How to Recognize Phishing Emails Targeting the University of Mary

For the past several years, University of Mary has been targeted by phishing emails. It is important that you recognize these scams so your UMARY account is not compromised.

What is Phishing?

Phishing is the criminal practice of attempting to trick someone into giving away personal information by masquerading as a trusted source.

University of Mary has been the target of phishing emails for several years. These phishing emails are designed to *look* like they are from the University. They attempt to trick you into giving away your UMARY account information (i.e. your UMARY username and password).

Never send your password in email!

University of Mary will NEVER ask you to send your password in email.

Some phishing emails ask you to "verify your account" by replying with your UMARY user name and password. In reality, if you send your password in email, you are giving it to the phishing scammers.

Be cautious when asked to log in with your UMARY username and password.

Be suspicious of emails that ask you to "log in" to verify your account.

Some phishing emails include links to websites where you are asked to log in. The idea is that by logging in, you are "verifying your account" so that you don't lose it. In reality, the website is a fake, just like the email. It might even *look* like a real University of Mary website, but when you "log in" you are really sending your UMARY username and password to the phishing scammers.

What should I do if I got phished?

If you replied to a phishing email and sent your UMARY username and password, you should change your password and security question immediately.

Likewise, if you clicked a link in a phishing email and "logged in" to the associated website, you should change your password and security question immediately.

How to Recognize Legitimate vs. Phishing Emails

In order to better help the end user identify legitimate emails from the IT staff or technology department as a whole, IT now uses digitally signed emails. There are slight differences between users who use Outlook and users who use Outlook Web Access. (http://mail.umary.edu)

Screen shots at the end of this document to showing various legitimate and phishing emails.

Look at the many parts of an email or website to help you decide if it's legitimate or a fake.

Subject Lines

Here are some example subject lines from phishing emails sent to University of Mary:

- "IT Services Desk - Dear Staffs/Students."
- "E-Mail Account Maintenance"
- "WebNews / Web Email Account Update"
- "Confirm Email Account"

From: Addresses

Check the From:, Reply-To:, and Sender: address in emails you receive. Official University of Mary emails are usually sent From: (and, if visible, have Reply-To: and Sender:) email addresses that end with **@umary.edu**.

Occasionally, University of Mary will send official emails from non-UMARY email addresses. One example is **it@collegevote.com**, which is the official UMARY online survey / evaluation company and **umary@supportcenteronline.com**, The email address used buy our UMARY helpdesk. This can make it more difficult to determine if an email is real or fake. When in doubt, contact the Help Desk for assistance in verifying the authenticity of an email before you act on it.

Here are some example From: and Reply-To: addresses from **phishing emails** sent to Illinois State:

- info**@itservices.net**
- support-team**@web.nl**
- webmail**@mail.zinnianet.net**
- lolata**@sercomtel.com.br**
- helpdesks**@inmail24.com**

Email Message

Look for suspicious phrases like these:

- "Verify your email address or your account will be deactivated."
- "Upgrade your account."
- "Confirm your email account."

University of Mary will never ask you to verify or confirm your account in this way.

Web Addresses

Check the web address of any website that asks you to log in or enter personal information.

The domain name portion of official University of Mary websites usually ends with **umary.edu**. Occasionally, University websites will not conform to standard University of Mary domain names, which can make it difficult to tell if the site is real or fake. When in doubt, contact the Help Desk for assistance in verifying the authenticity of a website before logging in.

The domain name portion of a web address is included in the first part of the address before any slashes.

- **Example #1:** In the web address, video.google.com, **google.com** is the domain name.
- **Example #2:** In the web address, www.att.net/wireless, **att.net** is the domain name portion of the address.

Here are some examples of authentic web addresses for the University of Mary:

- www.**umary.edu**
- my.**umary.edu**/ics
- bookstore.**umary.edu**/home.aspx
- d2.parature.com/ics/support/default.asp?deptID=8302 (This one is different, this is the University of Mary’s Help Desk hosting company)

Here are some examples of web addresses for fake university sites:

- www.umary.**web.org**/umary
- www.umary.**itservices.org**
- www.**itnews.com**/umary-helpdesk
- www.**support-umary.edu** (This one is tricky, but **support-umary.edu** is not the same as the official **umary.edu**.)

