Apples, Oranges…

John Scott
Head of Security Education
Bank of England

…and Phish

What's the problem?

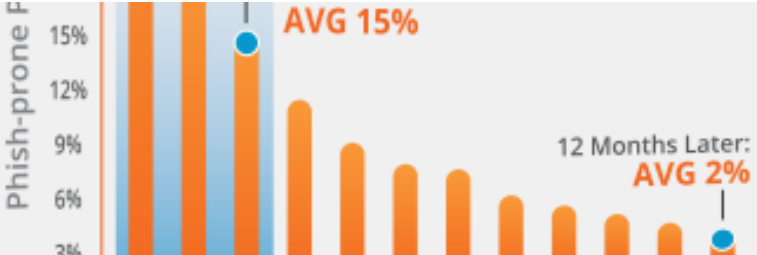
Why Cofense PhishMe?

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

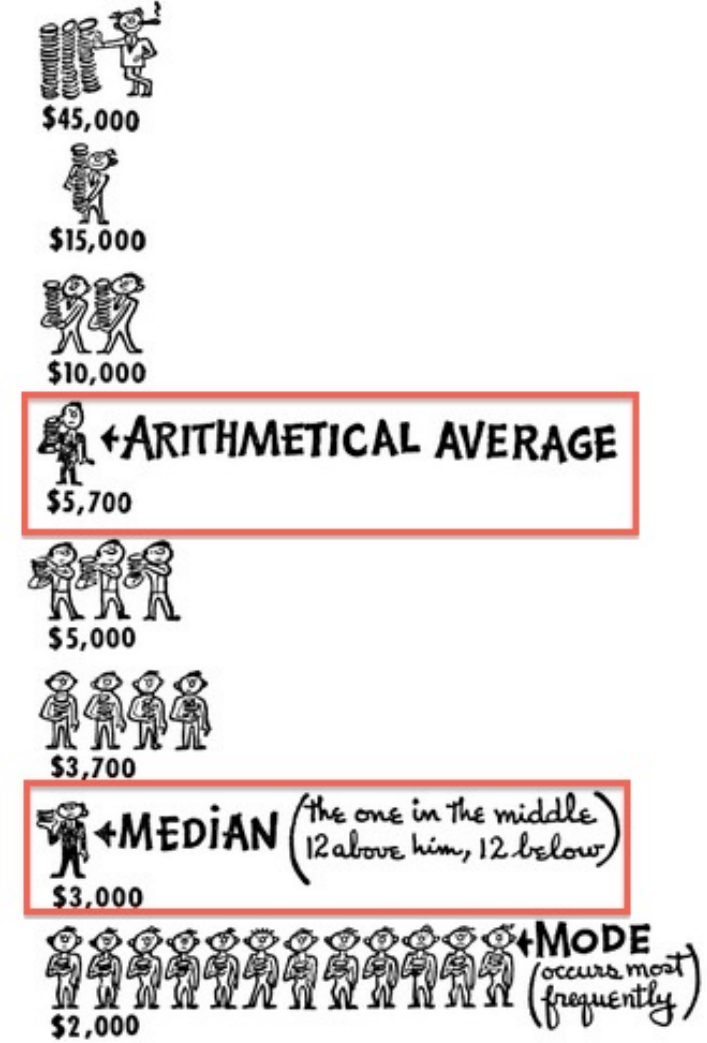
Engage your end users and arm them against real-world cyber attacks, using personalised security awareness training based on our industry-leading threat intelligence. Instead of wasting time with one-size-fits-all content, we help you deliver the right cybersecurity awareness training to the right people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

