Phishing Scenario #4

On October, 14 at 8:40 PM we sent out our fourth phishing simulation from PhishMe.com. The email, which claimed that the recipient's EagleMail account had been compromised and asked them to change their password, was sent to 953 emich.edu mailboxes. Of those recipients 35 provided a username and password on the landing page. A breakdown of the simulation and results is attached below.

The Phishing Email

From: Division of Information Technology <ithelpdesk@emich.edu>
Subject: Your EagleMail account has been compromised

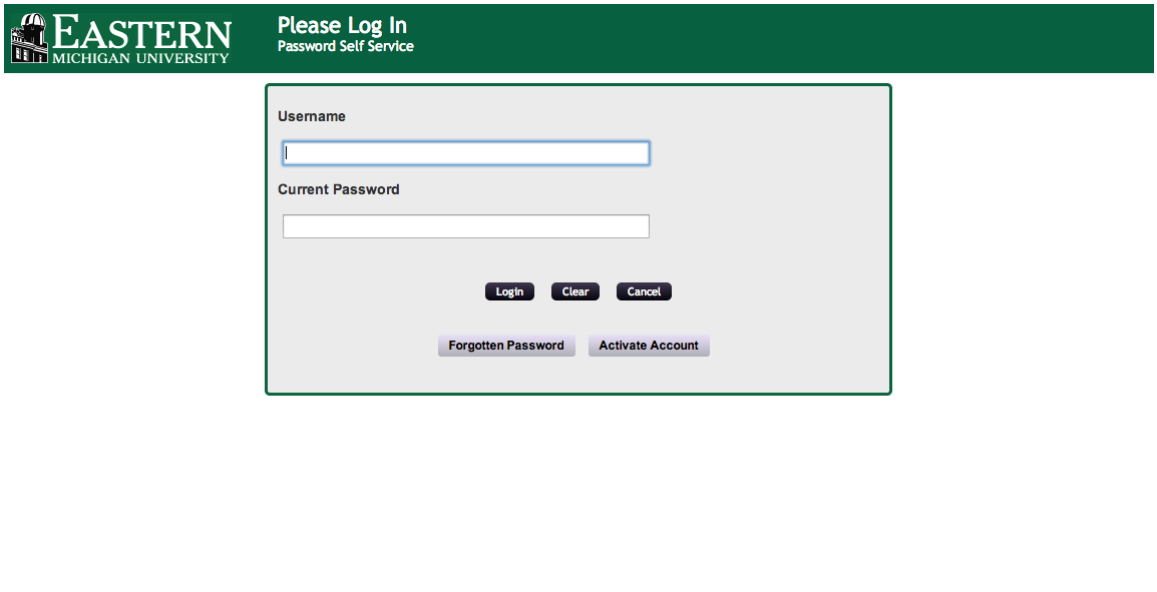
Good Afternoon,

We have detected that your EagleMail account is being used to send spam messages to other EMU accounts. This is generally a sign that your account has been compromised and is being used by a hacker. Please immediately change your account password with the link below:

Emich Account Password Reset

Thank you,
EMU IT Help Desk
106 Halle Library
Eastern Michigan University
Education First

The Landing Page

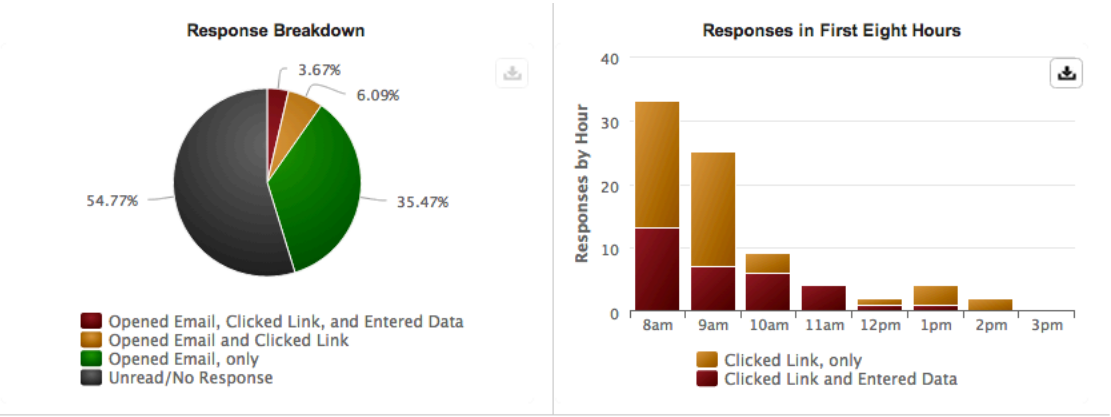


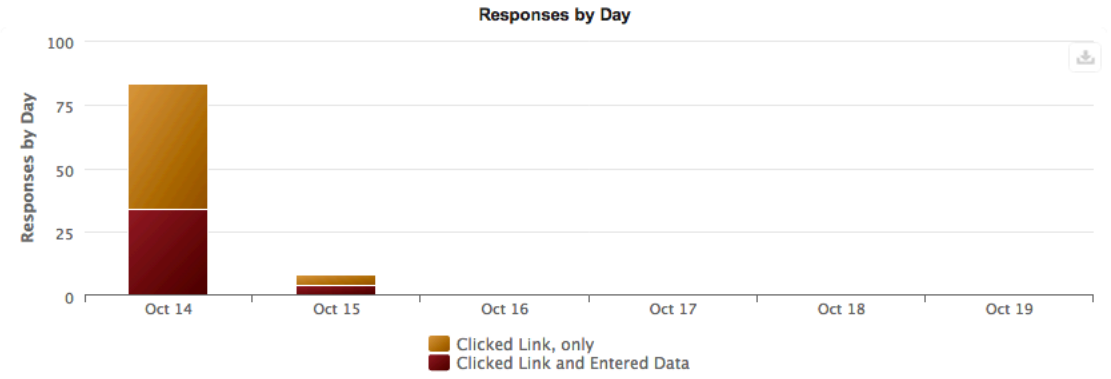
The Education Page

How it Works

When the recipient opens the email they are enticed to click on the link provided, in this case “Emich Account Password Reset” This link would have actually brought them to the landing page at “http://account.it-security-group.com/” where they would be asked for their username and password. If they submitted the form they would have been redirected to the education page.

The Results





- Of the **338** individuals who opened the email in a way we could track, **58** of them clicked the link, and **35** of them entered data in the password field and submitted the form.
- **37%** of those who entered a password did so within the first **20 minutes**.
- **153** recipients used the Zimbra 

button to report the message as spam. Once again very similar to past scenarios.
    - This time 20 of these individuals were given a security awareness month T-Shirt as a prize.

Repeat Offenders

- This month **17** of the **35** people who entered a password have done so in a previous scenario.
- **One** of those individuals has also had their EagleMail account compromised in the past.
    - On **three** different occasions.
- **One** of the repeat offenders is a 4th time offender.
- **Two** of the repeat offenders are 3rd time offenders.
- **10** of the repeat offenders did not watch the educational video.
- **None** of the three or four time offenders watched the educational video.

Education

Education Delivered this Month	Total Education Delivered
22 Minutes	**199** Minutes

Conclusion

- This scenario is back to the difficulty of our first two, and as such we saw a similar number of respondents.
    - Month 1: 42
    - Month 2: 34
    - Month 3: 185
    - Month 4: 35
- There was an increase in the percentage of respondents watching the video. (43%)
- Once again a larger than average portion of the repeat offenders did not watch the educational video this month.