

# Sending and Receiving [secure] Encrypted Emails

UMB faculty, staff and students have the ability to send encrypted emails by simply adding [secure] to the subject in an outgoing email. When sending any confidential information (PHI, PII, credit card information, etc), it is strongly recommended to use this method to ensure that only the recipient can view the information.

### Sending a [Secure] email

To encrypt a message, add [secure] to the beginning of the subject line. Be sure to include the brackets and add a space after:



Note: Once sent, the message will not appear as encrypted in the Sent folder. To verify and track encryption, it's recommended to CC yourself.

### Receiving a [secure] email – Internal Recipient

For recipients who are internal to UMB and are using the Outlook client, Outlook mobile client or the Outlook web interface, the email will look similar to the following:



The email can be opened, read, and replied to as usual. Encryption cannot be removed by the recipient. The email will continue to be encrypted when replying/ replying to all.

If the recipient is using a 3<sup>rd</sup> party mail client (such as Apple iOS built-in mail client), they will likely need to verify themselves as external recipients will need to. See Pg 2, Receiving a [secure] Email – External Recipient.



#### Receiving a [secure] Email – External Recipient

These steps are using Gmail but will be similar to other providers.

• Once the message is received, click **Read the message**.

UNIVERSITY & MARYLAND BALTIMORE		
Steinberg, Sarah ( <u>sesteinberg@umaryland.edu</u> ) has sent you a protected message.		
<u>A</u>		
Read the message		
Learn about messages protected by Office 365 Message Encryption.		
Privacy Statement		
Email encryption powered by Office 365. <u>Learn More</u> Microsoft Corporation, One Microsoft Way, Redmond, WA 98052		

Using Gmail as the example, at this point, there are 2 options – "Sign in with Google" or "Sign in with a One-time passcode". Providers such as Google, Yahoo, and Outlook.com are trusted by Microsoft and the recipient can select *Sign in with Google* and will be able to view the message.

All providers will offer "Sign in with a One-time passcode" and some will offer only this option. To use this option:

• Click Sign in with a One-time passcode.

NOTISETTY MARILAND		
sesteinberg@umaryland.edu has sent you a protected message		
<u>ê</u>		
Sign in to view the message		
G Sign in with Google		
Sign in with a One-time passcode		
Need Help?		
Privacy Statement		

• A one-time passcode will be sent to the recipient's email address, as noted below:

Lovision Annual Viela		
	We sent a one-time passcode to steinberg.sarah @gmail.com.	
	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.	
	Ocntinue	
	Didn't receive the one-time passcode? Check your spam folder or get another one-time passcode.	

# **Encrypted Emails**



The email will appear "from" Microsoft Office 365 Message Encryption and will include the one-time passcode, as shown below:



• In the passcode window, enter the given passcode into the **One-time passcode** field and press **Continue**:

UNIVESITY/MARIAND MATIMORE	
	We sent a one-time passcode to steinberg.sarah @gmail.com.
	Please check your email, enter the one-time passcode and click continue. The one-time passcode will expire in 15 minutes.
	One-time passcode  94595837  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 <u>get another one-time</u> passcode.

The email contents will now be visible in the browser window and can be viewed, replied to, and downloaded. Encryption cannot be removed by the recipient. The email will continue to be encrypted when replying/ replying to all.

## **Requesting Sensitive Information From External Users**

If a UMB employee needs to request sensitive information from an external user, by sending a [secure] email to the recipient, their reply and any sensitive data will automatically be encrypted. This process works too in situations where it is known that an external user doesn't have access to an encryption tool. Any replies to a [secure] email that is initiated by UMB will remain encrypted.