Valdosta State University

Email Encryption

Securing the University's digital information, including information communicated through email, is a priority for the Division of Information Technology. This document is intended to help you understand the importance of encryption and how to encrypt your emails that contain sensitive and personally identifiable information (PII).

Learn to Encrypt your Email Messages:

1. Why do you need to encrypt email
2. How to encrypt email
   - Office 365 Outlook Web Client
   - Do Not Forward and Encrypt Messages

For additional assistance:

Contact VSU Solutions Center:
229-245-4357 or solutions@valdosta.edu
www.valdosta.edu

VALDOSTA STATE UNIVERSITY

Why do you need to encrypt email

With very little information, an attacker can create false accounts, steal identities, and perform other malicious acts using personally identifiable information (PII). Personally Identifiable Information is data that could be used to identify a specific individual. Any two or more pieces of identifying data communicated together are also considered PII. Examples of PII that incorporate sensitive data include but are not limited to the following:

- Full name
- Birthdate
- Birthplace
- Social Security Number or Driver's license
- Student/employee identification number, or any other personal ID number
- Financial account number or credit card number
- Regulated Information: Medical Information (HIPAA data), Employment Information, Student Records (FERPA data).

By default, email is sent as unencrypted text so that it can be read by anyone—including those who are not the intended recipients. As such, 'regular' email messages that contain PII are vulnerable to being hijacked for malicious intent.

To protect student and employee personally identifiable information, emails that contain sensitive information should be encrypted.

Encrypting an email causes the readable plain text to be converted into scrambled cryptic text ***while in transit*** to the intended recipient. Upon delivery, the recipient can read the message as normal. The encryption cannot be removed by the recipient, even if the message is forwarded.

Optionally, the sender can select the '**Do Not Forward**' restriction that will not allow the intended recipient to forward the message to a different recipient; however, the message is not encrypted.

Note: It may take a few additional seconds when sending an encrypted message. A status notification will appear when applicable.

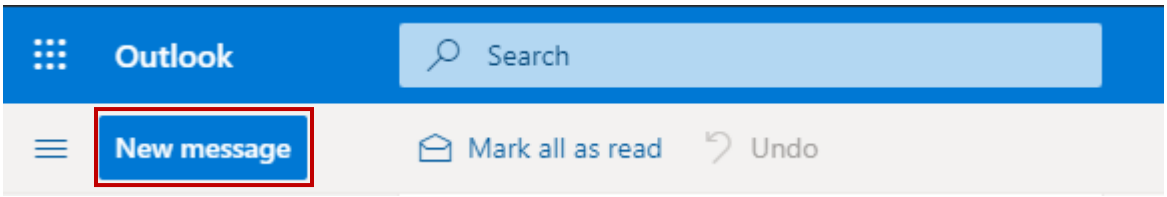
[Top of Page]

How to encrypt email

Encrypted emails must be sent and received through VSU Office 365 Web Client. Currently, the encryption function is not available through VSU Outlook desktop application.

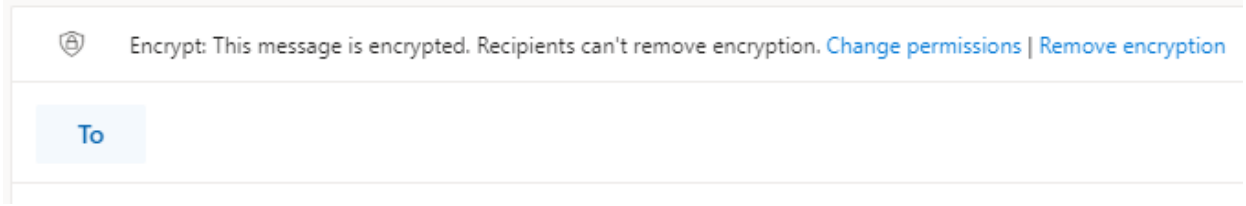
To access Office365 Web: Log in to **MyVSU** > Click the **Email** button located in the top, right section of the page.

1. Click **New Message** to create email.



2. Before composing the email, click the encrypt button.

A banner will appear that reads: *Encrypt: This message is encrypted. Recipients can't remove encryption.* **Write your email message and Send as normal.**

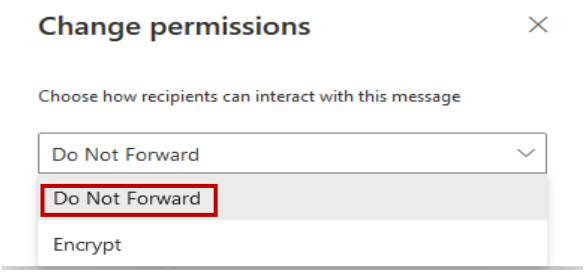


Note: Click the **Remove encryption** link within the banner to disable this function if desired.

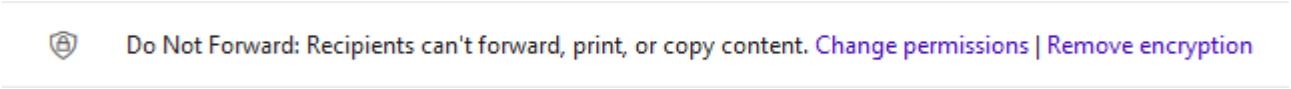
[Top of Page]

To enable the **Do Not Forward** function only without encryption:

1. Within the encryption banner, click the **Change Permissions** link > Select **Do Not Forward** from the dropdown menu > Click **OK**.



A banner will appear that reads: *Do Not Forward: Recipients can't forward, print, or copy content.*



2. **Write your message and Send as normal.**

Note: Click the **Remove encryption** link within the banner to disable this function if desired.

If the recipient attempts to forward the message, a notification appears stating *"You cannot perform this action. Permission to this message is restricted."*

[Top of Page]