MIAMI INFORMATION TECHNOLOGY

# SecureMail FAQs


| | |
|---|---|
| Point Solutions - Support | Gables One Suite 1100 |
| UMIT Helpdesk | (305) 284-6565 |
| Technical Support Email | itsupportcenter@miami.edu |

# Contents

# SecureMail FAQs

## Basics

**What is an address "outside UM?"**
Any address that does not end in miami.edu is considered an outside address. There are also some email systems within the University, maintained by particular schools or departments, that are not yet part of the encryption process and so are considered outside. Some examples are Rosenstiel School (RSMAS), School of Law and School of Business.

**What content is "sensitive" enough to require encryption?**
In general, you should consider any information about the operations of the University to be sensitive, whether it involves clinical, research, educational or administrative activities. Health, education or financial information that is associated with identifiable persons is considered particularly sensitive, and protected by federal and private requirements (e.g., FERPA, GLBA, HIPAA, PCI).

You can read the UM Data Classification Policy for guidance on data sensitivity. If you're not sure about what qualifies as sensitive data in your work environment, ask your supervisor.

**How does this system know an outbound message has CCNs, MRNs, or SSNs?**
The encryption utility examines each outbound message, scanning for patterns of numbers and words that, according to its rules, suggest such content. This is similar to how the spam utility inspects inbound messages for suspicious content.

**UMail emails are encrypted, but do I need to encrypt email that goes to a UM address at another campus?**

This is a harder question. In general, UM addresses are safe destinations because email is encrypted as it travels between campuses and within the major UM email systems. However, not all UM email systems are encrypted. Also, many people use @miami.edu email aliases that forward email to external systems.

As a general rule, if the information seems particularly sensitive, encrypt it until you can confirm that the address at the other campus is secure**.**

**What about email traveling to other health or education facilities?**
In general, any message with sensitive content that is going to an external address should be encrypted.

# How-To

**What do I need to do to secure my email?**

| | | RECIPIENT | | | |
|---|---|---|---|---|---|
| | | **Office 365** | **Med** | **Other UM*** | **Outside+** |
| **SENDER** | **Office 365** | No action required | No action required | Action required* | Action required+ |
| | **Med** | No action required | No action required | Action required* | Action required+ |
| | **Other UM*** | N/A | N/A | N/A | N/A |
| | **Outside+** | N/A | N/A | N/A | N/A |

- *Rosenstiel School (RSMAS), School of Law, School of Business, et cetera* – see question "How do I tell Email Privacy that I want a message encrypted?"

+ *Gmail, Yahoo, AOL, et cetera* – see question "How do I tell Email Privacy that I want a message encrypted?"

**How do I tell SecureMail that I want a message encrypted?**

Insert "[secure]" in the subject line, without the quotes, as in the example to the right. Any recipient with an address external to UMail or Med will receive an encrypted copy of that message.

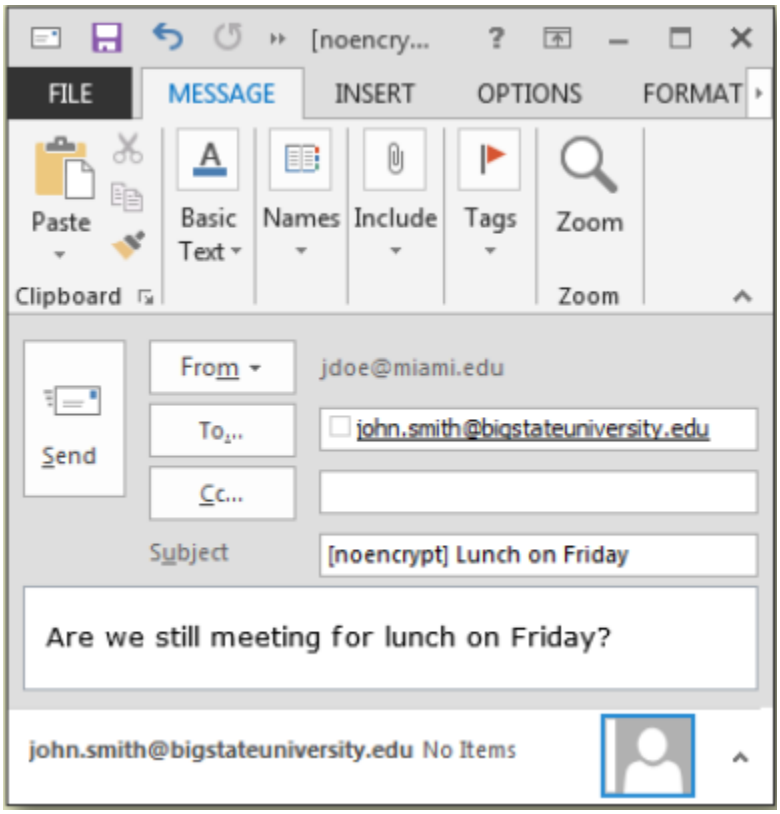
Note that this addition to the subject line has no effect for recipients with UMail or Medical Campus Exchange accounts. Encryption occurs automatically for them (but transparently, so you don't notice it).

**How will I know that encryption of my email has occurred?**

You will receive an email notification message indicating that an outbound message has been encrypted, and indicating the recipient(s) for whom it has been encrypted. You will also receive an email notification when any recipient opens an encrypted message.

**How do I tell SecureMail that I do not want a message encrypted?**

Insert "[noencrypt]" in the subject line, without the quotes, as in the example to the right. This will guarantee that the email will not be encrypted and that all recipients will be able to open the message as they would a regular email.




**Please Note:** You will be assuming responsibility for certifying that the transmission **does not** contain sensitive/personal information.

**What do recipients have to do to "un-encrypt" my message?**

The first time a correspondent receives an encrypted email from the UMail system, they will have to register their email address with the Email Privacy service, a process that includes creating an access password. For subsequent messages, the recipient will have to enter the password to un-encrypt.

Most people find the un-encrypt process easy, but not everyone. You can refer correspondents to UMIT Service Desk for additional information..

# Registering Email Addresses and Systems

**How many email addresses can I register with SecureMail?**
SecureMail only allows for the registration of one (1) email address per person.

**Do I need to make any changes to my email system to support SecureMail?**
It depends. If your users are only recipients of a secure envelope, then no change is necessary. Your email system continues to send email as normal. If your users need to send secure messages using SecureMail, then your email server will need to use the SecureMail as a smarthost. You may contact IT Security for additional information.

**How do I register my email system to use the IronPort smarthost?**
You must complete the online form. To access the form, you will need to provide your @miami.edu address on the Office 365 login screen. Press Tab on your keyboard and you will be redirected to our Single Sign-On page. On the Single Sign-On page provide your and your CaneID password.

Please contact itsupportcenter@miami.edu if you have any problems accessing the form.