How to Read an Encrypted Email from the PPL Secure Email System

Overview

To protect its proprietary information, PPL Corporation encrypts confidential emails. This is done via PPL's Secure Email System.

The first time you try to read an encrypted email, you have to prove that you're the person for whom the message was intended. This process is called authentication.

System requirements

In order to read an email from the PPL Secure Email System, your system must meet the following requirements:

• You must have a working Internet connection each time you want to read any encrypted message – even a message that you have previously read.

• You must be using a popular Web browser, such as Internet Explorer, Firefox, Google Chrome, Safari, etc.

• Your computer must be able to accept cookies and certificates. If you need help checking or changing these settings, please contact your IT support organization.

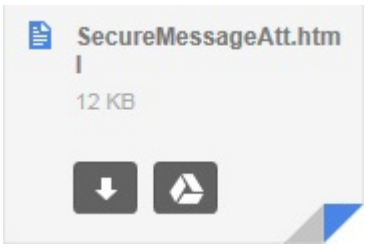
• You must go through a short authentication process to read encrypted emails from PPL. Details on this process can be found in the following section.

First time Users

1. The encrypted email will include the following boilerplate information:

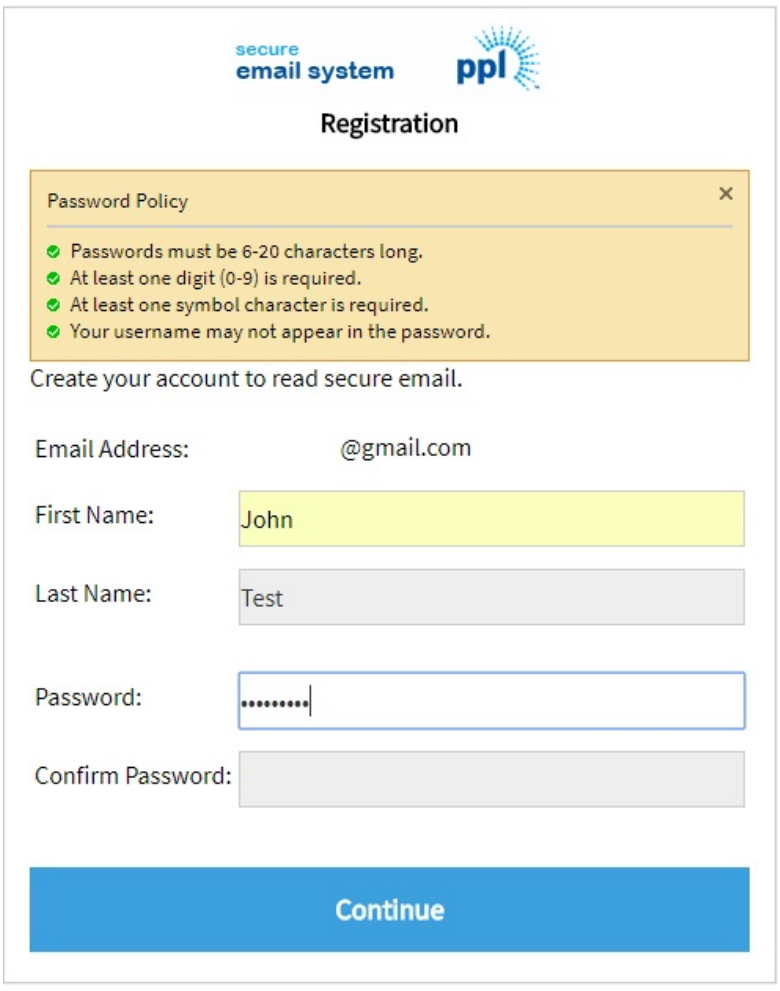
Disclaimer: This system is provided to PPL employees and their authorized clients for business purposes only. To protect the system from unauthorized use and to ensure that the system is functioning properly, administrators monitor this system. Anyone using this system expressly consents to such monitoring, which may include recording by administrators of their access to PPL's system.

2. **Open** the attachment.
    a. The attachment will always be titled SecureMessageAtt.html.