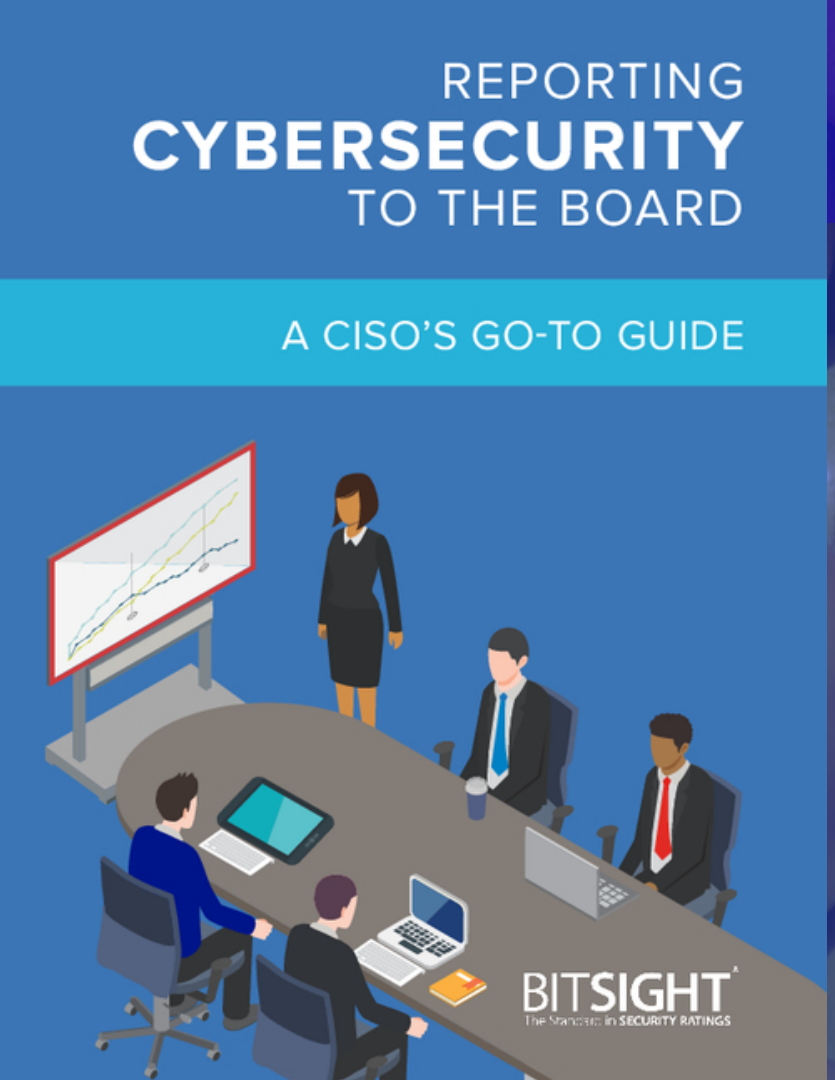

Up to 95%
Up to 90%
Minimised to 2%

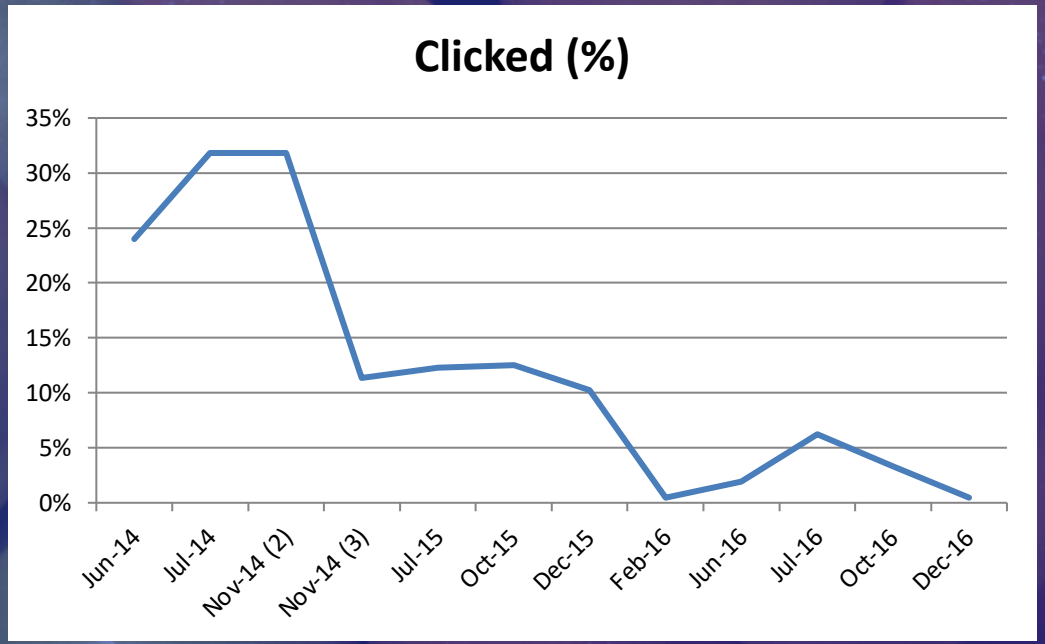


How to lie with statistics

- 95% of what?
- Compared to what?
- Using what phish?
- Show your working!

