To: The Marist Community
From: A. Harry Williams
Re: Phony email
Date: September 6, 2010

Over the weekend, and email arrived on campus that claims to be from Mail Administrator and asking that you provide your login credentials to keep your acccount active.

This Message is from the Marist College,We are currently carrying-out a mentainace process to your marist.edu
account,please send us your current login credentials to keep your acccount active.

Marist Account:
Password:

Online Poughkeepsie New York
Marist College Webmaster

This is just one of several email scams floating around recently. Besides the spam we have become accustomed to seeing, there are new and more dangerous ones out today. These email are known as phishing, are attempting to get you to divulge personal or financial information. This will be used to either perform identify theft, charge purchases to your credit cards, withdraw funds from your bank account or other things that will take a long time to correct.

Some tips to help identify potential phishing attempts involving Marist.

No one in Information Technology will ask you for your password.

While we do not claim perfection, the spelling and grammar is far worse than we normally write. Be suspicious of email that sounds poorly written.

Email from Information Technology will always have the name of a person associated with the email. Be suspicious of email that only uses generic names for authorship.

We will add contact information in an email so that if you have additional questions, you have a place to call. Be suspicious of email that does not provide a method for contacting someone, especially if there is no phone number.

We will always use a marist.edu email address to send out email. The

email in question came from mail.tm02@gmail.com. Be suspicious of email that does not come from the place that is requesting information.

If you have any specific questions about an email, please feel free to contact the Helpdesk at Helpdesk@marist.edu or (845) 575-HELP (4357).

Some additional details about phishing:

The Anti-Phishing informational web site has a lot of useful information and is available at

http://www.antiphishing.org/

The US Federal Trade Commission (FTC) has some good information on how to not get hooked at

http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm

Webopedia defines phishing as

fish´ing) (n.) The act of sending an <
http://www.webopedia.com/TERM/p/e_mail.html>e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a <
http://www.webopedia.com/TERM/p/Web_site.html>Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user"s information. For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user"s account was about to be suspended unless he clicked on the provided <http://www.webopedia.com/TERM/p/hyperlink.html >link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a Web site look like a legitimate organizations site by mimicking the <
http://www.webopedia.com/TERM/p/HTML.html>HTML <
http://www.webopedia.com/TERM/p/code.html>code, the scam counted on people being tricked into thinking they were actually being contacted by eBay and were subsequently going to eBay"s site to update their account information. By spamming large groups of people, the "phisher" counted on the e-mail being read by a percentage of people who actually had listed

credit card numbers with eBay legitimately.

Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting. Other forms: phish (v.)
http://www.webopedia.com/TERM/p/phishing.html

Please make sure your McAfee Virus scanner is up to date prior to opening any attachments.

http://www.marist.edu/it/training/avupdate_steps.html