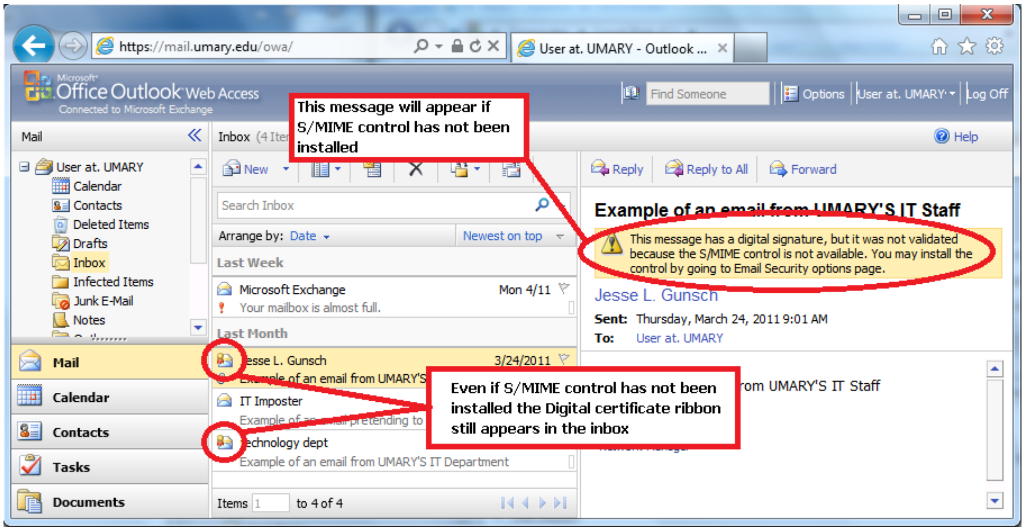
Get Help First

If you receive an email or visit a website that threatens to remove your account or makes you suspicious for any reason, contact the University of Mary Help Desk to discuss the situation. The Help Desk can help you determine if the message or website in question is legit or a phishing scam. You should get help before following the instructions.

Outlook Web Access

Outlook web access will show the digital certificate ribbon in the main inbox screen but may show a warning in the email itself if you have not installed S/MIME controls. You can install S/MIME controls by doing the following.

- Click Options in the upper right hand corner
- Click E-mail Security on the menu on the left
- Click install the Outlook Web Access S/MIME control



This message will appear if S/MIME control has not been installed

Example of an email from UMARY'S IT Staff

This message has a digital signature, but it was not validated because the S/MIME control is not available. You may install the control by going to Email Security options page.

