

## Introduction

Unencrypted email is not a secure method for transmitting confidential information or sensitive data over the Internet. If you have reviewed the information below and determined that it is necessary to send such information, take steps to secure it by encrypting your message, taking into account the sensitivity of the data being transmitted and the level of security at the source and destination systems.

At Long Island University, do not send sensitive data via email unless:

- It is required by your role within the university and you've reviewed your role within the university.
- You've reviewed **Choosing an Appropriate Storage Solution** for more secure alternatives.
- The message either:
  1. is encrypted by the Cisco Registered Envelope Service (CRES) and you've reviewed **Sensitive Data Sent Outside Long Island University**, or
  2. stays within the LIU email systems (Microsoft Exchange; not LIUmail) and you've reviewed **Sensitive Data Sent Within Long Island University**.

## Your role within the university

You should only send sensitive data via email if it is absolutely required in order to conduct the business function of the university. If you are unsure whether email is appropriate for a particular situation, consult with the university Data Steward in charge of the data involved, as well as with the University Information Policy Office.

### Sensitive Data Sent Outside Long Island University

Microsoft's **Office Mail Encryption (OME)** allows for encrypted email to be sent from LIU mail servers to recipients outside the LIU network. While all outgoing mail is scanned for sensitive data, you should always force encryption of messages you know to contain such information. The receiving party will need to authenticate their identity to read the message.

### Sensitive Data Sent Within Long Island University

Encrypted mail sent from one LIU Outlook account to another allows for a seamless experience. Users will not need to log in or verify their identity once they are logged into their Outlook email.

## Guidelines

As you are aware, data breaches are in the news nearly daily. We at LIUIT want to remind all of you of the urgency and necessity to refrain from sending sensitive information through emails. As a reminder, university policy prohibits Personally Identifying Information (PII) including but not limited to the examples below from being communicated via email:

- Social security numbers
- Academic student information
- Date of birth, address, and bio-demographical information
- Credit card and debit card information
- Passport information
- Driver's license and state ID information
- Healthcare related information

There are secure methods for receiving/sending sensitive information containing PII data. In the event that data of this nature must be transmitted via email, please contact your local Information Technology office for more information on secure methods available.

As a precaution, the university has implemented a Data Loss Prevention (DLP) protocol to prevent the possibility of inadvertently sending sensitive information out. Here are some illustrations of this new product that has been turned "on".

A screen will appear in Outlook if you attempt to send an email that is determined to contain sensitive data.

If the DLP system mistakenly flags an email as containing sensitive data in error, you can override the policy by clicking the override link.

You must provide a reason for this override in the field provided. These will be reviewed by our Information Technology security team and you will be contacted to discuss the override at a later date. Information Technology takes security of all LIU information systems, assets and data very seriously. As is the case with any new solution, there may be unforeseen issues that may arise. Please communicate with us and let us know how the process is going for you.

For more information about IT security best practices, policies, and your IT services visit [it.liu.edu](http://it.liu.edu).

## Sending Encrypted Email

To send encrypted email to non-LIU email addresses all you have to do is put the **[encrypt]** tag in the subject of your email. This works for liu.edu emails only.

## Receiving Encrypted Email

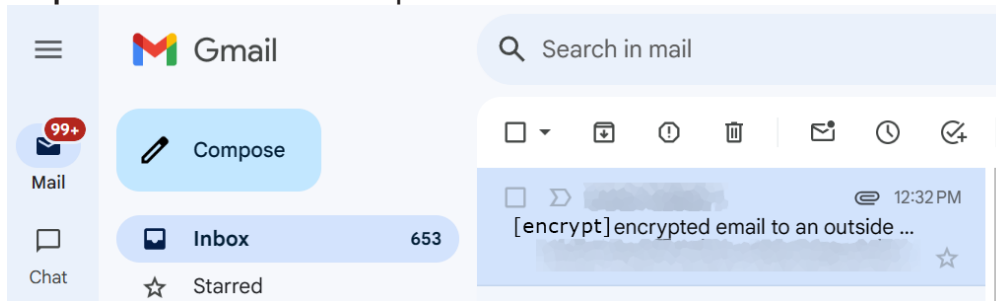
-Outlook: Your experience will be seamless and no action needs to be taken. The encrypted message

# LIU Email Encryption

will open and simply display a message stating that the email is encrypted.

