Phishing Scenario #2

On August 22, at 1:35 PM we sent out our second phishing simulation from PhishMe.com. The email, which claimed that the recipient's mailbox was over quota, was sent to 952 emich.edu mailboxes. Of those recipients 34 provided a username and password on the landing page. A breakdown of the simulation and results is attached below.

The Phishing Email

From: <itsupport@emich.edu>
Subject: WebMail Quota Warning!

Recipient addressed by name:

Your Eastern Michigan Univeristy mailbox has reached its quota! If your quota is not expanded within 24 hours you will stop receiving new email messages.

Please click here to expand your quota.

Thank You,
IT Department
EASTERN MICHIGAN UNIVERSITY

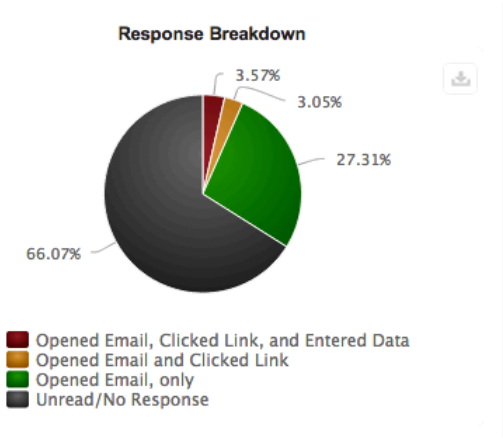
The Landing Page

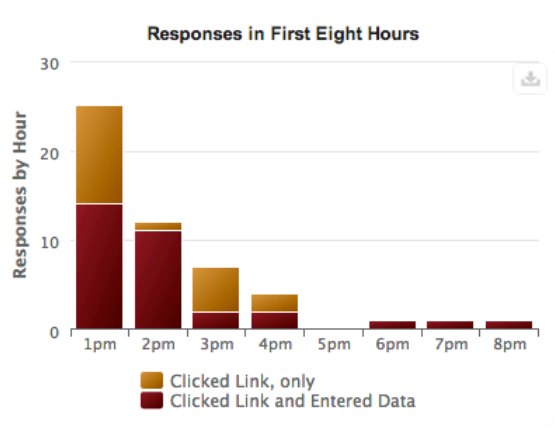
The Education Page

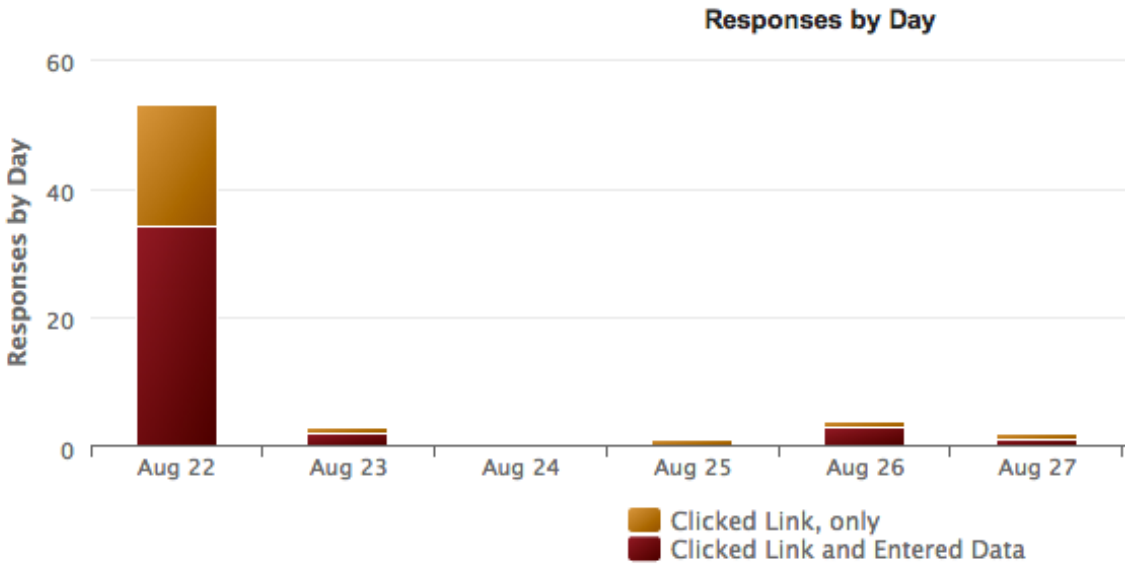
How it works

When the recipient opens the email they are enticed to click on the link provided, in this case click "here." This link would have forwarded them to the landing page where they are asked for their username and password. If they submitted the form they would have been redirected to the education page.

The Results

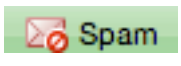






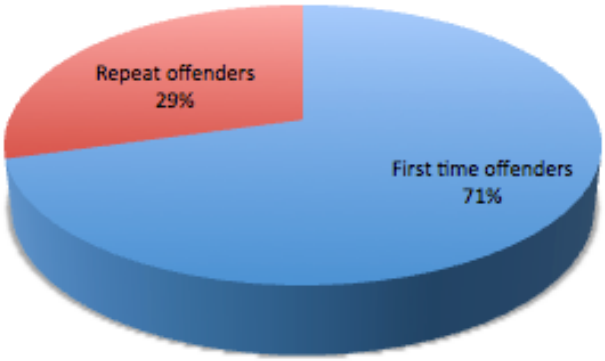
323 of the recipients opened the email in a way that we could track. Of those **63** clicked the link, and **34** of those provided a username and password.

Most of the passwords received were entered with **85** minutes of receiving the phish.

148 recipients labeled the Phish Spam with the Zimbra 

button.

Repeat Offenders



Conclusion

The overall number of individuals who entered a password decreased this month to 34 from 42 in the last month.

Once again 15% of the recipients used the Zimbra Spam button.

Only about one third of individuals who entered a password watched the education video in its entirety.

10 out of the 34 individuals, who entered a password this month, entered a password last month as well.

Only 1 out of the 34 individuals who entered a password this month has had their account compromised and locked.