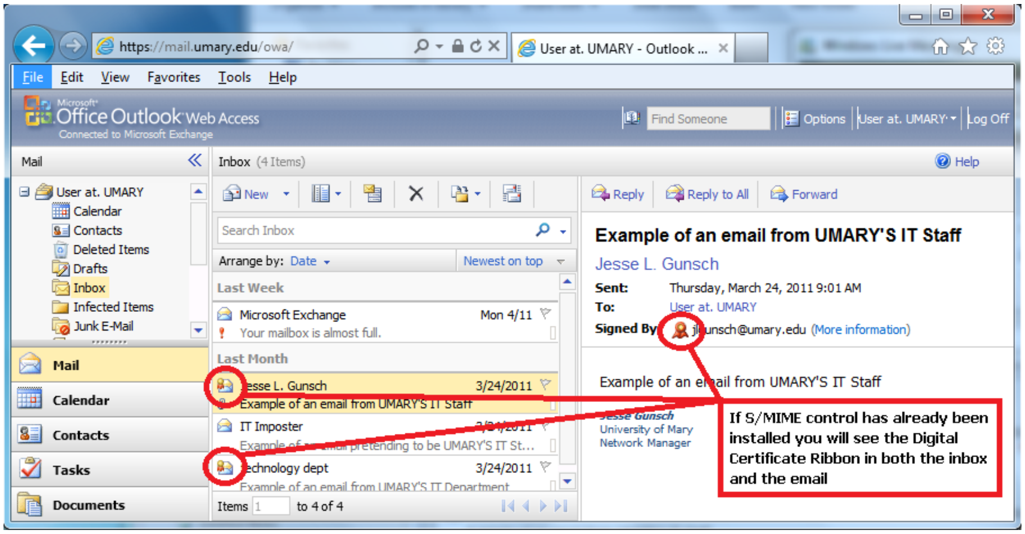
Jesse L. Gunsch

Sent: Thursday, March 24, 2011 9:01 AM

To: User at. UMARY

Even if S/MIME control has not been installed the Digital certificate ribbon still appears in the inbox

After S/MIME has been installed



Example of an email from UMARY'S IT Staff

Jesse L. Gunsch

Sent: Thursday, March 24, 2011 9:01 AM

To: User at. UMARY

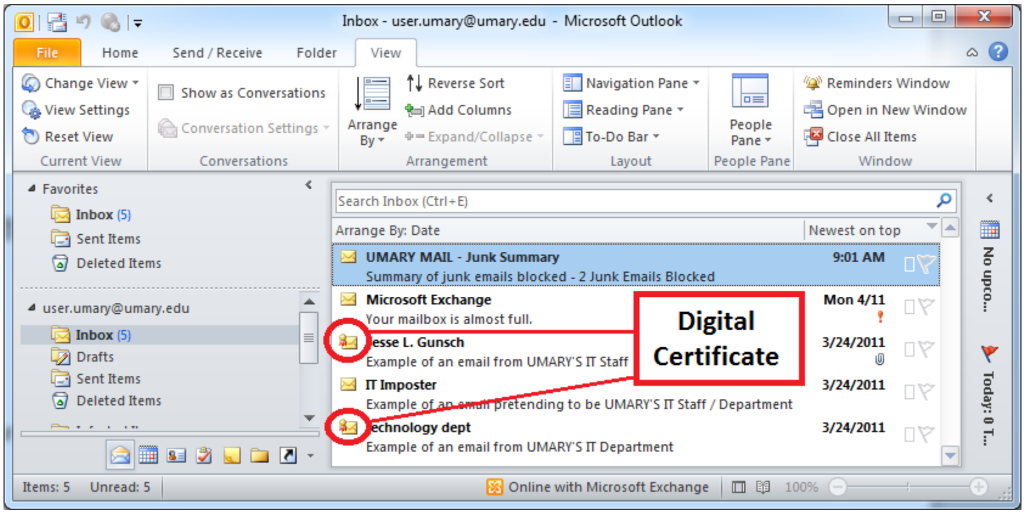
Signed By: jgunsch@umary.edu (More information)

Example of an email from UMARY'S IT Staff

Jesse Gunsch
University of Mary
Network Manager

If S/MIME control has already been installed you will see the Digital Certificate Ribbon in both the inbox and the email

Legitimate email examples



UMARY MAIL - Junk Summary 9:01 AM
Summary of junk emails blocked - 2 Junk Emails Blocked

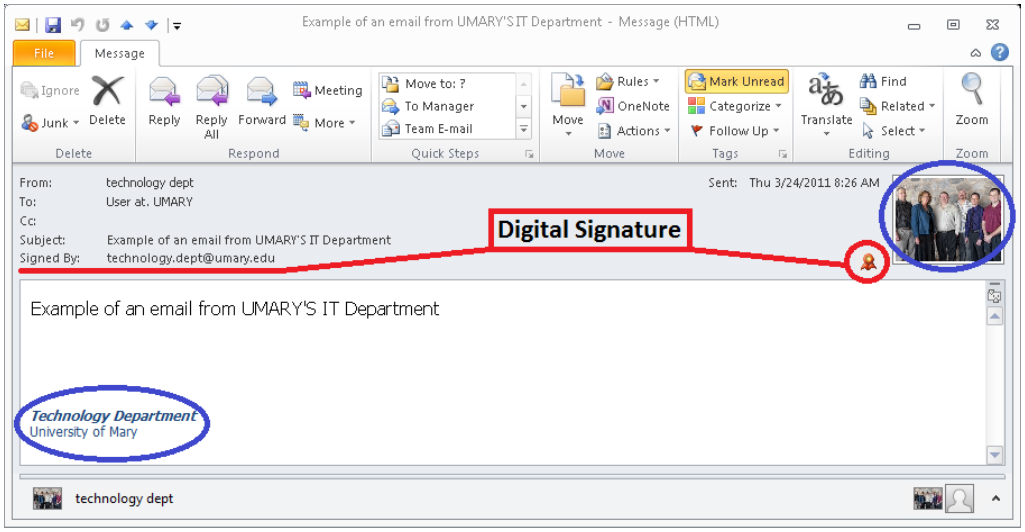
Microsoft Exchange Mon 4/11
Your mailbox is almost full.