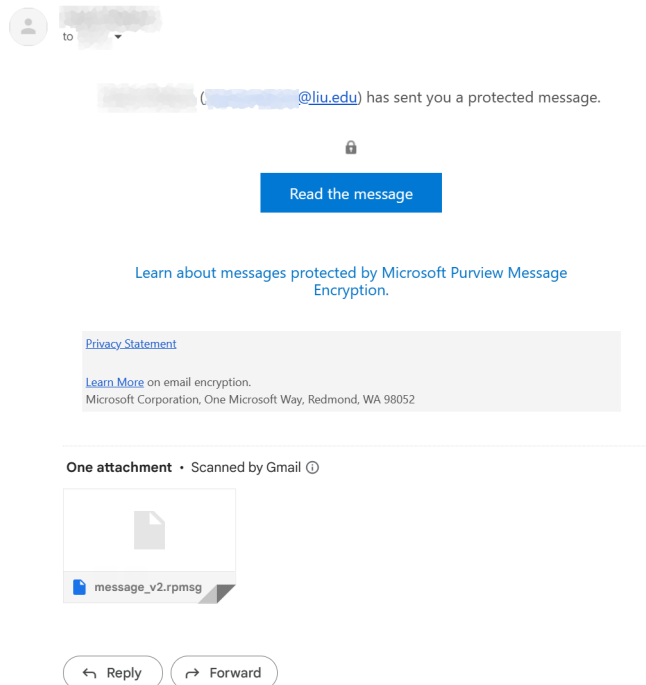
- **Gmail/Yahoo:** Upon clicking the email, you will be able to log in using your Gmail or Yahoo account as authentication to read the email.
- **Other Email services:** Upon clicking the email, you will have the option to use a One-Time-Passcode (OTP) for authentication. You will be emailed a code to enter and open the encrypted email.

## Step 1 – click the email to open it



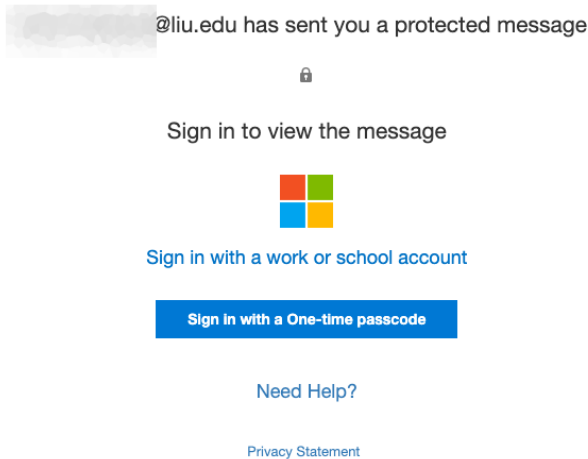
## Step 2 – Click on the “Read the Message” Button

[encrypt] encrypted email to an outside email ▾ Inbox x



# LIU Email Encryption

## Step 3 - Select "Sign in with a One-Time Passcode"



## Step 4 - Once you reached this screen, check your mail again for the passcode

We sent a one-time passcode to [redacted]@my.liu.edu.

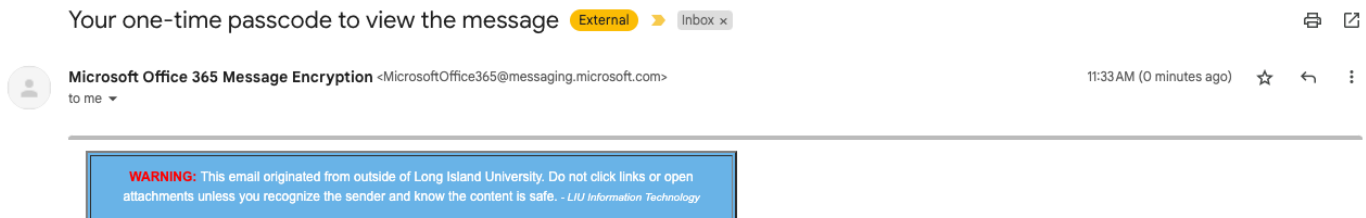
Please check your email, enter the one-time passcode and click continue. The one-time passcode will expire in 15 minutes.

One-time passcode

This is a private computer. Keep me signed in for 12 hours.

[Continue](#)

Didn't receive the one-time passcode? Check your spam folder or [get another one-time passcode](#).



To view your message, enter the code in the web page where you requested it.

NOTE: This one-time passcode expires 15 minutes after it was requested.

This message is automatically generated. Please don't reply to it.

## Step 5 - Enter the code and click "Continue" to read the Encrypted Message

We sent a one-time passcode to [redacted]@my.liu.edu.

Please check your email, enter the one-time passcode and click continue. The one-time passcode will expire in 15 minutes.

One-time passcode

This is a private computer. Keep me signed in for 12 hours.

 Continue

Didn't receive the one-time passcode? Check your spam folder or [get another one-time passcode](#).

## [encrypt] encrypted email to an outside email



Encrypt: This message is encrypted. Recipients can't remove encryption.

## Secret message

