Phishing Scenario #1

On July 30, at 9:45 AM we sent out our first phishing simulation from PhishMe.com. The email, which claimed that the recipient's mailbox was scheduled for deletion, was delivered to 952 emich.edu mailboxes. Of those recipients 42 individuals provided a username and password on the landing page. A breakdown of the simulation and results is attached below.

The Phishing Email

From: Information Technology <it@webaccess-alert.com>
Subject: Accounts scheduled for deletion

Eaglemail
EASTERN MICHIGAN UNIVERSITY

Warning Code:VQ2G88AAJ

To EMU email users:

This message is from the Eastern Michigan University messaging center to all EMU email users.

We are currently updating our data base and e-mail center. All unused accounts will be deleted. To ensure that any active accounts are not deleted you are required to verify that your account is active by confirming your email identity. This will prevent your email from been closed during this process. In order to confirm your email address, click here.

Warning!!! Any EMU email user that refuses to verify and subsequently update his or her email within seven days of receiving this notice will lose his or her email privileges permanently.

Thank you for your assistance.

Eastern Michigan University IT Security Team

****

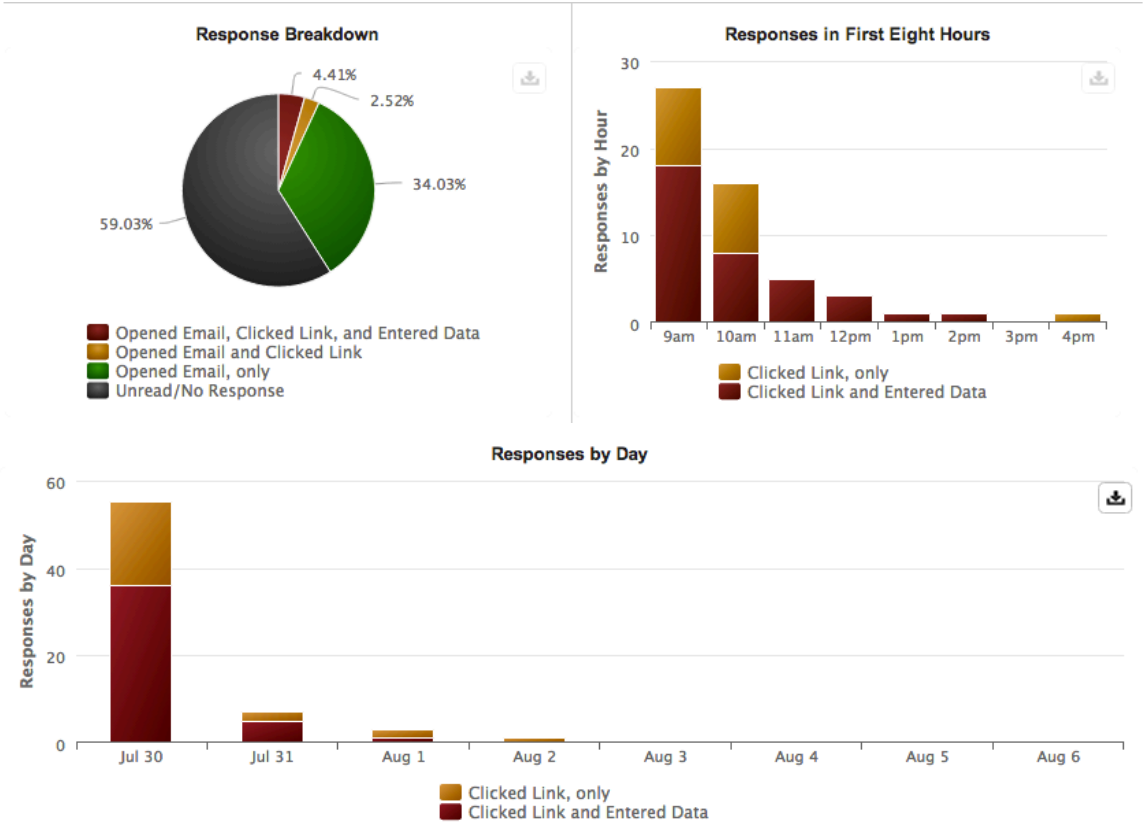
The Landing Page

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.

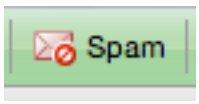
The Results



41% of recipients opened the email in a way that we could track. Tracking was done when the images in the email loaded, so folks who use plain text email were not tracked unless they click through to the link.

Nearly **50%** of those who responded to our simulation did so within the first **15 minutes** of receiving it. 9:45 – 10:00.

Although the scenario ran for 5 days, we only received password submissions on the first 3, most were received on **day 1.**



148 copies of the simulated Phish labeled as Spam by the recipient with the EagleMail Spam button.

Conclusion

74% of recipients were on an EMU IP address when they read our simulation. That means that the Infoblox DNS Firewall could protect these individuals. However, because most of the responses came in the first 15 minutes it would be hard to get a blacklist in place in time.

Two thirds of those who entered a password on the landing page watched the educational video in its entirety.

15% of recipients hit the Spam button.

I was not expecting to get so many individuals entering data. The help desk said that this Phish was more difficult than usual. Even so, I have never seen 42 passwords get compromised from one Phish, even a well-designed and wide spread Phish.

Only 2 of the 42 individuals who entered data have had their emich account compromised in the past year.

Moving forward, if there are repeat offenders, they will show up in this report.