Implementing an Enterprise Phishing Program & Lessons Learned

Events that drove the Project

- Increase in Business Email Compromise (BEC) attempts
- Increase in Wire Transfer Requests via Spoofed email
- CEO Spoofed emails
  - Several attempts to CFO via email
  - CFO responded once, then realized it was a spoofed email.
  - Many other departments also receiving spoofed emails from CEO/CFO
- Phone calls impersonating CEO asking for Wire Transfers
- Lack of employees following annual training guidance and ad-hoc "alert" communications. Needed another layer.

Two products for PoC

- Focus was on Phishing Awareness and Correcting Negative behaviors.
- Solution needed to be SaaS
- Ability to “report” Phishing Attempts required
- Budget conscious
- Multi-Language Support

Products selected for live Proof of Concepts:

- PhishMe
- KnowBe4

PHISHME

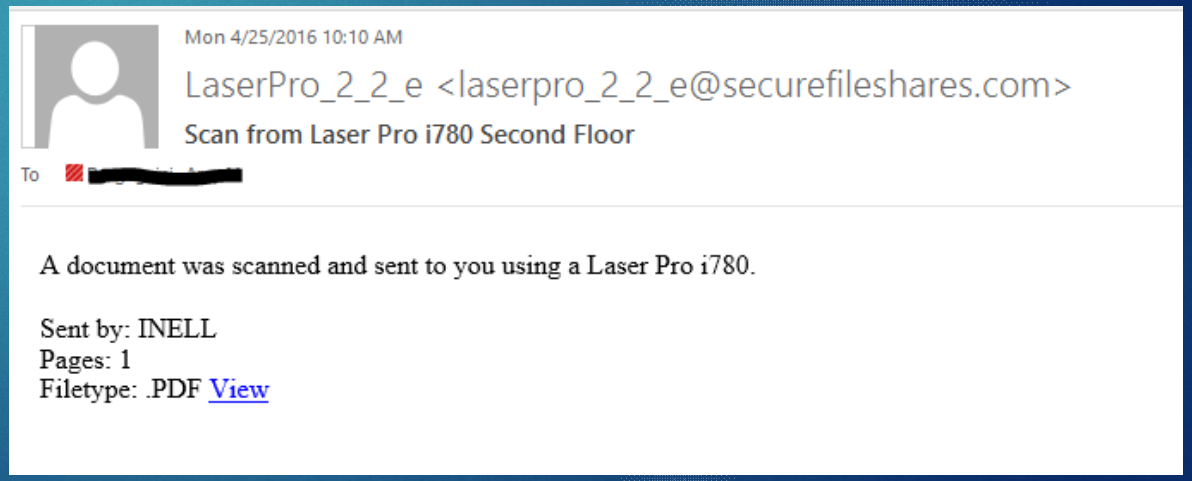
KnowBe4
Human error. Conquered.

Proof of Concept Summary

- Aligned approach with critical department heads
  - Legal
  - Compliance
  - HR
  - IT
  - Internal Audit
- Two Live tests with approximately 200 employees each with master Finance Roles in our ERP system.
- Goal was to determine ease of use with tool, feature capabilities, and reporting functionality

