Mayo’s Way: Systematic Anti-Phishing Campaign Pays Dividends

Mark Parkulo, MD & JoEllen Frain
You have a new voicemail!

From: Unknown Caller  
Received: 09/26/2015  
Length: 00:52

Dear Employee,

You are receiving this message because we were unable to deliver it, the voice message did not go through because the voicemail was unavailable at that moment.

To listen to this message, please click here.

This message will only be available until 11:59:59 pm.

* The reference number for this message is qvfl_cjl09-9107319601-2125579909-62.

The length of transmission was approximately 52 seconds.

Thank you.

This is a system-generated message from a send-only address.  
Please do not reply to this email.

© 2013 CorpVM Inc.
You’ve Been Phished
Proactive Phishing Overview

- Proactive Phishing began in Sept 2015

- Objectives
  - Increase good security behaviors among staff
  - Decrease susceptible email behavior
  - Encourage users to report all suspicious emails
Proactive Phishing Overview

• Campaigns were inclusive of 65k+ employees/students

• Third party vendor (PhishMe) was the partner for conducting campaigns

• Campaigns were standard campaigns that could be benchmarked against other organizations

• Project included endorsement from various governance group
  – Information Technology from a capabilities standpoint
  – Security Operations support
Proactive Phishing Overview

• Trending data is available on susceptibility rates, reporter rates and no-action rates.

• Susceptibility Rates = individuals who have fallen victim because they clicked on a link or opened an attachment within the simulated training exercise.

• Reporter Rates = individuals who have identified the simulated training exercise as suspicious, did not click any links or attachments and have reported the email using the Report Phishing button.

• Did Nothing Rates = individuals who have not reported or fallen victim to the simulated training exercise.
Campaign Results Sept 2015 to February 2016

- % Fell Victim
- % Reported
- % Did Nothing
CURRENT STATE

FEELING

“I’m safe because I work at Mayo.”

“My IT protects me.”

REALITY

We’re not as safe as we think.

Technology can’t stop all threats.

FUTURE STATE

Employees equipped to support a

MAYO CULTURE

that is ...

AWARE OF THE RISKS

BETTER EQUIPPED & PREPARED
BEHAVIOR CHANGE
CHANGING BEHAVIORS …
we all have a role to play
Security Awareness Module

• Launched February 2016
• General Information Security Awareness Module launched to 65,000
• Focused on raising awareness to the threat and highlighted phishing awareness
• 97% completion rate by March 2016
TECHNOLOGY HAS CHANGED US...
CYBER CRIME HAPPENS EVERY DAY

the threat to you and to your organization is real
NATION-STATE
Cyberterrorism, hacktivist, IP

SYNDICATED CRIME
Access data for sale

INSIDER THREAT
Personal Gain

OURSELVES
Mixed data, lack of awareness
it’s always phishing season
Phishing

• Deceitful emails designed to capture personal information from the recipient

• Coax recipient to click on a link, open a document or submit credentials

• The majority of data breaches begin with a phishing campaign.*

*2016 Verizon Data Breach Report
From: Security Watchers [Securitywatchers@trxstr.com]
Sent: December 6, 2014 7:36:41 PM CST
To: undisclosed-recipients
Subject: ALERT!!! Your Account Has Been Suspended

Dear Employee,

Your account has been suspended because we notice a problem on your account.

We determined someone used your account without your permission. For your security we suspended your account. To gain access to your account

Click Here>>> Follow the steps to Update your account or use the attached form below.

Note: If not resolved we will be forced to suspend access to the computer.

Thank you for your cooperation in this matter.

Thank you,
Security Watchers of Mayo

1. Subject line and message create a sense of urgency
2. Sensitive data is requested
3. Hovering over links reveals a non-Mayo Web address
4. Message invokes strong emotions, like greed or fear
5. Email contains incorrect grammar or spelling
6. Watch for vague or missing signature
HOW TO REPORT

- PhishMe button deployed to all Windows workstations
- Click any time you suspect a phishing attempt
## Susceptibility by Region

