Gone Phishing, an Anti-Phishing Program Journey

Ava Logan-Woods, Information Security Specialist
Eshante Lovett, Information Security Specialist
CACI International Inc
6/19/2017
CACI International Inc Overview

- Founded in 1962
- Approximately 20,000 employees worldwide with over 120 locations.
- CACI provides information solutions and services in support of national security missions and government transformation for Intelligence, Defense, and Federal Civilian customers.
- Member of Fortune 1000 Largest Companies, the Russell 2000 Index, and the S&P SmallCap600 Index.
Overview

- Introduction
- The Journey
- Success Factors
- Setting Up the Anti-Phishing Program
- Lessons Learned
- Summary
Quick Phacts

- April 2013 company baseline assessment was at a **25%** susceptibility rate.

- CACI employees have been receiving phishing awareness training for about 4 years.

- January’s susceptibility rate was **2.8%**

- February’s susceptibility rate was **26%**

From: HR <mdexecutive@sendsecure.eu>
Subject: Attn!! W-2 Amended
CACI's Phishing Journey

Awareness Program – 2009 to present

- **2010-2011**: Budget approved for staff and phishing tool.
- **2012**: Process work, first phishing campaign
- **2013**: Pitching Phishing Awareness Program
- **2014**: Getting senior management buy-in for escalations
- **2015**: Escalations started, more company engagement
- **2016**: Generate context from metrics, improve campaign sophistication
- **2017**: Continue to show value in program, more employee engagement

- All quiet on the pitching front
- Budget scare
The First Phishes – Ad hoc

- **Campaigns:**
  - Varying number of emails sent over the months
  - Varying groups sent emails over different months
  - Missing months

- **Metrics Reporting:**
  - First few campaigns weren’t reported up to management
  - Ad hoc, thereafter

---

**Susceptibility Rates in the First Year of Phishing**

<table>
<thead>
<tr>
<th>Date</th>
<th>Emails Sent</th>
<th>Susceptibility Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/12/2013</td>
<td>0</td>
<td>0.00%</td>
</tr>
<tr>
<td>5/12/2013</td>
<td>2000</td>
<td>10.00%</td>
</tr>
<tr>
<td>6/12/2013</td>
<td>8000</td>
<td>40.00%</td>
</tr>
<tr>
<td>7/12/2013</td>
<td>12000</td>
<td>50.00%</td>
</tr>
<tr>
<td>8/12/2013</td>
<td>14000</td>
<td>60.00%</td>
</tr>
<tr>
<td>9/12/2013</td>
<td>10000</td>
<td>50.00%</td>
</tr>
<tr>
<td>10/12/2013</td>
<td>8000</td>
<td>40.00%</td>
</tr>
<tr>
<td>11/12/2013</td>
<td>6000</td>
<td>30.00%</td>
</tr>
<tr>
<td>12/12/2013</td>
<td>4000</td>
<td>20.00%</td>
</tr>
<tr>
<td>1/12/2014</td>
<td>2000</td>
<td>10.00%</td>
</tr>
<tr>
<td>2/12/2014</td>
<td>0</td>
<td>0.00%</td>
</tr>
<tr>
<td>3/12/2014</td>
<td>2000</td>
<td>10.00%</td>
</tr>
<tr>
<td>4/12/2014</td>
<td>8000</td>
<td>40.00%</td>
</tr>
<tr>
<td>5/12/2014</td>
<td>12000</td>
<td>50.00%</td>
</tr>
<tr>
<td>6/12/2014</td>
<td>14000</td>
<td>60.00%</td>
</tr>
<tr>
<td>7/12/2014</td>
<td>10000</td>
<td>50.00%</td>
</tr>
<tr>
<td>8/12/2014</td>
<td>8000</td>
<td>40.00%</td>
</tr>
<tr>
<td>9/12/2014</td>
<td>6000</td>
<td>30.00%</td>
</tr>
<tr>
<td>10/12/2014</td>
<td>4000</td>
<td>20.00%</td>
</tr>
<tr>
<td>11/12/2014</td>
<td>2000</td>
<td>10.00%</td>
</tr>
<tr>
<td>12/12/2014</td>
<td>0</td>
<td>0.00%</td>
</tr>
</tbody>
</table>
**Current Phishing – Quarterly Testing**

