Phishing Freakonomics
(aka “Picking Winners”)

Russell Butturini
Senior Information Security Architect, Top 20 CPA Firm
Defcon 27 Packet Hacking Village
-Senior security architect and head of all things IT security along with my governance and compliance dictatress at a top 20 CPA/financial services firm.

-@tcstoolhax0r on Twitter

-Presenter at various Bsides, Derbycon, PHV, etc.

-Occasionally releases poorly written Python code that does cool things.

-Everything said in this talk is mine and doesn’t represent the views of my employer.
Why give this talk?

- "Phishing always works"
- "Users are stupid"
- "People are the weakest link"
- "It only takes one"
The Story

- No previous training and awareness program

- Never done phish testing

- Unstructured reporting for email threats, lack of centralized security awareness resources for end users
The story

Test 1: 5.60%
The story
A New Approach

-Treat the problem like a software or code issue.

-Figure out why people are “vulnerable”.

-How do we patch them???

-USE THE DATA IN FRONT OF US
Warning: Not a Data Scientist
I do this instead...
American Pharoah

Owned: Zayat Stables LLC

B. c. 3 (Feb) FTS AUG13 $300,000
Sire: PioneeroftheNile (Empire Maker) $60,000
Dam: Littleprincesses (Yankee Gentleman)
Br: Zayat Stables (Ky)
Tr: Baffert Bob

<table>
<thead>
<tr>
<th>Race Date</th>
<th>Dist</th>
<th>Finish</th>
<th>Time</th>
<th>Odds</th>
<th>Jockey</th>
<th>Trainer</th>
<th>Earnings</th>
<th>Win</th>
<th>Place</th>
<th>Show</th>
<th>Feet</th>
<th>Odds</th>
<th>Weight</th>
<th>Year</th>
<th>Status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>6Jun15-11El</td>
<td>1½</td>
<td>1½</td>
<td>:48.4</td>
<td>1.13</td>
<td>2</td>
<td>2.02</td>
<td>2.26</td>
<td>Belmont - G1</td>
<td>105</td>
<td>5</td>
<td>11½</td>
<td>11</td>
<td>12</td>
<td>13½</td>
<td>Espinoza</td>
<td>L126</td>
</tr>
<tr>
<td>16May15-13Pr</td>
<td>1½</td>
<td>1½</td>
<td>:46.2</td>
<td>1.11</td>
<td>2</td>
<td>1.37</td>
<td>1.59</td>
<td>Prkns - G1</td>
<td>102</td>
<td>1</td>
<td>11</td>
<td>12½</td>
<td>13</td>
<td>14</td>
<td>17</td>
<td>Espinoza</td>
</tr>
<tr>
<td>2May15-11CD</td>
<td>1½</td>
<td>1½</td>
<td>:47.1</td>
<td>1.11</td>
<td>1</td>
<td>1.36</td>
<td>2.03</td>
<td>KyDby - G1</td>
<td>105</td>
<td>15</td>
<td>3½</td>
<td>31</td>
<td>32</td>
<td>3½</td>
<td>11</td>
<td>Espinoza</td>
</tr>
<tr>
<td>11Apr15-11DP</td>
<td>1½</td>
<td>1½</td>
<td>:45.4</td>
<td>1.10</td>
<td>2</td>
<td>1.35</td>
<td>1.48</td>
<td>ArkDby - G1</td>
<td>105</td>
<td>6</td>
<td>23½</td>
<td>23</td>
<td>21</td>
<td>13½</td>
<td>18</td>
<td>Espinoza</td>
</tr>
<tr>
<td>14Mar15-100P</td>
<td>1½</td>
<td>1½</td>
<td>:24.2</td>
<td>1.15</td>
<td>1</td>
<td>1.1</td>
<td>1.15</td>
<td>Rebel - G2</td>
<td>100</td>
<td>4</td>
<td>1½</td>
<td>11</td>
<td>11</td>
<td>14</td>
<td>16½</td>
<td>Espinoza</td>
</tr>
<tr>
<td>27Sep14-6SA</td>
<td>1⅛</td>
<td>1½</td>
<td>:23</td>
<td>1.14</td>
<td>1</td>
<td>1.14</td>
<td>1.14</td>
<td>Fort Lmnnr - G1</td>
<td>101</td>
<td>5</td>
<td>1½</td>
<td>11</td>
<td>12½</td>
<td>13½</td>
<td>Espinoza</td>
<td>L122</td>
</tr>
<tr>
<td>3Sep14-80mr</td>
<td>7F</td>
<td>7F</td>
<td>:22</td>
<td>1.08</td>
<td>1</td>
<td>1.21</td>
<td>1.21</td>
<td>DMrFut - G1</td>
<td>101</td>
<td>4</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>14</td>
<td>Espinoza</td>
<td>L116</td>
</tr>
<tr>
<td>9Aug14-40mr</td>
<td>6F</td>
<td>6F</td>
<td>:22</td>
<td>1.09</td>
<td>1.15</td>
<td>5</td>
<td>2½</td>
<td>Md Sp Wt 76k</td>
<td>75</td>
<td>6</td>
<td>5</td>
<td>2nd</td>
<td>21</td>
<td>29½</td>
<td>Garcia M</td>
<td>L118</td>
</tr>
</tbody>
</table>