<table>
<thead>
<tr>
<th>Location</th>
<th>Susceptible</th>
<th>Recipients</th>
<th>% Susceptible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rochester, Minnesota</td>
<td>3,492</td>
<td>35,166</td>
<td>9.93%</td>
</tr>
<tr>
<td>Jacksonville, Florida</td>
<td>492</td>
<td>5,561</td>
<td>8.85%</td>
</tr>
<tr>
<td>Phoenix, Arizona</td>
<td>345</td>
<td>4,045</td>
<td>8.53%</td>
</tr>
<tr>
<td>Eau Claire, Wisconsin</td>
<td>338</td>
<td>3,774</td>
<td>8.96%</td>
</tr>
<tr>
<td>La Crosse, Wisconsin</td>
<td>299</td>
<td>2,834</td>
<td>10.55%</td>
</tr>
<tr>
<td>Mankato, Minnesota</td>
<td>265</td>
<td>2,428</td>
<td>10.91%</td>
</tr>
<tr>
<td>Scottsdale, Arizona</td>
<td>220</td>
<td>2,154</td>
<td>10.21%</td>
</tr>
<tr>
<td>Waycross, Georgia</td>
<td>94</td>
<td>1,280</td>
<td>7.34%</td>
</tr>
<tr>
<td>Albert Lea, Minnesota</td>
<td>141</td>
<td>1,135</td>
<td>12.42%</td>
</tr>
<tr>
<td>Austin, Minnesota</td>
<td>115</td>
<td>999</td>
<td>11.51%</td>
</tr>
<tr>
<td>Red Wing, Minnesota</td>
<td>85</td>
<td>739</td>
<td>11.50%</td>
</tr>
<tr>
<td>Menomonie, Wisconsin</td>
<td>80</td>
<td>641</td>
<td>12.48%</td>
</tr>
<tr>
<td>Fairmont, Minnesota</td>
<td>63</td>
<td>579</td>
<td>10.88%</td>
</tr>
<tr>
<td>Owatonna, Minnesota</td>
<td>44</td>
<td>412</td>
<td>10.68%</td>
</tr>
<tr>
<td>Barron, Wisconsin</td>
<td>31</td>
<td>366</td>
<td>8.47%</td>
</tr>
<tr>
<td>New Prague, Minnesota</td>
<td>31</td>
<td>318</td>
<td>9.75%</td>
</tr>
<tr>
<td>Bloomer, Wisconsin</td>
<td>25</td>
<td>241</td>
<td>10.37%</td>
</tr>
<tr>
<td>Onalaska, Wisconsin</td>
<td>22</td>
<td>241</td>
<td>9.13%</td>
</tr>
<tr>
<td>Sparta, Wisconsin</td>
<td>20</td>
<td>216</td>
<td>9.26%</td>
</tr>
<tr>
<td>Cannon Falls, Minnesota</td>
<td>18</td>
<td>195</td>
<td>9.23%</td>
</tr>
<tr>
<td>Osseo, Wisconsin</td>
<td>18</td>
<td>194</td>
<td>9.28%</td>
</tr>
<tr>
<td>Lake City, Minnesota</td>
<td>20</td>
<td>179</td>
<td>11.17%</td>
</tr>
<tr>
<td>Waseca, Minnesota</td>
<td>16</td>
<td>144</td>
<td>11.11%</td>
</tr>
<tr>
<td>Andover, Massachusetts</td>
<td>8</td>
<td>117</td>
<td>6.84%</td>
</tr>
<tr>
<td><strong>Total: Locations 100+</strong></td>
<td>6,282</td>
<td>63,958</td>
<td>9.82%</td>
</tr>
<tr>
<td><strong>Total: 45 OtherLocations</strong></td>
<td>157</td>
<td>1,315</td>
<td>11.94%</td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td>6,439</td>
<td>65,273</td>
<td>9.86%</td>
</tr>
</tbody>
</table>
## Susceptibility of 20 largest job titles