Jesse L. Gunsch 3/24/2011
Example of an email from UMARY'S IT Staff

IT Imposter 3/24/2011
Example of an email pretending to be UMARY'S IT Staff / Department

Technology dept 3/24/2011
Example of an email from UMARY'S IT Department

Digital Certificate



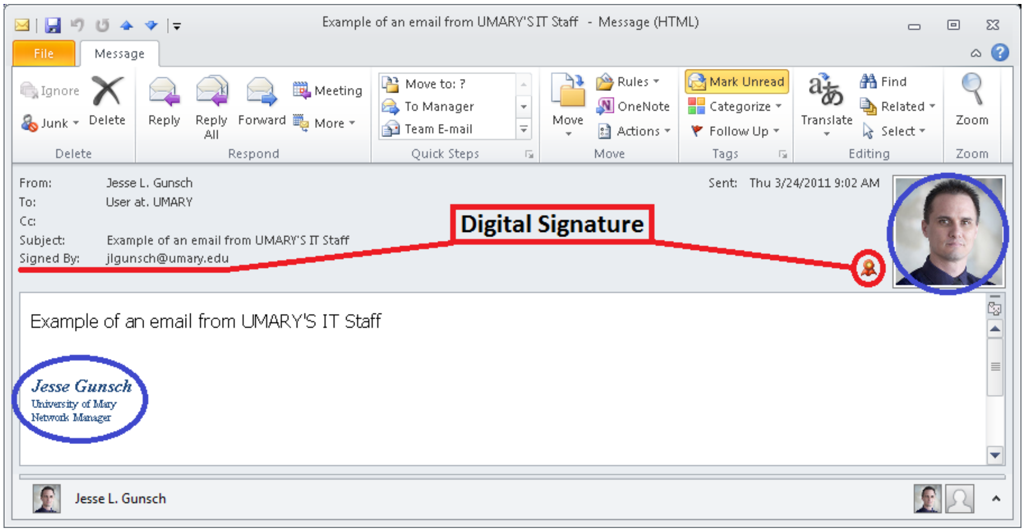
From: technology dept
To: User at. UMARY
Cc:
Subject: Example of an email from UMARY'S IT Department
Signed By: technology.dept@umary.edu
Sent: Thu 3/24/2011 8:26 AM

