Proofpoint Secure Email FAQ

Frequently Asked Questions About Secure Email

What is email encryption?

Email encryption is the process of protecting the content of email messages (containing restricted confidential data) from being read by unintended recipients. By leveraging the University’s Proofpoint appliances, which are responsible for scanning for spam and viruses, we are able to provide our users with the ability to send encrypted email whenever necessary.

Why and when should I encrypt email?

Use of UMass Lowell's secure email system is intended to address the need for communicating restricted/confidential data (i.e. PHI) in a safe and secure manner and in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). However, it can also be used to secure other sensitive information including, but not limited to, personal identifiable information (PII), financial or student information. **You are required to use secure email whenever you send a message that contains sensitive information such as PHI or PII to a recipient on the Internet.** For guidance on the types of email that should be encrypted, please review the [Data Classification Policy](#) on the Information Technology website.

How do I get setup to use secure email?

All faculty and staff with a uml.edu email account can use the secure email system. There is no pre-registration or setup required.

Faculty and staff who use the Proofpoint secure email system should consider sending a [pre-notification email](#) or letter to potential recipients before sending them their first secure email. This will alert them that you will be using secure email to communicate with them and explain how they can correspond with you in a secure manner. Please note that, if you send the pre-notification message via email, you should send it as a normal, non-secure email.

Do I need special software on my computer to send a secure email?

No special software or installation of software is required or needed. However, a very helpful Outlook plugin, the “Send Securely”, button is available for download to simplify the process. The plugin can be downloaded from apps.uml.edu,

Who will decide if my mail is encrypted?

Based upon the content you are sending; you make the decision about whether or not an email will be encrypted. The email you send will only be encrypted if you [follow these steps](#).

How do I encrypt messages?

To send an encrypted email using the secure email system, you simply need to add "[secure]" (without quotes) to the subject line of the email or use the "Send Securely" button within Outlook. (This assumes
you have downloaded and installed the Proofpoint Secure Email Plugin). Be sure to include the brackets but do not include the quote marks. Here are some examples of subject lines that will trigger the message to be sent encrypted:

[secure] Confidential Spreadsheet
Confidential Spreadsheet [secure]
Confidential [secure] Spreadsheet

** NOTE: The subject line of the email is not encrypted; therefore, you should not include sensitive information in subject line of the email.

Can recipients reply to my messages securely?

Yes, recipients of your secure messages can reply securely by accessing the URL or attachment in the email they receive. Their reply to your email will be automatically decrypted by the secure email system and will appear in your Exchange mailbox as a normal, readable email. The process is seamless and the only indication that the message was originally encrypted will be the "[secure]" in the subject line.

Can business associates outside UMass Lowell initiate secure messages to me?

No, third parties cannot initiate an encrypted communication using UMass Lowell’s secure email system. The initial email must be sent by someone (using the ‘secure’ method) within the UMass Lowell community and then the recipient can reply to that email in a secure, encrypted manner.

How will secure mail recipients receive encrypted messages?

Recipients of a secure email from UMass Lowell will receive a notice in their email inbox that they have received a secure message from you. The message will contain an encrypted attachment or URL, which when opened, will take you to the secure email server. The first time the recipient receives a secure message, they will be asked to create a passphrase that will be used to view or reply to their secure messages. After logging in with their self-assigned passphrase, the recipient can then view the email and use the "Reply" button to reply to the message.

How long is a secure message available to the recipient?

Encrypted emails will be available to the recipient for 7 days from the date sent.

Can I send a message while I travel?

Yes, you can send secure messages using the Outlook web access page located at https://exchange.uml.edu. This website provides most of the functionality of regular e-mail on campus. Again, an email will not be encrypted unless you place "[secure]" in the subject line.

Is the subject line of the message encrypted?

The subject of the email is not encrypted; therefore, you should not include sensitive information in the subject line.

Can I send attachments?

Yes, the total size of attachments you send must not exceed 15 megabytes.
How can I make sure my messages are being encrypted? Can I test the system?

We encourage you to familiarize yourself with the system by sending secure messages to your home e-mail address or business associate that you would like to communicate with securely. It will be very easy to tell if the message was encrypted because recipients will have to register their email address and use a password to access the message.

What will happen if I attempt to encrypt an email to someone with a UMass Lowell email address?

Email sent within the UMass Lowell Exchange email system is secure, and it is permissible to include protected health information (PHI) or Personal Identifiable Information (PII) in e-mail from one UMass Lowell email address to another UMass Lowell email address. Therefore, email sent with "[secure]" in the subject line to someone with an "@uml.edu" address will not be encrypted using the Proofpoint secure email system and will be sent just like any other email. Only email sent to a recipient on the Internet will be encrypted.

Can anyone use the secure email system?

Yes, anyone with an @uml.edu email address can use the secure email system. However, use of the system should be limited to those individuals with a need to exchange protected health information (PHI), personal identifiable information (such as social security numbers, credit card, bank information, etc.) or other sensitive financial, legal or research information with others over the Internet. **The secure email system should not be used for personal business.**

Will I be able to read the secure message on my smartphone?

 Mostly-yes. However, some smartphones cannot download files or modify HTML files. The secure message is sent as an HTML attachment, so it is possible that you may not be able to read it on your smartphone.

What happens if I forget the password I set on the Proofpoint Encryption window during registration?

If you forget your password you set during the Proofpoint encryption registration, you can click the “Forgot Password” link. A password reset message, with two challenge and response questions, will be sent to the email address you had registered. Please click the link in that message to reset your password.

Who should I contact if I have questions about secure email?

Faculty and staff with questions about secure email that are not covered by this FAQ, should contact the University IT Service (help@uml.edu or 978-934-HELP for additional assistance.)