<table>
<thead>
<tr>
<th>Job Title</th>
<th>Susceptible</th>
<th>Recipients</th>
<th>% Susceptible</th>
</tr>
</thead>
<tbody>
<tr>
<td>RN 24/7 BSN</td>
<td>177</td>
<td>2,867</td>
<td>6.17%</td>
</tr>
<tr>
<td>RESIDENT-ROCHESTER</td>
<td>159</td>
<td>1,244</td>
<td>12.78%</td>
</tr>
<tr>
<td>RN 24/7 AD/DIP</td>
<td>70</td>
<td>1,057</td>
<td>6.62%</td>
</tr>
<tr>
<td>CLINICAL ASSISTANT</td>
<td>100</td>
<td>837</td>
<td>11.95%</td>
</tr>
<tr>
<td>ADMINISTRATIVE ASST</td>
<td>122</td>
<td>665</td>
<td>18.35%</td>
</tr>
<tr>
<td>PATIENT CARE ASSISTANT-SMH</td>
<td>57</td>
<td>568</td>
<td>10.04%</td>
</tr>
<tr>
<td>RN-INPT/365 (B OR MN)-AZ</td>
<td>36</td>
<td>560</td>
<td>6.43%</td>
</tr>
<tr>
<td>HEALTH UNIT COORDINATOR</td>
<td>78</td>
<td>531</td>
<td>14.69%</td>
</tr>
<tr>
<td>MEDICAL SECY</td>
<td>103</td>
<td>525</td>
<td>19.62%</td>
</tr>
<tr>
<td>PATIENT APPT COORD</td>
<td>73</td>
<td>497</td>
<td>14.69%</td>
</tr>
<tr>
<td>IT SR ANALYST/PROGRAMMER</td>
<td>27</td>
<td>495</td>
<td>5.45%</td>
</tr>
<tr>
<td>RTP-RESEARCH FELLOW-LS</td>
<td>84</td>
<td>493</td>
<td>17.04%</td>
</tr>
<tr>
<td>MSHS STUDENT</td>
<td>27</td>
<td>471</td>
<td>5.73%</td>
</tr>
<tr>
<td>RN EXTENDED BSN</td>
<td>35</td>
<td>453</td>
<td>7.73%</td>
</tr>
<tr>
<td>RN 24/7-AD/DIP</td>
<td>22</td>
<td>440</td>
<td>5.00%</td>
</tr>
<tr>
<td>CLINICAL LAB TECHNOLOGIST</td>
<td>17</td>
<td>400</td>
<td>4.25%</td>
</tr>
<tr>
<td>RN DAY BSN</td>
<td>32</td>
<td>398</td>
<td>8.04%</td>
</tr>
<tr>
<td>CLINICAL LAB TECH-CLS</td>
<td>23</td>
<td>389</td>
<td>5.91%</td>
</tr>
<tr>
<td>LPN-CLINIC</td>
<td>32</td>
<td>385</td>
<td>8.31%</td>
</tr>
<tr>
<td>MED/SURG TRANSCRIPTIONIST</td>
<td>13</td>
<td>371</td>
<td>3.50%</td>
</tr>
<tr>
<td><strong>Total: 20 Largest Titles</strong></td>
<td>1,287</td>
<td>13,646</td>
<td>9.43%</td>
</tr>
<tr>
<td><strong>Total: 6,411 Other Titles</strong></td>
<td>5,152</td>
<td>51,627</td>
<td>9.98%</td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td>6,439</td>
<td>65,273</td>
<td>9.86%</td>
</tr>
</tbody>
</table>
Most susceptible job titles with at least 50 recipients