Conversations with my boss





Sophisticated?

To: [your email address]

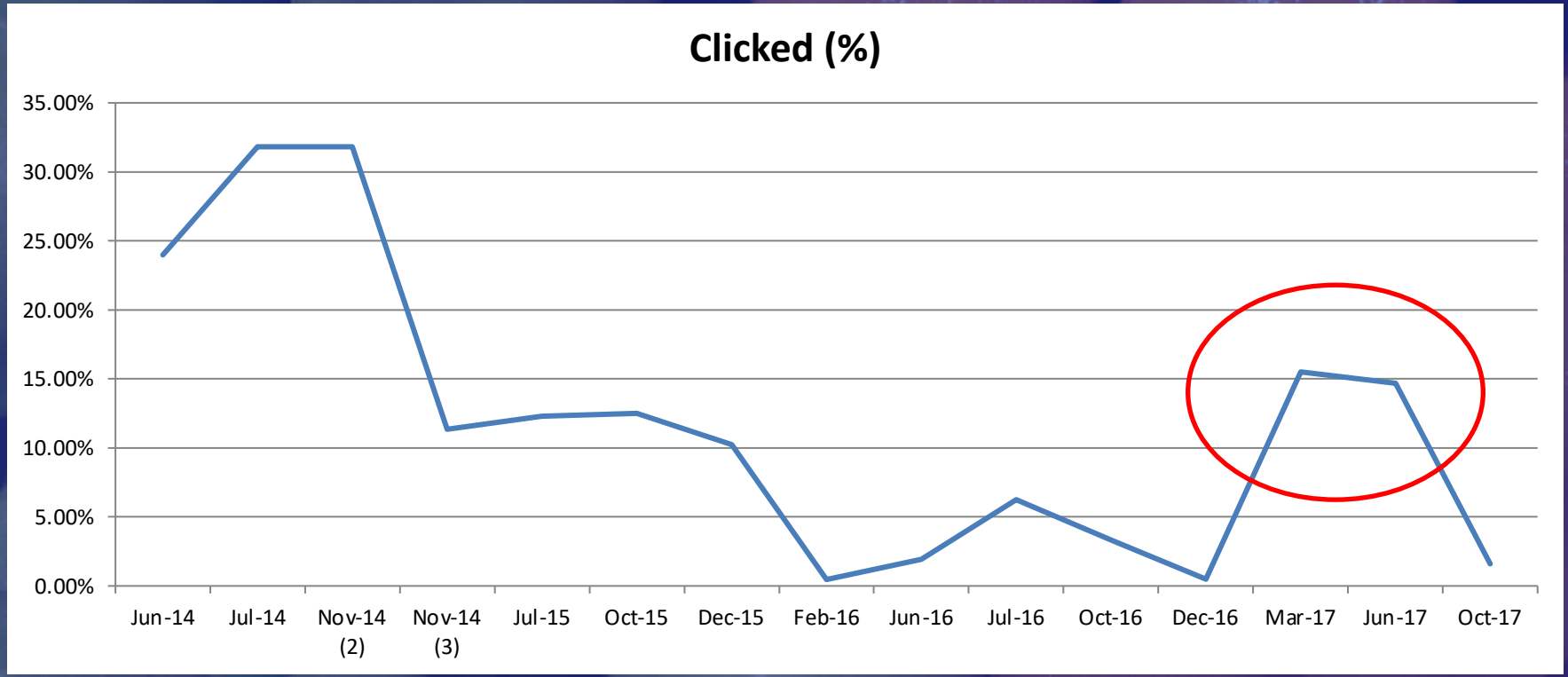
From: peter123@gmail.com

Subject: FYI

Attachment: doc1.doc

Body text:

