Apples, Oranges...

...and Phish

John Scott
Head of Security Education
Bank of England
What’s the problem?

Why Cofense PhishMe?

With over 29 million employees trained in 160 countries, Cofense PhishMe has been proven to reduce the threat of employees falling victim to advanced cyber attacks by up to 95% — preparing your last line of defense to recognize and resist tricky phishing attempts.

OVERVIEW

Engage your end users and arm them against real-world cyber attacks, using personalised security awareness training based on our industry-leading threat intelligence. Instead of wasting time with one-size-fits-all content, we help you deliver the right cybersecurity awareness training to the right people at the right time.

Our SaaS-based solutions and Continuous Training Methodology were developed by Wombat Security Technologies (acquired in March 2018) and born from research at the world-renowned Carnegie Mellon University. Using them, customers have reduced successful phishing attacks and malware infections by up to 90%.

Fortunately, the data showed that this 30% can be brought down more than half to just 15% in only 90 days by deploying new-school security awareness training. The 365-day results show that by following these best practices, the final Phish-prone percentage can be minimized to 2% on average.

What’s the problem?

Why Cofense PhishMe?

With over 29 million employees trained in 160 countries, Cofense PhishMe has been proven to reduce the threat of employees falling victim to advanced cyber attacks by up to 95% — preparing your last line of defense to recognize and resist tricky phishing attempts.

OVERVIEW

Engage your end users and arm them against real-world cyber attacks, using personalised security awareness training based on our industry-leading threat intelligence. Instead of wasting time with one-size-fits-all content, we help you deliver the right cybersecurity awareness training to the right people at the right time.

Our SaaS-based solutions and Continuous Training Methodology were developed by Wombat Security Technologies (acquired in March 2018) and born from research at the world-renowned Carnegie Mellon University. Using them, customers have reduced successful phishing attacks and malware infections by up to 90%.

Fortunately, the data showed that this 30% can be brought down more than half to just 15% in only 90 days by deploying new-school security awareness training. The 365-day results show that by following these best practices, the final Phish-prone percentage can be minimized to 2% on average.
Up to 95%
Up to 90%
Minimised to 2%
How to lie with statistics

- 95% of what?
- Compared to what?
- Using what phish?
- Show your working!
**ROYAL BANK of NIGERIA**

I have emailed everyone I can possibly find, my Prince, but no-one wants to help you move your money.

---

**Today**

<table>
<thead>
<tr>
<th>Time</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:51 AM</td>
<td>Canceled Call</td>
</tr>
<tr>
<td>11:47 AM</td>
<td>Incoming Call</td>
</tr>
<tr>
<td>11:44 AM</td>
<td>Incoming Call</td>
</tr>
</tbody>
</table>

**main**

1 (800) MYAPPLE

homepage
http://www.apple.com
More conversations with my boss

Clicked (%)
Oh ... and ...
So ...

Metrics for CISO
+ Need for thesis subject
+ Dissatisfaction with click rate as a stat
= An idea!
The Idea

• Create 10 phishing emails of different levels of sophistication
• Ask Security Awareness professionals to rate them
• Run those phishes against my organisation to compare the ratings
<table>
<thead>
<tr>
<th>Phish 01</th>
<th>SIMPLE Urgent help needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phish 02</td>
<td>SIMPLE Governor Request</td>
</tr>
<tr>
<td>Phish 03</td>
<td>BASIC Check CV</td>
</tr>
<tr>
<td>Phish 04</td>
<td>BASIC Contact Info</td>
</tr>
<tr>
<td>Phish 05</td>
<td>INTERMEDIATE Secure email</td>
</tr>
<tr>
<td>Phish 06</td>
<td>INTERMEDIATE Compromised Account</td>
</tr>
<tr>
<td>Phish 07</td>
<td>DIFFICULT discussed link</td>
</tr>
<tr>
<td>Phish 08</td>
<td>DIFFICULT Spam mail removal</td>
</tr>
<tr>
<td>Phish 09</td>
<td>COMPLEX GDPR Breach</td>
</tr>
<tr>
<td>Phish 10</td>
<td>COMPLEX Information Leak</td>
</tr>
</tbody>
</table>
Stage 2: The Wisdom of the Crowds

- 2 stage process:
  - Assess each phish by ‘gut reaction’ – 1-5
    - “Would this work in my organisation?”
  - Assess each phish on 5 psychological triggers
Stage 2: 5 psychological triggers

- Authority
- Curiosity
- Punishment or reward
- Time pressure
- Specificity
Stage 3: test the phishes live

- Run against my own organisation
  - 5500 people, so roughly 550 people per phish
  - Run 3 times to different groups each time (July, October, January)
  - Get an average susceptibility per phish

https://tinyurl.com/phishingMSc
Stage 4: Analysis

• Do the assessments carried out in stage 2 match the actual phishes in stage 4?
• Does it make a difference if the person doing the assessment in stage 2 works in Security Awareness?

https://tinyurl.com/phishingMSc
So did it work?

Short answer?

No.
Results from the surveys

- No correlation between the triggers and susceptibility
Are we better at spotting good phishes?

- 47.2% responses from Security Awareness practitioners
- 35.1% from Security but not Awareness practitioners
- 17.6% from non-Security practitioners
The interim results

Psy*Gut vs Susceptibility (SA)

Psy*Gut vs Susceptibility (SC)

Psy*Gut vs Susceptibility (Non-Sec)
3 takeways

• How would this have worked in a less mature organisation?
• Were these the right triggers?
• If this doesn’t work, how do we measure the different susceptibility levels?
Can I help?

https://tinyurl.com/phishingMSc

John Scott MSc
Thesis
Photo credits

- Slide 1: CC BY 2.0 EWS@Flickr
- Slide 1: CC BY-NC-ND 2.0 Vipez@flickr
- Slide 4: © Irving Gells, 1954
- Slide 9: Free to use from Pixabay

https://tinyurl.com/phishingMSc