Information Technology Services
http://www.lander.edu/its
help@lander.edu
864.388.8234

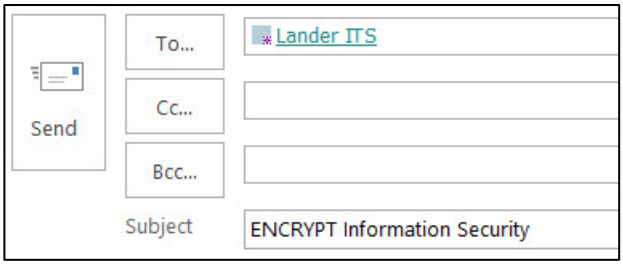
Email Encryption Instructions

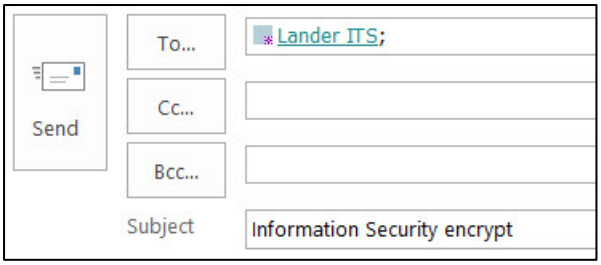
Do you need to send confidential information through email? While that should be avoided if possible, ITS has set up a simple encryption solution to protect any sensitive information transmitted through an email or email attachment. Available on all Lander email accounts, this feature can be used to send encrypted mail to both Lander and non-Lander accounts.

Note: This solution does not protect against sending an email to the wrong individual, so please ensure that you are entering the intended recipient's correct email address before sending.

How to Send an Encrypted Email

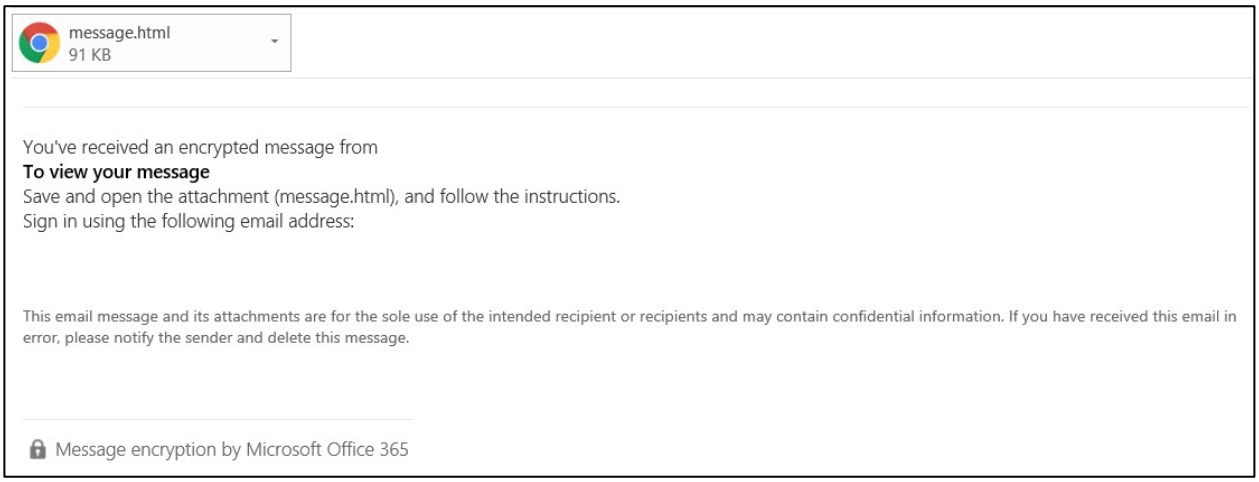
1. Type the word "encrypt" anywhere in the subject line. While proper spelling does matter, capitalization does not, so feel free to use any variant of "encrypt" (ENCRYPT, Encrypt, encrypt, etc.).
2. Verify that you are sending the email to only your intended recipient(s), and click "Send".





How to Open an Encrypted Email

If you receive an encrypted email, it will specify the sender and contain an attachment named "message.html" along with instructions on how to view the message.



1. Verify that you know the sender.
2. Click the drop-down arrow on the right side of the “message.html” attachment, and choose “Save As” (Outlook application) or “Download” (Office 365 online).
3. Open the downloaded “message.html” file. This will launch a webpage in your default browser.
4. From the “Encrypted Message” page, select “Sign in” and then choose “Work or school account”.
5. The next page will automatically fill in your Lander email address, so enter your email password and click “Sign in”.
6. You will now have access to the contents of the encrypted email, including any attachments.

When Should I Encrypt?

Required:

Any email or email attachment that contains personally identifiable information (PII), nonpublic personal information (NPI), protected health information (PHI), or any other sensitive data collected from students or employees must be encrypted. Examples of sensitive information include:

- Social Security numbers
- Medical records
- Driver’s license or other state identification card
- Banking information (account numbers, credit card numbers)
- Any student records not classified as “directory information”

Before sending an encrypted email containing sensitive information, ask yourself:

- Are all of the data fields necessary to complete the current process? If the task does not require SSNs, remove that field from your report before including it in the email.

- Can any sensitive information be masked or abbreviated? Include the least amount of information possible (for example, reveal only the last four digits of SSNs or credit cards).

- Do all recipients of the email have a legitimate business need to access the information sent? If replying to a conversation with multiple participants, only include recipients who actually need to access or handle the data to complete the specific task.

Recommended:

While many scenarios do not require encryption, ITS recommends securing any emails containing information that the sender or recipient would prefer to keep private, such as résumés or performance evaluations.