More conversations with my boss



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

Stage 1: 10 Phishes

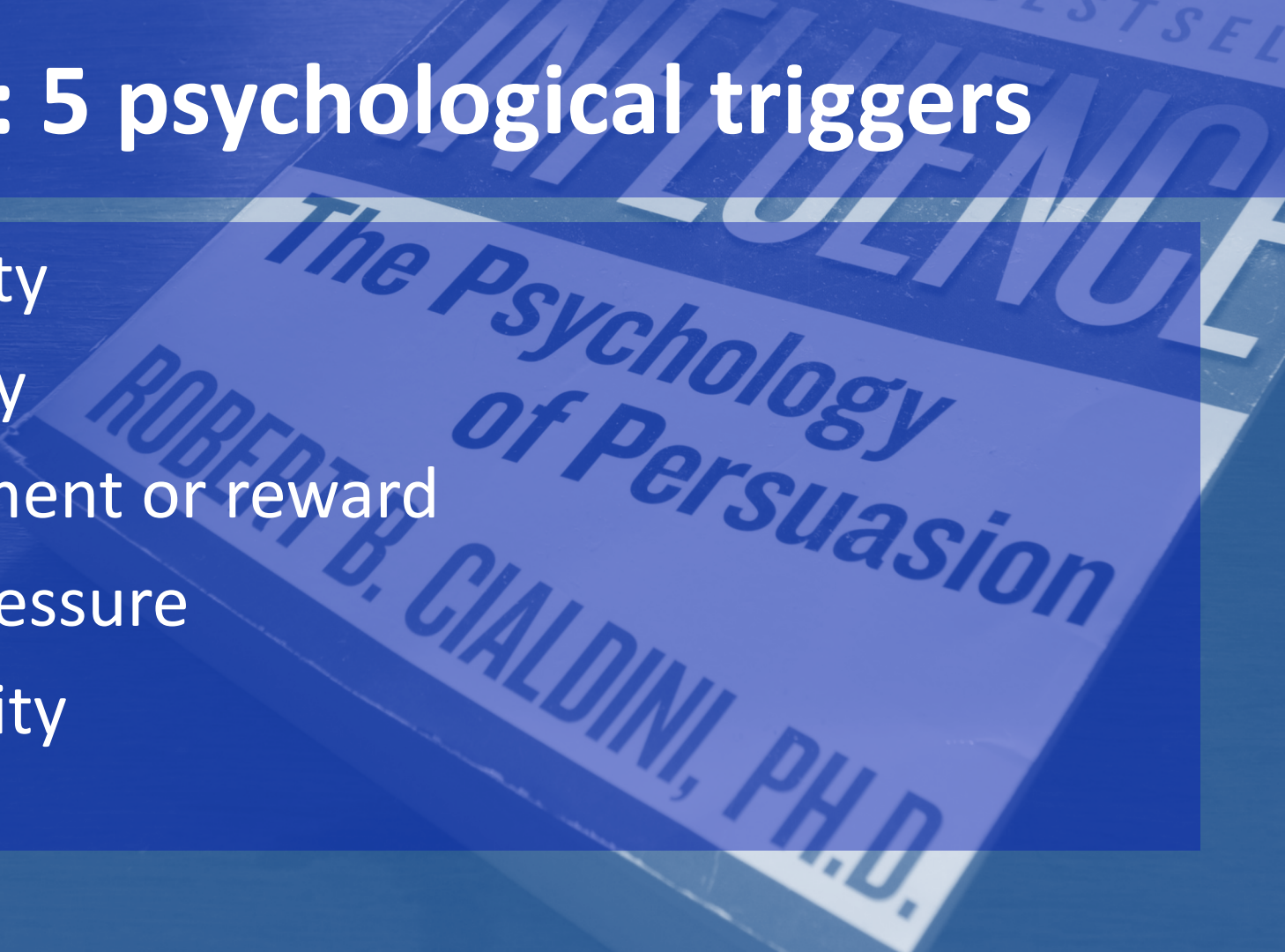
Phish 01	SIMPLE Urgent help needed
Phish 02	SIMPLE Governor Request
Phish 03	BASIC Check CV
Phish 04	BASIC Contact Info
Phish 05	INTERMEDIATE Secure email
Phish 06	INTERMEDIATE Compromised Account
Phish 07	DIFFICULT discussed link
Phish 08	DIFFICULT Spam mail removal
Phish 09	COMPLEX GDPR Breach
Phish 10	COMPLEX Information Leak