<table>
<thead>
<tr>
<th>Job Title</th>
<th>Susceptible</th>
<th>Recipients</th>
<th>% Susceptible</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASSOC OPS-SCM P2P</td>
<td>24</td>
<td>63</td>
<td>38.10%</td>
</tr>
<tr>
<td>PATHOLOGY REPORTING SPEC</td>
<td>15</td>
<td>67</td>
<td>22.39%</td>
</tr>
<tr>
<td>RN EXT BSN</td>
<td>12</td>
<td>55</td>
<td>21.82%</td>
</tr>
<tr>
<td>ASSOC CLINICAL RESEARCH COORD</td>
<td>41</td>
<td>193</td>
<td>21.24%</td>
</tr>
<tr>
<td>CLINICAL SPECIALTY REP-MML</td>
<td>13</td>
<td>64</td>
<td>20.31%</td>
</tr>
<tr>
<td>MEDICAL SECY</td>
<td>103</td>
<td>525</td>
<td>19.62%</td>
</tr>
<tr>
<td>RESEARCH SCIENTIST</td>
<td>10</td>
<td>51</td>
<td>19.61%</td>
</tr>
<tr>
<td>ADMINISTRATIVE ASSISTANT</td>
<td>32</td>
<td>165</td>
<td>19.39%</td>
</tr>
<tr>
<td>MGR-OPERATIONS</td>
<td>16</td>
<td>84</td>
<td>19.05%</td>
</tr>
<tr>
<td>SPV-CLINIC OPERATIONS</td>
<td>12</td>
<td>63</td>
<td>19.05%</td>
</tr>
<tr>
<td>RTP-RESEARCH ASSOCIATE-LS</td>
<td>26</td>
<td>138</td>
<td>18.84%</td>
</tr>
<tr>
<td>ANESTHESIA TECH</td>
<td>14</td>
<td>75</td>
<td>18.67%</td>
</tr>
<tr>
<td>ADMINISTRATIVE ASST</td>
<td>122</td>
<td>665</td>
<td>18.35%</td>
</tr>
<tr>
<td>CLINICAL RESEARCH COORDINATOR</td>
<td>22</td>
<td>121</td>
<td>18.18%</td>
</tr>
<tr>
<td>NURSE PRACTITIONER 24/7</td>
<td>24</td>
<td>133</td>
<td>18.05%</td>
</tr>
<tr>
<td>RESEARCH ASSISTANT</td>
<td>11</td>
<td>61</td>
<td>18.03%</td>
</tr>
<tr>
<td>RECRUITER</td>
<td>9</td>
<td>51</td>
<td>17.65%</td>
</tr>
<tr>
<td>RN STUDY COORD DAY BSN</td>
<td>9</td>
<td>51</td>
<td>17.65%</td>
</tr>
<tr>
<td>SECY-MED PRACTICE-AZ</td>
<td>24</td>
<td>138</td>
<td>17.39%</td>
</tr>
<tr>
<td>SOCIAL WORKER LICSW</td>
<td>9</td>
<td>52</td>
<td>17.31%</td>
</tr>
</tbody>
</table>
Report Timelines

- Reporter Timeline shows when the users reported the scenario. In this case the first report arrived before the first opening of an attachment. There were 21,717 total reports via PhishMe Reporter.
- Fastest Reporters data is available to show who reported the Phish via the PhishMe Reporter Plugin. The shortest time spent to evaluate and report the phish was 6 seconds.
  - 2,896 users reported the email within a minute of receiving it.
Using the Data

- Organizational Tier Approach
  - Tier 2 Executive
  - Tier 3 Physicians
  - Tier 4 High Fidelity
  - Tier 5 Support Areas (Help Desk, Work Station Support, Telecom, supervisors, etc.)
  - Tier 6 All employees

- Each tier has a separate strategy to engage the intended audience
  - Data from the campaigns guides targeted interventions
  - Quarterly scorecards are produced and shared
Phishing Results by Department

**PHYSICIANS**
- Did Nothing: 49%
- Reported Phish: 40%
- Fell Victim: 11%

**ALL OF MAYO CLINIC**
- Did Nothing: 41%
- Reported Phish: 50%
- Fell Victim: 9%

Phishing Results by Site

**PHYSICIANS**
- RST: 43%, 11%, 53%, 8%
- FL: 42%, 11%, 46%, 10%
- AZ: 39%, 11%, 49%, 10%
- MCHS: 33%, 17%, 45%, 11%

**ALL OF MAYO CLINIC**
- RST: 50%, 17%, 44%, 11%
- FL: 48%, 11%, 45%, 10%
- AZ: 50%, 11%, 41%, 10%
- MCHS: 50%, 17%, 44%, 11%
• Increased number of phish reports (spam, marketing, etc.)
  – Averaging ~ 1000 reports a day
    • 11% are phishing attempts
    • 75% are spam
    • 14% are internal Mayo business communications
• Defined path for “repeat offenders”
  – Direct communication to employee on phishing results
  – A request to the supervisor for their support (without identifying the individuals)
  – Ongoing monitoring for improvement
Phishing Module

- 10 interactive scenarios where employees determined best actions based on particular email
- Average score: 86.2%
- Completion rate for all staff as of September 2016: 95%
- Designed to further refine skills
  - Eliminate as many false positives
  - Reinforce good practices and behavior
  - Identify areas that would benefit from targeted interventions
**Scenario 1:** Nancy provided her Mayo Clinic email address while registering for an account with LinkedIn (a social media site for networking); she hasn't been logged in to her account in a while and received the communication below.