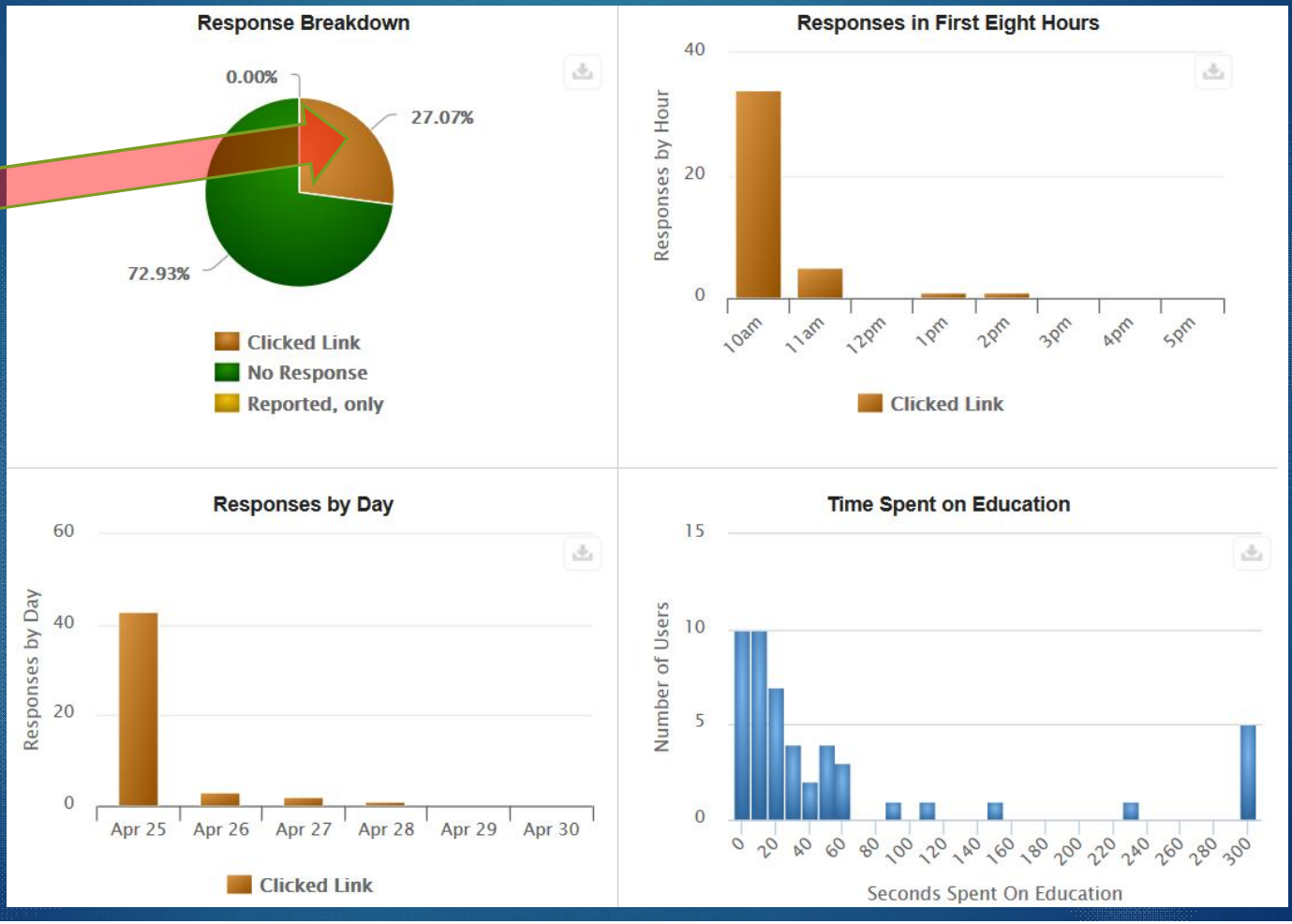
Baseline Tests

- SCOPE:
  - 180 ERP users
  - 20 Highly Visible email addresses found publicly on the internet
  - Test lasted 5 days.
- SCENARIO:
  - "Click Only" email scenario.
  - Simulated an attached PDF from an external multi-function device.
  - Clicks on the "View" link counted as a "Clicked Link"



Baseline Results!

27% CLICK RATE!!



Time to Choose a Platform

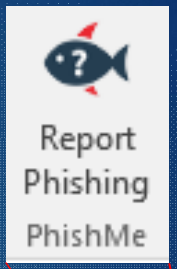
- Although platforms were very comparable, we chose PhishMe
- Long and trusted history with vendor
- PhishMe purposely does not use Copyright images in their scenarios
- Support team was very prompt
- Good multi-language support
- PhishMe Reporter prompts default to system language

Program

- Baseline tests were done without advanced notice
- Communication campaign launched
- Announced the Phishing program globally
- Announced the new way to report Phishing attempts
- Announced exclusive “prize” for first employee to correctly identify and report via PhishMe button a phishing scenario
- Summary emails of how the company did at the end of each scenario.
  - Publically “celebrate” the first employees to report and announce that they won a prize.

Report Phishing Attempts

- Outlook add-in button for reporting Phishing attempts
  - Announced and added via SCCM to all users Outlook ribbon
  - Also shows up via “right-clicking” an email in the Outlook inbox
- End user action is identical regardless of real or scenario Phish
- Reporter displays different messages when clicked
  - If real Scenario, displays “Congratulations! You have correctly identified a phishing attempt, thank you for keeping us safe!”
  - If real Phish, displays “Thank you for reporting the phishing attempt. The message has been routed to the InfoSec team for appropriate action”.