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



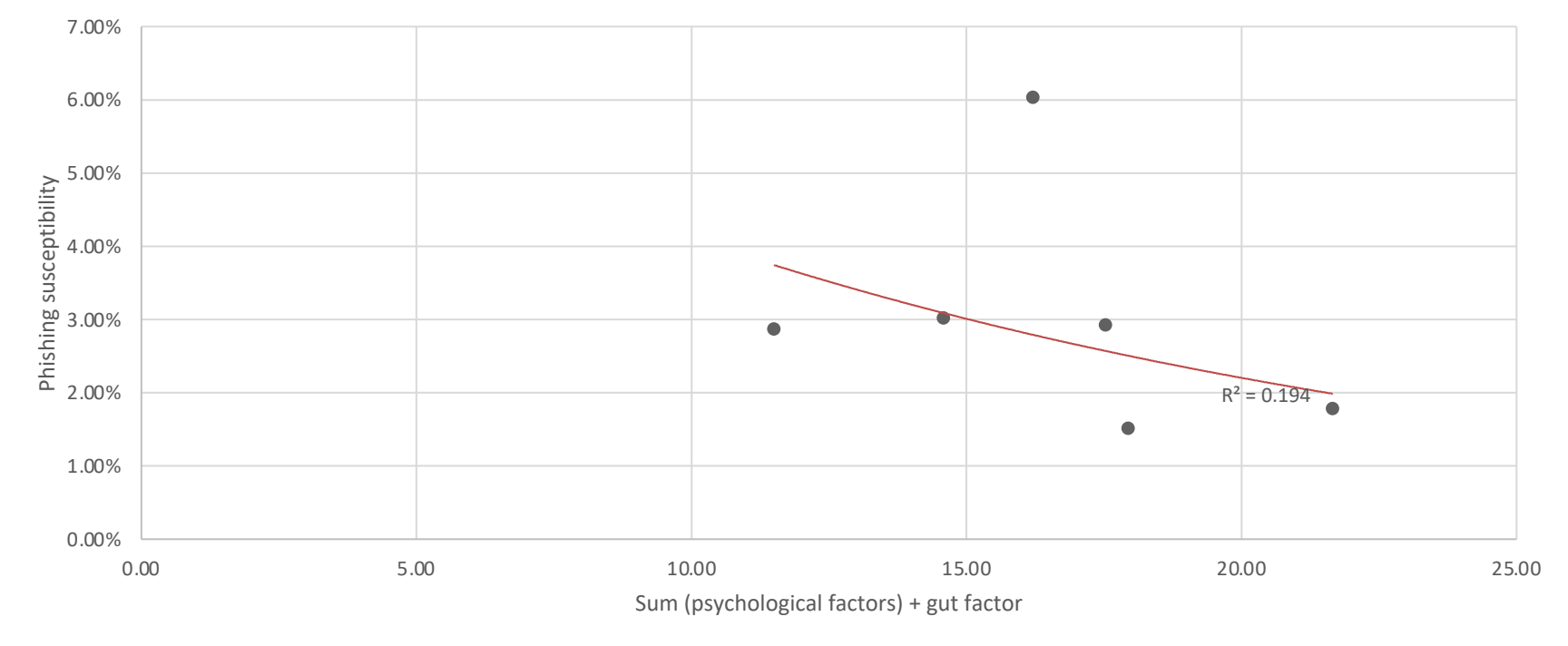
Stage 3: test the phishes live

- 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