Digital Signature

Example of an email from UMARY'S IT Department

Technology Department
University of Mary

technology dept



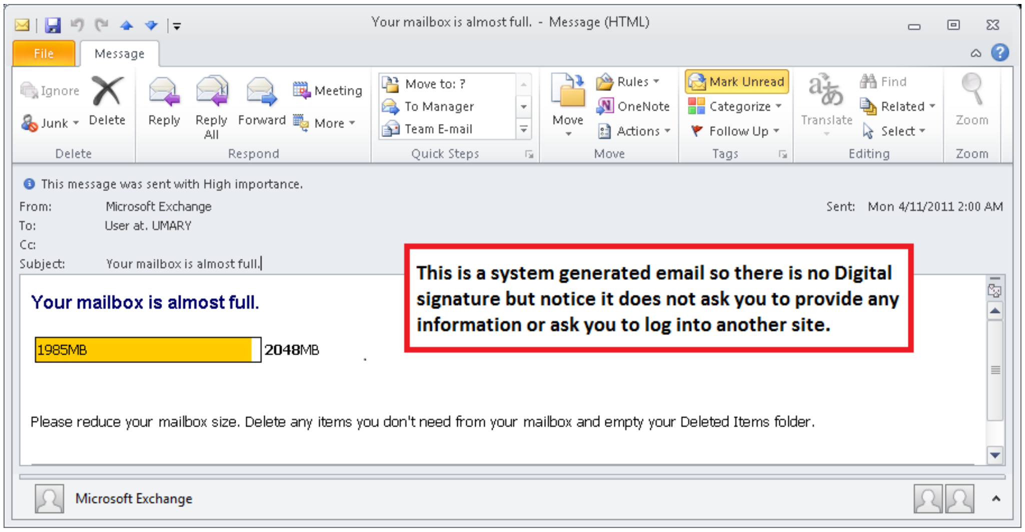
From: Jesse L. Gunsch
To: User at. UMARY
Cc:
Subject: Example of an email from UMARY'S IT Staff
Signed By: jlgunsch@umary.edu
Sent: Thu 3/24/2011 9:02 AM

Digital Signature

Example of an email from UMARY'S IT Staff

Jesse Gunsch
University of Mary
Network Manager

Jesse L. Gunsch



This message was sent with High importance.

From: Microsoft Exchange

Sent: Mon 4/11/2011 2:00 AM

To: User at. UMARY

Cc:

Subject: Your mailbox is almost full.

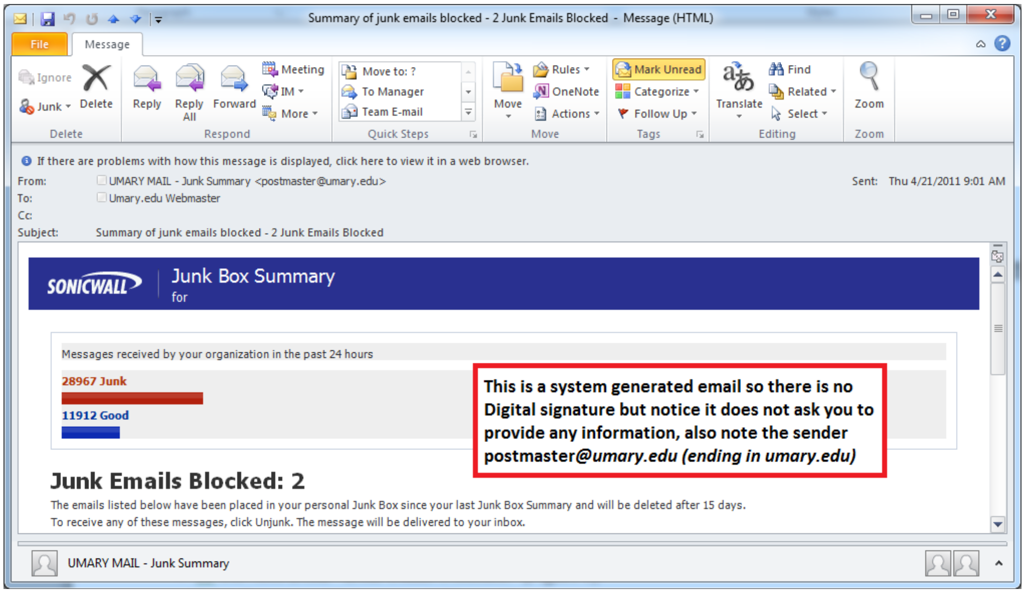
This is a system generated email so there is no Digital signature but notice it does not ask you to provide any information or ask you to log into another site.

Your mailbox is almost full.

1985MB 2048MB

Please reduce your mailbox size. Delete any items you don't need from your mailbox and empty your Deleted Items folder.

Microsoft Exchange



If there are problems with how this message is displayed, click here to view it in a web browser.

