Phishing Scenario #3
On September 16, at 1:00 PM we sent out our third phishing simulation from PhishMe.com. The email, which claimed that the recipient needed to update their direct deposit information, was sent to 952 emich.edu mailboxes. Of those recipients 185 provided a username and password on the landing page. A breakdown of the simulation and results is attached below.

The Phishing Email

From: EMU Payroll <payroll@emich.edu>  
Subject: Direct Deposit System Update

You are receiving this email because you have authorized University Payroll to pay you through direct deposit.

Due to a recent update to system, your direct deposit routing and account numbers will need to be updated by Friday, September 20th. Failure to do so will result in the loss of direct deposit status and require you to pick up your pay check from Payroll each pay period.

To update your direct deposit information please click the link below and verify your account.

https://payroll.emich.edu

Remember to save the direct deposit emails for your records.

--
Office of Payroll
201 Hover Building
EASTERN MICHIGAN UNIVERSITY
The Landing Page

Please sign in to the secure area to update your direct deposit information.

Username:  
Password:  
Log In
Forgotten Password?

The Education Page

This was an authorized phishing simulation.  
Don't worry! We're here to help you.

Please view the following video to learn more about Phishing!
How it works
When the recipient opens the email they are enticed to click on the link provided, in this case “https://payroll.emich.edu/” This link would have actually brought them to the landing page at “http://payroll.hr-­‐communications.com/emich.edu/” 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

- Of the 603 individuals who opened the email in a way we could track, 279 of them clicked the link, and 185 of them entered data in the password field and submitted the form.
- Once again a large majority (127) of these individuals who entered passwords did so within the first hour of the scenario.
- 143 recipients used the Zimbra button. This number is very similar to past scenarios.
Repeat Offenders

- This month 18 of the 185 people who entered a password have done so in a previous scenario.
- Only 3 of those 17 watched the education material in its entirety this month.
- Of those 17, 3 have fallen victim to all three scenarios.
  - None of the 3 time offenders watched the education material this month.
  - None of the 3 time offenders watched the education material last month
  - Only 1 of the 3 three time offenders watched the first month’s education video.

Education

<table>
<thead>
<tr>
<th>Education Delivered This Month</th>
<th>Total Education Delivered</th>
</tr>
</thead>
<tbody>
<tr>
<td>142 Minutes</td>
<td>177 Minutes</td>
</tr>
</tbody>
</table>

Conclusion

- This scenario was significantly more difficult than the past two. And so the number of individuals who entered data dramatically increased from 34 to 185.
- Once again only about 1/3 of the victims watched the full education video.
- 14 individuals who entered their password this month have had their account actually compromised in the past.
  - 70% of these individuals watched the education video in its entirety.