Link:

The “Click here” link in encrypted emails can take up to 30 seconds to be active. If you are trying to open an encrypted email immediately after receiving it, you might receive an error. If you wait just a few seconds and try again, the link should work.

NOTE:

Expiration:

Proofpoint encrypted emails expire after 365 days.