We have been informed that other colleges and universities are receiving a phishing email crafted to look as if it is coming from TIAA. The email provides a link for you to log in to your TIAA account to update your account details. The email appears to be highly targeted and includes the newest TIAA logo so it is more difficult to recognize as phony. We are unaware of any such emails arriving on campus, however if you receive one, do not log in using the link provided. If you have received this email and have clicked on the link, contact TIAA’s Security department at 1-800-842-2252.

TIAA’s web site has a Security Center where they identify how to Prevent identity theft, how to recognize phishing emails, and how to resolve problems if your identity is stolen. You can find the Security Center by clicking on the Security link at the bottom of the TIAA home page, or by typing phishing into the search box at the top of the TIAA home page.

Sample phishing email received at another institution:

---

**[MARSTAFF] TIAA Phishing email**

Harry Williams

to:
MARSTAFF
09/02/2016 12:16 PM
Sent by:
Marist Staff <MARSTAFF@VM.MARIST.EDU>
Hide Details
From: Harry Williams <Harry.Williams@marist.edu>
To: MARSTAFF@VM.MARIST.EDU
Sent by: Marist Staff <MARSTAFF@VM.MARIST.EDU>
Please respond to Harry Williams <Harry.Williams@marist.edu>

To: The Marist Community
From: A. Harry Williams
Re: Phony TIAA email
Date: September 2, 2016

We have been informed that other colleges and universities are receiving a phishing email crafted to look as if it is coming from TIAA. The email provides a link for you to log in to your TIAA account to update your account details. The email appears to be highly targeted and includes the newest TIAA logo so it is more difficult to recognize as phony. We are unaware of any such emails arriving on campus, however if you receive one, do not log in using the link provided. If you have received this email and have clicked on the link, contact TIAA’s Security department at 1-800-842-2252.

TIAA’s web site has a Security Center where they identify how to Prevent identity theft, how to recognize phishing emails, and how to resolve problems if your identity is stolen. You can find the Security Center by clicking on the Security link at the bottom of the TIAA home page, or by typing phishing into the search box at the top of the TIAA home page.

Sample phishing email received at another institution:
Below are 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 would 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.

Information Technology will add contact information in an email so that if you have additional questions, you have a place to call or email. 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. Be suspicious of email that does not come from the place that is requesting the information.

Be suspicious of web pages that do not look like Marist College web pages.

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 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 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 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 organization’s site by mimicking the 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.)