Key Questions

-Can we use various data points ("angles") to predict which users have a higher likelihood of falling victim to a phishing attack than others?

-Are there seemingly unrelated factors that should be examined to find patterns of phishing failures?
HUMAN NATURE

SUMMED UP IN ONE PICTURE
Data Points

- 10 years of phishing test results and training data from 3 different large environments.

- Phishing related security incidents

- HR data

- Survey results

- Miscellaneous data

- Sample size of ~3,200 fails; not all correlations had the same amount of data
Elasticsearch/Kibana

- **FREE**

- Allowed for analyzing dissimilar events with different data points quickly.

- Simple to populate using Python
Failures by Years of Experience

- 0-2: 42%
- 2-4: 26%
- 4-6: 15%
- 6-8: 5%
- 8-10: 3%
- More than 10: 9%
-Subdividing the 10+ group further, 40% of the failures came from 22+ years of experience.

-New grads explained spikes....Timing changes risk!

Action: Have office managers work with “elderly” colleagues and new hires to ensure they not only complete but understand security awareness. Add additional content to new hire training.
Survey

- Did you previous employer conduct security awareness training or phishing tests?

- Do you feel internal mass communications (i.e. emails from IT, HR, benefits) are easy to identify as legitimate?
Did your previous employer conduct security awareness training or phishing tests?
- Not enough employers are investing time in training people!!!

- One round of training may not be enough.

Action: Continue to aggregate data and track participation in training programs to improved results at an individual level.
# Failures by Category

<table>
<thead>
<tr>
<th>Category</th>
<th>Failure Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Resources</td>
<td>19.8%</td>
</tr>
<tr>
<td>IT</td>
<td>13.2%</td>
</tr>
<tr>
<td>Online Services (email notifications, file sharing, etc.)</td>
<td>10.9%</td>
</tr>
<tr>
<td>Coupons</td>
<td>7.1%</td>
</tr>
<tr>
<td>Business and Financial Services</td>
<td>6.3%</td>
</tr>
</tbody>
</table>
Do you feel internal mass communications (i.e. emails from IT, HR, benefits) are easy to identify as legitimate?
- Huge disconnect between the employees and corporate communications.

(i.e. They don’t know what they don’t know)

Action: Work with corporate marketing to develop a standardized look and feel for mass communications all departments can use.
Timing

PERFECT TIMING

AT ITS FINEST
Failures by Time to Complete Training

- 0-30: 43%
- 30-60: 18%
- 60-90: 34%
- 90+: 5%
Completing the training early doesn’t mean it was effective.

People who wait for the right time to do awareness training and maximize its value are the least risky.

Action: Communicate better with staff around training reminders. Don’t make them feel rushed to complete it. If a busy time is coming up, encourage staff to complete beforehand.
-Training effects last about 60 days!

-Less frequent reinforcement = More fail.

Action: Provide frequent reinforcement. Evaluate doing multiple small trainings throughout the year vs. one large annual training.
Environmental Factors/Weird Stuff

SO THEY BLAMED IT ON

ENVIRONMENTAL FACTORS
A few more thoughts...

- Make contact human and personal

- Avoid shaming at all costs

- Contests don’t work

- Always accentuate the positive
Results

-Haven’t implemented everything yet, but still saw a nearly 2% improvement from the previous “bad” test to the next test.

-Not enough data accrued yet to decide if this is coincidental or a hard result.

-Informal, anecdotal feedback has been VERY positive!
That’s it!

- Thanks to PHV for having me and thanks to all of you!

- @tcstoolhax0r on Twitter

- Slides will be up at github.com/tcstool later

- Questions?