February 2015 Phishing Report
The 14th PhishMe.com simulation I.T. sent via email began on February 3, 2015 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 197 individuals were tricked into entering their password.

Statistics also revealed that:
- 76 were repeat victims
- 51 were third time victims
- 19 were fourth time victims
- 6 were fifth time victims
- 2 were sixth time victims
- 44 flagged the email as spam
- 86 min. of education delivered for this Phish
- 635 min. of education delivered since 6/2013
- 205 victims responded in the first ½ hour
- 342 victims responded in the first 8 hours
- 368 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 were interested in receiving a discounted meal plan from Dining Services. This link actually brought them to a fake landing page that looked like a my.emich login page (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 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

Enter your NetID and Password:

NetID: 
Password: 

LOGIN