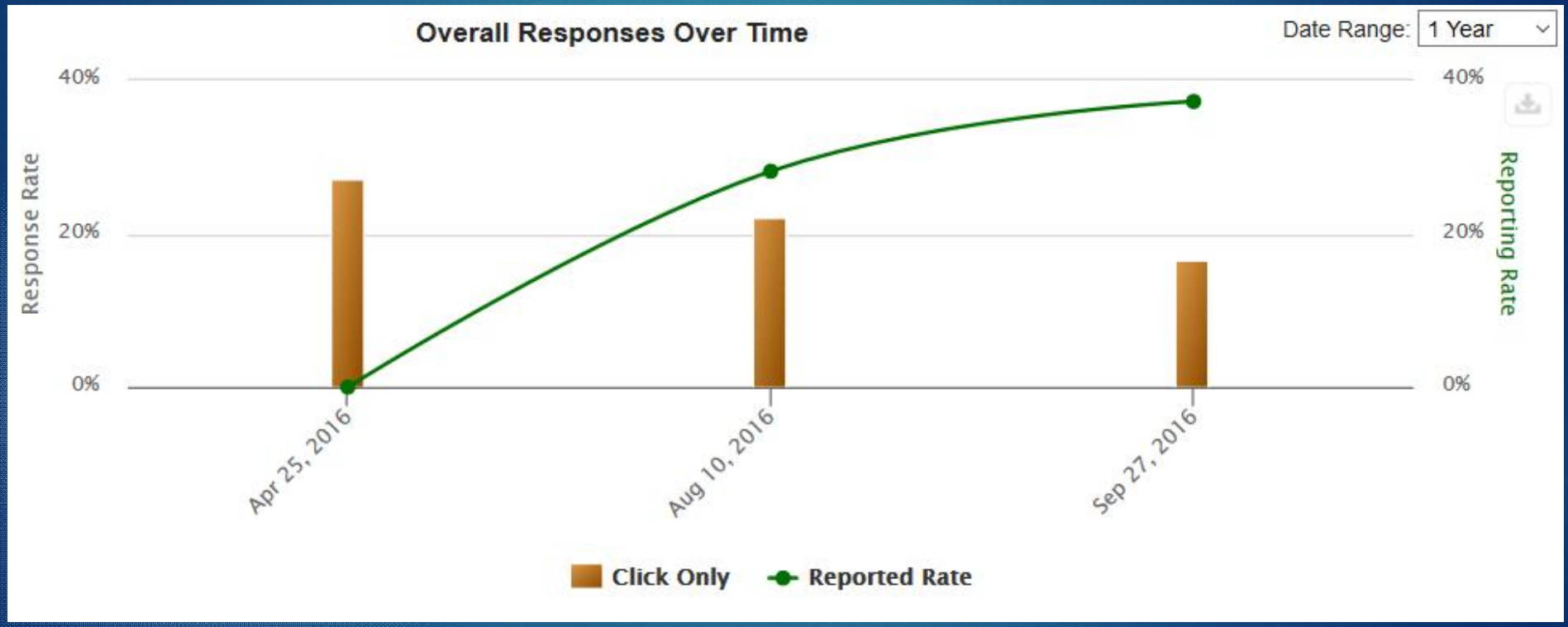
Progam Announcment

[Custom Emails Details Removed]

Reporter Announcement

[Custom Emails Details Removed]

Trends


Overall Responses Over Time
Date Range:
1 Year
40%
20%
0%
Response Rate
Reporting Rate
Apr 25, 2016
Aug 10, 2016
Sep 27, 2016
Click Only
Reported Rate

Repeat Offenders

- After first three scenarios, 275 users had a 100% click rate
- This represents about 8% of our workforce apparently will click and open anything.
- Future thoughts – provide additional live training to repeat offenders
  - Determine threshold at which point you notify employees manager
  - Determine if we take further action for repeat offenders

Lessons Learned

- We allowed external emails spoofing our domain to come in.
  - This has been stopped.
  - Lots of whitelisting
- Focus on correcting negative behaviors in a positive way
- Communication is required
- Partner with Infrastructure, Legal, Compliance, HR
  - Infrastructure may be your Triage team
- Lots of “spam” being reported as phishing.
  - Goal is to train users what Phishing really is, and to report Phishing and not spam

Thank you!