- **Campaigns**
  - Every month, 1/3 of the company is tested
  - Clickers are automatically enrolled in the next campaign (started late 2014)
  - Using real-world examples to be more relevant

- **Metrics Reporting**
  - Reporting monthly to Information Security management
  - Reporting quarterly and annually to senior management and the board of directors.

---

**Susceptibility Rates for the Past Year**

- **Clickers** are 30.00% automatically enrolled in the next campaign (started late 2014)
- 25.00% in 6200
- 20.00% in 6000
- 15.00% in 5800
- 10.00% in 5600
- 5.00% in 5400
- 0.00% in 5200

**Difficulty**

- Emails sent
- Response rate
Moving the Phishing Program Forward

- **Campaigns**
  - Increase the frequency
  - Include enrolled interactive training as part of the escalation process.
  - Make reporting phishing emails easier by implementing a “reporter” button.
  - Target more susceptible populations and higher value targets

- **Metrics Reporting**
  - Providing better/more intelligence
  - Report on different susceptible populations
## Success Factors

### People
- Executive support
- Dedicated resources on the Information Security team
- Cross-departmental resources (HR, Corporate Communications, IT, Training)

### Processes & Policies
- Report a Phish process
- Escalation process
- Campaign process
- AUA and Awareness Program policy

### Technology
- Leveraged mail analysis tool for program justification
- Building campaigns
- Training & Communication
- Data compilation and analysis
Setting Up CACI’s Anti-Phishing Program

1. Recognize the risk
2. Lay the foundation – getting others to recognize the risk
3. Lobby for resources
4. Scan the market, in-house or vendor provided tool, understand requirements, what would it look like?
5. Flesh out the implementation plan
   - How will you integrate this program?
   - Consider staffing – there is work before, during, and after the campaign
   - First processes planned; experience changes things
6. Phish & Report - this will evolve over time.
7. Continuous Improvement
Lessons Learned

- The first test set the tone for what needed to be done. Each time we phished, we learned more.
- Never underestimate collaboration with the IT department.
- Some groups needed to be excluded.
- Consequences of reporting training results - these are humans.
- Sophistication levels need to be fleshed out and change over time.
- The anti-phishing program is a living, changing thing.
- Success isn’t solely based on low click rates.
- Escalation is controversial.
- Tracking the data is crucial.
- Keep up the hype.

*The technology doesn’t make the change, it’s the vehicle to touch the users directly*
How to Spot Success

- **Getting Buy-in**
  - Blog
  - Community of Practice

- **Money for swag**

- **Corporate messaging is getting more attention**

- **More engagement with employees**
  - People reporting – “I Clicked!”
  - “I got this email that’s a bit suspicious…..”

- **Fewer angry emails; More pleasant emails**
“KEEP SENDING CRAP ON MY GOVERNMENT COMPUTER AND I WILL KEEP OPENING IT UNTIL THE GOVERNMENT CONTACTS YOU”

“Thank you very much for the notice. I was on vacation last week when I rec’d this message and I clicked on it from my phone and knew it was a mistake immediately. I intended to send a message to <incident response email> to let you know of my error but am still digging out from work emails. I have read info below and completely understand the importance of this topic and will exercise extra diligence going fwd (even on vacation).”
Summary

- The beginning of our program was all about learning and we continue to do so.
- You’re in it for the long haul ... the program doesn’t change things overnight.
- Promoting the program is critical to its success – share wins
- The Anti-Phishing Program has helped promote the Information Security team, influence policy, increase interest in the Awareness Program, and improve relationships.
- The Information Security team is seen as more accessible now.
QUESTIONS