**Question:** Since Nancy is a registered user of LinkedIn and would like to know who is viewing her profile, she should:

- [ ] Click on the links provided in the email.
- [ ] Open Internet browser, navigate to LinkedIn and log in to her account.
- [ ] Report the email as phishing.
Scenario 9: Mike received this email. He was not expecting any deliveries, and hasn't placed any orders with Walgreens.

Question: What should he do?

- Copy the URL from the email and paste it in to his Internet browser.
- Click on the link provided in the email.
- Open Internet browser, navigate to the Walgreens website and log in to his account.
- Report as phishing.
**Scenario 9:** Mike received this email. He was not expecting any deliveries, and hasn’t placed any orders with Walgreens.

**Question:** What should he do?

- [ ] Copy the URL from the email and paste it into his Internet browser.
- [ ] Click on the link in the email.
- [ ] Open Internet Explorer and navigate to the website and log in to his account.
- [ ] Report as phishing.

---

**Correct**

This is the best choice. Whenever unsure or uncertain about an email and its legitimacy, it is appropriate to report it using the Report Phishing button in Outlook. By doing so, Mike is not only keeping his own identity safe, he is also helping Information Security keep other Mayo Clinic staff members safe.

---

Kindly request these not to be sent when you let us know your preference:

4342 County Road 203 Durango Co 81301-3715

We thank you for being part of our updates but if you wish to no longer be apart then tell us now and you will not hear more. PO Box 1960 #22445 Wilmington, DE 19899
Campaign Results Aug 2016 to Oct 2016

![Bar chart showing campaign results from Aug 2016 to Oct 2016. The chart compares the percentage of people who fell victim, reported, and did nothing for campaigns labeled 1 and 2.](chart.png)
Success Stories

• Large Scale “Amazon” Email phishing campaign entered the organization in June 2016
• Targeted the physicians
• 4000 recipients
From: Amazon Security <support@amazon.sec>
Subject: Amazon.com need to update your information with the Visa, Mastercard issuer

Dear Amazon User,
We have placed a hold on your account because the billing details for your Visa, Mastercard did not match the details on file with the card issuer. You will not be able to access your account or place orders with us until we confirm your information. You can help us resolve this issue by replying to this message with the billing name, address, and phone number registered to your Visa, Mastercard. Please reply from the email address registered to your Amazon.com account. If you have recently moved, you may need to update your information with the card issuer before you reply to this message. For your security, we restrict access to your billing details to a team of account specialists. Our Customer Service team cannot access these details or provide you with more information on this issue. They can only verify that we sent this request. We ask that you not open new accounts as any order you place may be delayed.

Please Verified Your Account.

Sincerely, Amazon.com
Outcomes

- First report from end user was 2 minutes after first email arrived, 11 people interacted
- 200 total reporters
- Security Operations Center was able to determine the email was malicious
  - Immediately blocked the malicious link
  - Removed remaining emails from end user mailboxes
- Identified 11 users who had interacted with the link for remediation
Future Program Plan

- Full (all staff) campaigns on a quarterly basis
- Spear campaigns on a quarterly basis
- Monitor data
Business Case

• It is estimated that over 156 million phishing emails are sent on a daily basis, with 80,000 falling victim*

• The sophistication of these types of attacks constantly evolves and improves, bypassing the technology that is meant to stop it

• Activating the “Human Sensor” is a low cost, but highly effective way to increase your security posture (for prevention, detection and reduction in time to remediation)

*IT ProPortal
Business Case

• Decreases the risk of end users interacting with suspicious emails

• Increases the ability for the organization to identify the threat before harm

• Decision on the up front preventative cost vs. the cost of remediation or a breach

• Consistency in the plan and utilize the data to track the risk reduction to the organization

*IT ProPortal
Mark Parkulo, MD
& JoEllen Frain

Mayo Clinic