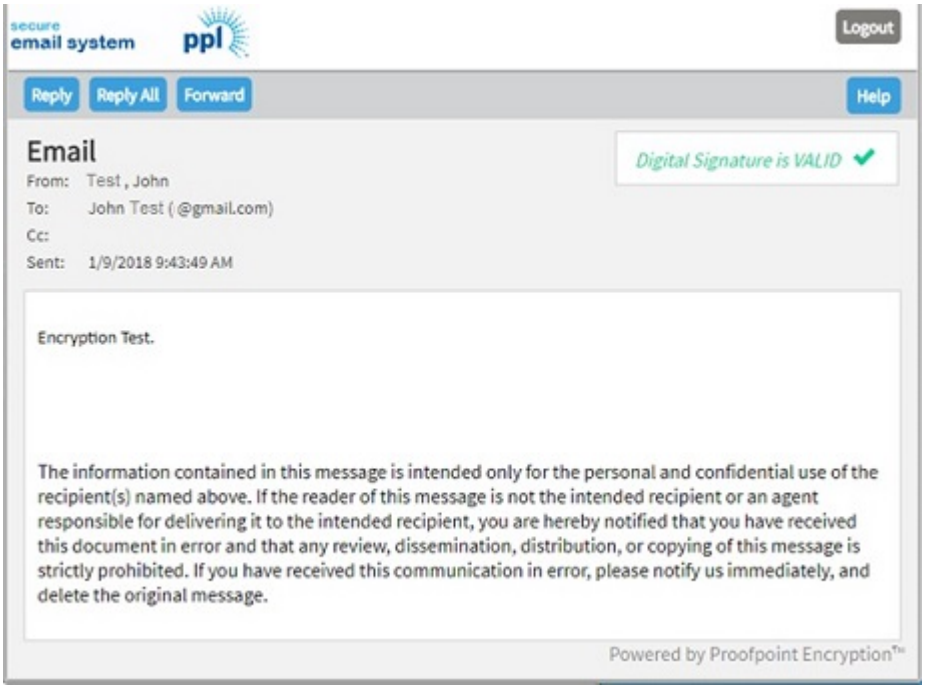


3. Click the **Click to read message** button.

4. **Create** a password for use in the system. Enter your first name and last name in the designated fields. Next, choose a unique password. You will use it to open all secure email from PPL. Click **Continue** upon completion.



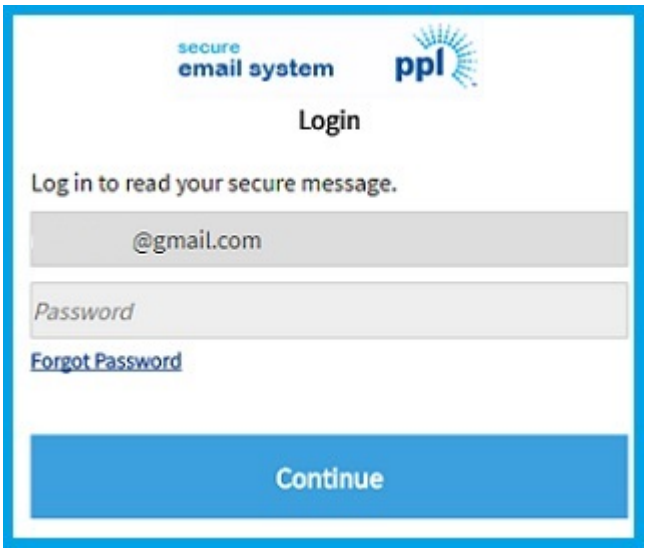
5. The decrypted message will appear in a unique browser window, like the one below.



Note: Authentication is good for 12 hours when the browser window remains open. During that time, the recipient can read all encrypted emails from PPL without having to take any additional steps. After 12 hours, the recipient will have to go through the authentication process again. If the recipient closes the browser window, he or she must also go through the authentication again.

Returning Visitors

1. **Open** the attachment.
    a. The attachment will always be titled SecureMessageAtt.html.
2. Click the **Click to read message** button.
3. Enter **your password** and click **Continue**.