From: UMARY MAIL - Junk Summary <postmaster@umary.edu>

Sent: Thu 4/21/2011 9:01 AM

To: Umary.edu Webmaster

Cc:

Subject: Summary of junk emails blocked - 2 Junk Emails Blocked

Junk Box Summary
for

Messages received by your organization in the past 24 hours

28967 Junk

11912 Good

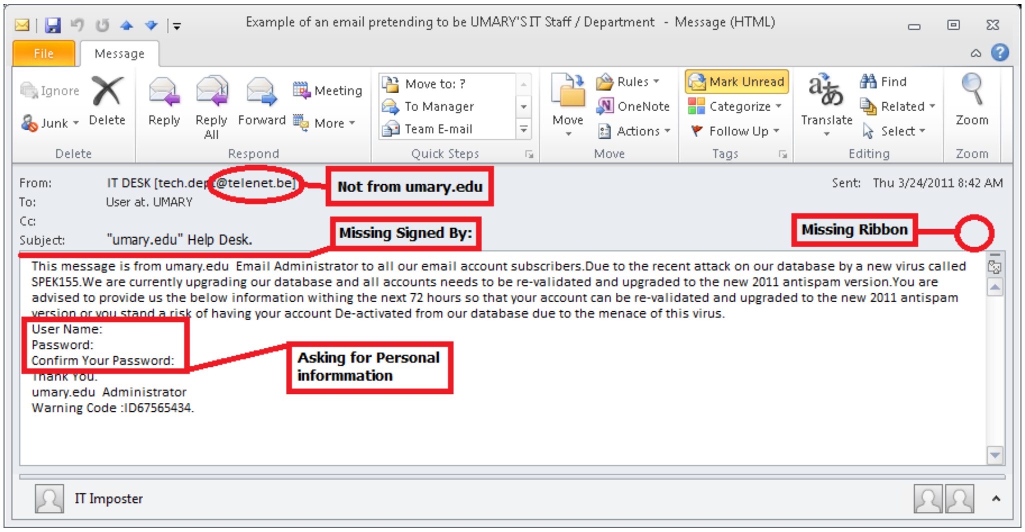
This is a system generated email so there is no Digital signature but notice it does not ask you to provide any information, also note the sender postmaster*@umary.edu (ending in umary.edu)*

Junk Emails Blocked: 2

The emails listed below have been placed in your personal Junk Box since your last Junk Box Summary and will be deleted after 15 days.
To receive any of these messages, click Unjunk. The message will be delivered to your inbox.

UMARY MAIL - Junk Summary

Example of Phishing email



From: IT DESK [tech.dept@telenet.be]

Not from umary.edu

Sent: Thu 3/24/2011 8:42 AM

To: User at. UMARY

Cc:

Subject: "umary.edu" Help Desk.

Missing Signed By:

Missing Ribbon

This message is from umary.edu Email Administrator to all our email account subscribers.Due to the recent attack on our database by a new virus called SPEK155.We are currently upgrading our database and all accounts needs to be re-validated and upgraded to the new 2011 antispam version.You are advised to provide us the below information withing the next 72 hours so that your account can be re-validated and upgraded to the new 2011 antispam version or you stand a risk of having your account De-activated from our database due to the menace of this virus.

User Name:
Password:
Confirm Your Password:
Thank You.
umary.edu Administrator
Warning Code :ID67565434.

