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

After S/MIME has been installed
Legitimate email examples

Example of an email from UMARY'S IT Department - Message (HTML)

From: technology dept
To: User at UMARY
Subject: Example of an email from UMARY'S IT Department
Signed By: technology.dept@umary.edu

Example of an email from UMARY'S IT Department

Example of an email from UMARY'S IT Staff - Message (HTML)

From: Jesse L. Gurnich
To: User at UMARY
Cc: Jesse L. Gurnich
Subject: Example of an email from UMARY'S IT Staff
Signed By: jlgurnich@umary.edu

Example of an email from UMARY'S IT Staff

Phishing Emails
Example of Phishing email

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.

Example of Phishing email

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)
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

After S/MIME has been installed