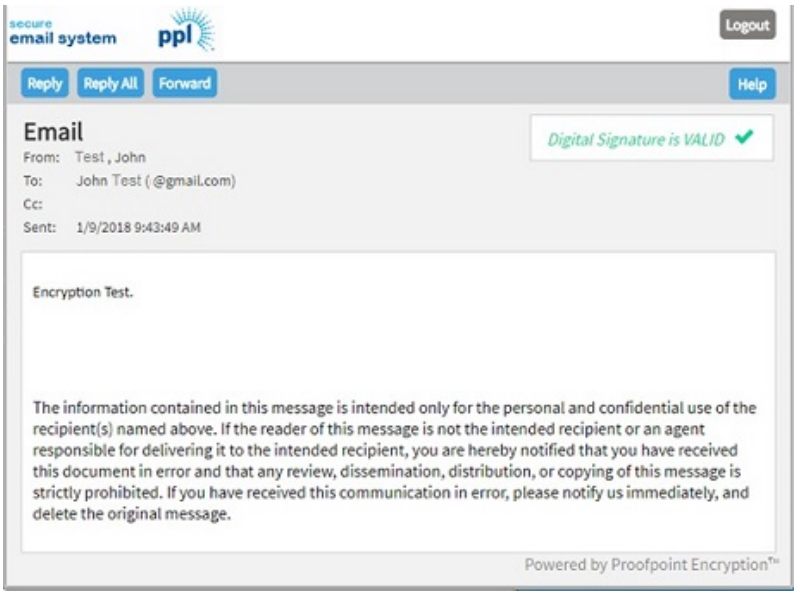


The decrypted message will appear in a unique browser window.

Note: Authentication is good for 12 hours when the browser window remains open. During that time, the recipient can read all encrypted emails from PPL without having to take any additional steps. After 12 hours, the recipient will have to go through the authentication process again. If the recipient closes the browser window, he or she must also go through the authentication again.

Working with the encrypted email

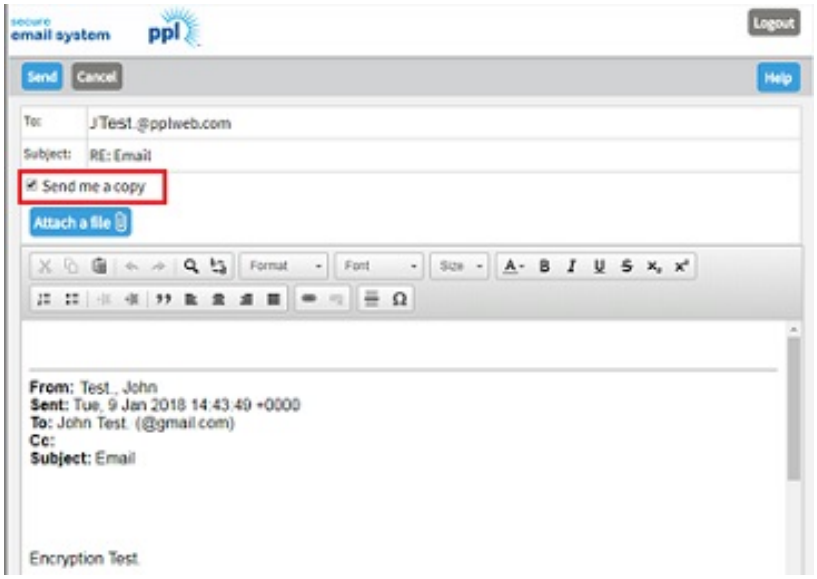
The decrypted email will look similar to the one below. Please reference this example while reviewing the Reply, Forward and Logout information that follows. (In some cases, Internet software will not allow pictures to download. This will not affect the message.)



You can perform many traditional email functions from your decrypted message window. These include the following:

Reply: You can reply to the encrypted message. Your reply will be automatically encrypted. To reply, you must use the Reply or the Reply All buttons in the encrypted message. If you use the "normal" Reply button in the original email before you go through the authentication process, your recipient will not be able to decrypt the message.

You can change, add and remove recipients in the TO: field of the reply. Your email system will **not** save a copy of your reply. If you want a copy of your reply, be sure click Send me a copy.



Forward: You can forward the encrypted message by clicking the Forward button and adding the email addresses of your intended recipients in the TO: field of the new window. The forwarded message and any attachments will be automatically encrypted. If you use the "normal" Forward button in the original email, your recipient will not be able to decrypt the message.

Your email system will **not** save a copy of your forwarded message. If you want a copy of your forwarded message, be sure to click Send me a copy.

Logout: To logout, click the Logout button on the top right hand side of the new window.

Questions?

If you have questions that these instructions haven't answered, please visit http://securemail.pplweb.com/help/enus_encryption.htm.

If you're having a problem reading an encrypted email from the PPL Secure Email System and your system meets the requirements listed above, please notify the sender. Ask the sender to have PPL's IT department investigate the problem.