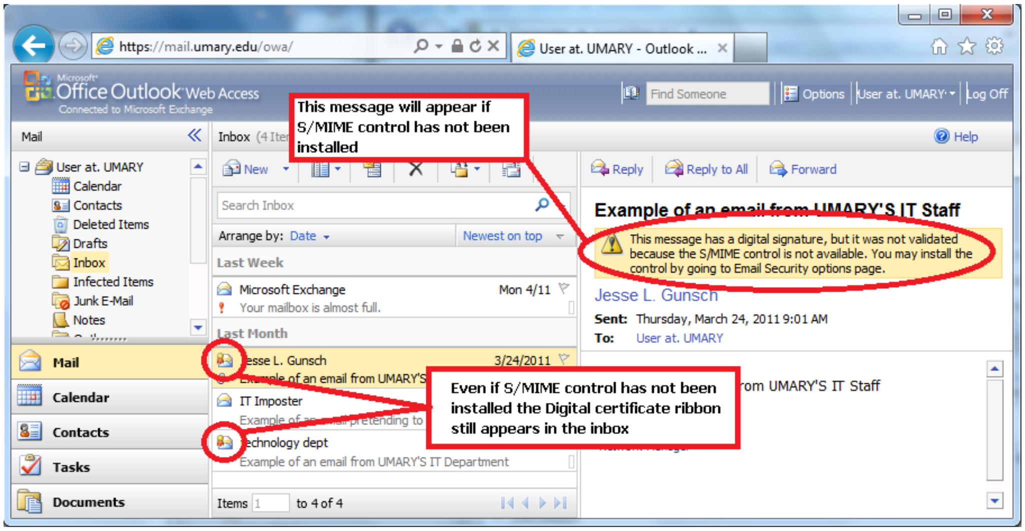
Asking for Personal informmation

IT Imposter

Outlook Web Access

Outlook web access will show the digital signature ribbon in the main inbox screen but may show a warning in the email itself if you have not installed S/MIME controls. You can install S/MIME controls by doing the following.

- Click Options in the upper right hand corner
- Click E-mail Security on the menu on the left
- Click install the Outlook Web Access S/MIME control



This message will appear if S/MIME control has not been installed

Example of an email from UMARY'S IT Staff

This message has a digital signature, but it was not validated because the S/MIME control is not available. You may install the control by going to Email Security options page.

Jesse L. Gunsch

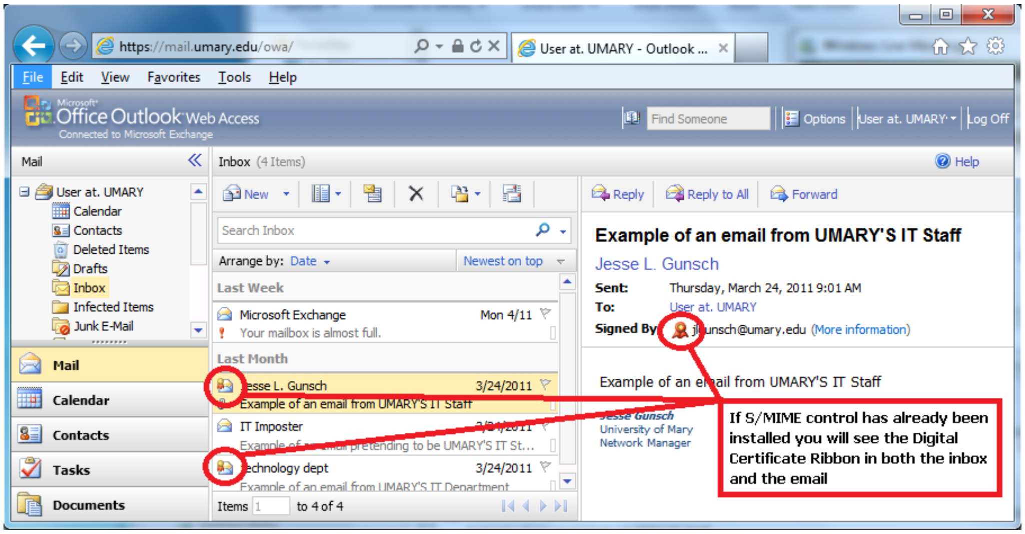
Sent: Thursday, March 24, 2011 9:01 AM

To: User at. UMARY

...rom UMARY'S IT Staff

Even if S/MIME control has not been installed the Digital certificate ribbon still appears in the inbox

After S/MIME has been installed



Example of an email from UMARY'S IT Staff

Jesse L. Gunsch

Sent: Thursday, March 24, 2011 9:01 AM

To: User at. UMARY

Signed By: jlgunsch@umary.edu (More information)

Example of an email from UMARY'S IT Staff

Jesse Gunsch
University of Mary
Network Manager

If S/MIME control has already been installed you will see the Digital Certificate Ribbon in both the inbox and the email