October 2014 Phishing Report
The ninth PhishMe.com simulation I.T. sent via email began on October 14, 2014 and ran for 5 full days with delivery to 980 user’s emich.edu mailboxes. As can be seen by the chart below, at least 244 individuals were tricked into entering their password.

Statistics also revealed that:
- 130 were repeat victims
- 37 were third time victims
- 18 were fourth time victims
- 6 were fifth time victims
- 77 flagged the email as spam
- 70 min. of education delivered for this Phish
- 505 min. of education delivered since 6/2013
- 143 victims responded in the first ½ hour
- 303 victims responded in the first 8 hours
- 309 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 link if they wanted to carry over 40 additional hours of paid time off into the next fiscal year. This link actually brought them to a fake landing page that looked like an EMU login page (see Landing Page below). If they entered their username and password and clicked the "Log in" button or pressed the return key on their keyboard, they were redirected to the education page to view a 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
Landing Page

Please sign in to complete our short 5 minute survey and be entered to win a $50 prepaid gas card.

Username: 
Password: 
Verify

GAS $50
1234 5678 8911 2700
1255