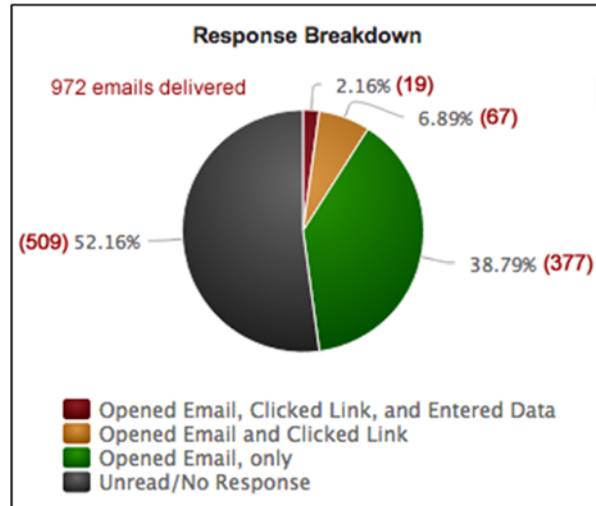


April 2014 Phishing Report

The ninth PhishMe.com simulation I.T. sent via email began on April 21, 2014 and ran for 5 full days with delivery to 972 staff emich.edu mailboxes. As can be seen by the chart to the right, at least 19 individuals were tricked into potentially changing their password.

Statistics also revealed that:

- 7 were repeat victims
- 3 were third time victims
- 1 was a fourth time victim
- 110 flagged the email as spam
- 12 min. of education delivered for this Phish
- 371 min. of education delivered since 6/2013
- 14 victims responded in the first hour
- 18 victims responded in the first 8 hours
- 18 victims responded on the first day



How it Worked

When the EMU recipient opened the email (see **Phishing Email** below) they were instructed to click on a familiar link and change their password. This link actually brought them to a fake landing page that looked exactly like EMUs login page for my.emich (see **Landing Page** below). If they entered their username and password and clicked the "Login" button or pressed the return key on their keyboard, they were redirected to the education page to view a 12 minute video.

If after critically reviewing a message, you still cannot tell if a message is a phishing attack, ask peers or the department that supposedly sent the message. In addition to all other options, the I.T. team is always willing to help you sort out such issues. Contact the Help Desk at 734.487.2120.

Phish Email

<p>From: IT Help Desk <IT-HELP@emich.edu> Subject: Heartbleed Password Security</p> <p>Dear Users,</p> <p>As you may have heard, a massive security vulnerability was discovered recently called the "heartbleed bug" that effects over 65% of all websites on the Internet. Please rest assured that the moment we learned about this bug our team took the necessary measures to protect our users. Because the bug was identified so late we are requiring that all users do a mandatory password reset by going to the following link:</p> <p>https://my-emich.edu/</p> <p>URL: https://heartbleed.it-security-group.com/78f5fb/</p> <p>Your safety is our number one priority.</p> <p>Thank you, Help Desk Information Technology</p>	<p>April 21, 2014 8:55AM</p> <p>No Other Notices - There were no warnings or other communications sent to advise users about an issue as important as this.</p> <p>Fraudulent Link - Rolling-over the address revealed that the hyperlink went to a different address than an emich.edu location. IT will only send you to an emich.edu location in regards to your password.</p>
---	---

Landing Page

Not My.emich - A fake page appears as if it is my.emich. The user is sent to this page where the hacker would steal the username and password when entered.

EASTERN MICHIGAN UNIVERSITY | my.emich

Secure Access Login
User Name:
Password:

[Having problems logging in? Click here.](#)

Welcome to the Eastern Michigan University Portal.
This secure site provides students, faculty and staff with access to many campus services. This is where you can check e-mail, register for courses, and stay informed.

Alternate Access Links:
To access EagleMail directly, go to mail.emich.edu.
To access Banner Self Service using your EID and PIN click [here](#).

What is my.emich?
[How do I get my user name and password?](#)
[How do faculty/staff get their user name and password?](#)
[Where can I find instructions for getting my username and password?](#)
<http://account.emich.edu>

What's Inside?

- E-mail:** Send and receive e-mail, and create your own personal address book.
- Calendar:** Access and manage your personal, course and school calendars.
- Groups:** Create, manage and join group homepages for clubs, affiliations and interests.

and much more...

Copyright © SunGard Higher Education 1998 - 2010. [Top](#) **DIVISION of INFORMATION TECHNOLOGY**