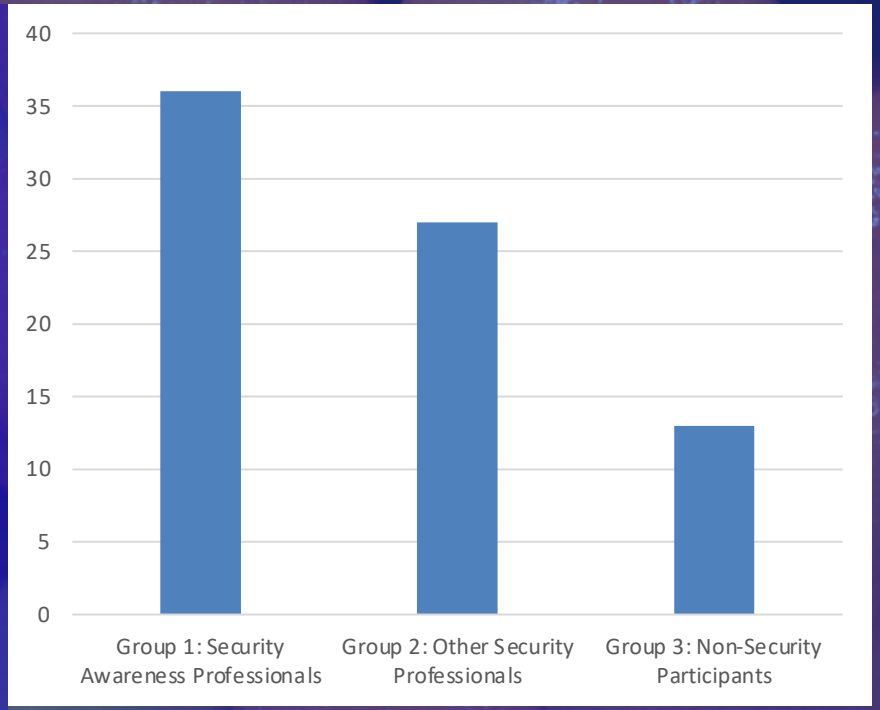
Stage 4: Analysis

- 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?

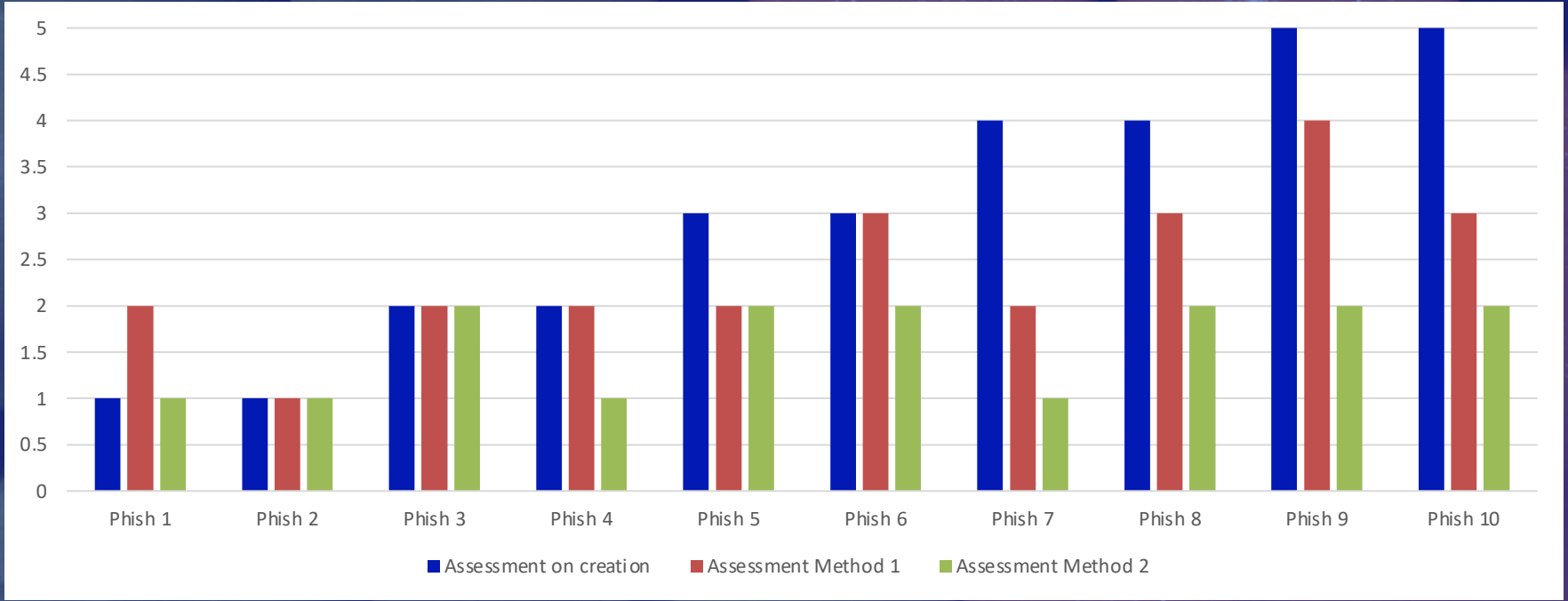
So, did it work? … kinda ….



- **47.2%** responses from Security Awareness practitioners
- **35.1%** from Security but not Awareness practitioners
- **17.6%** from non-Security practitioners



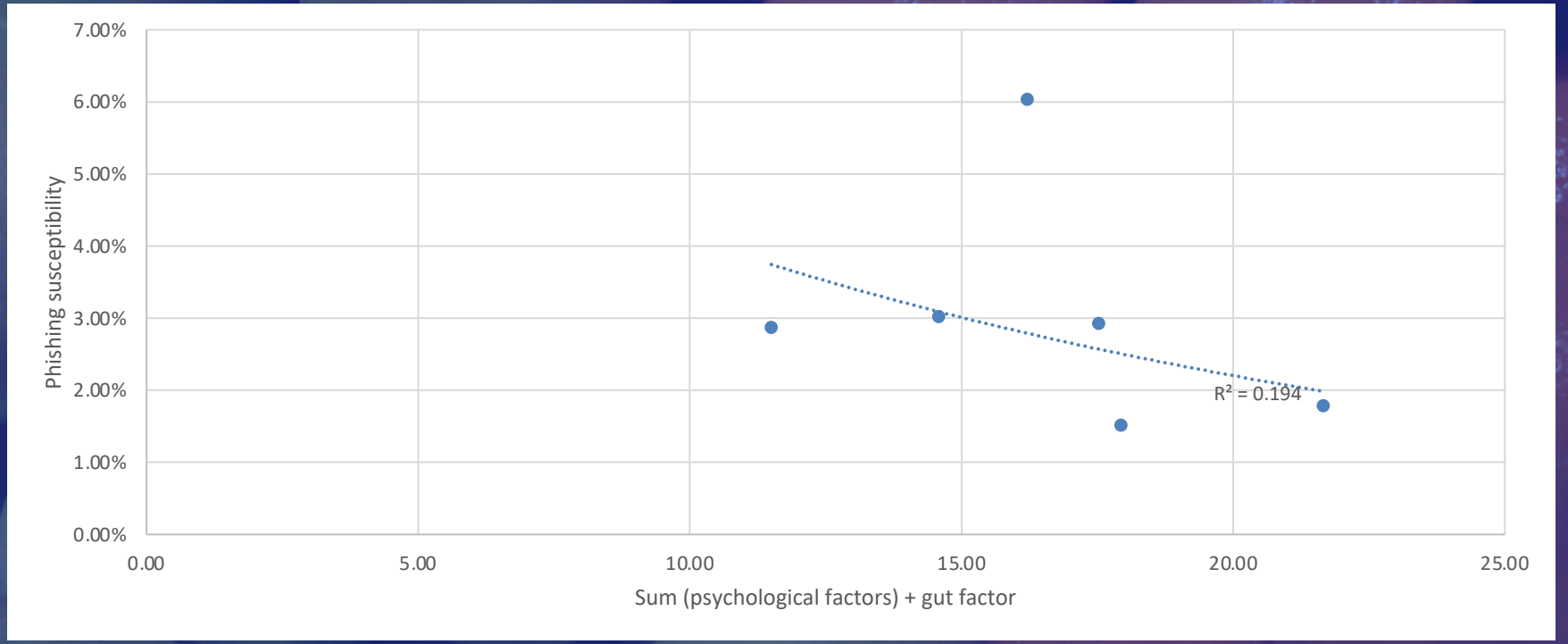
Results from the surveys



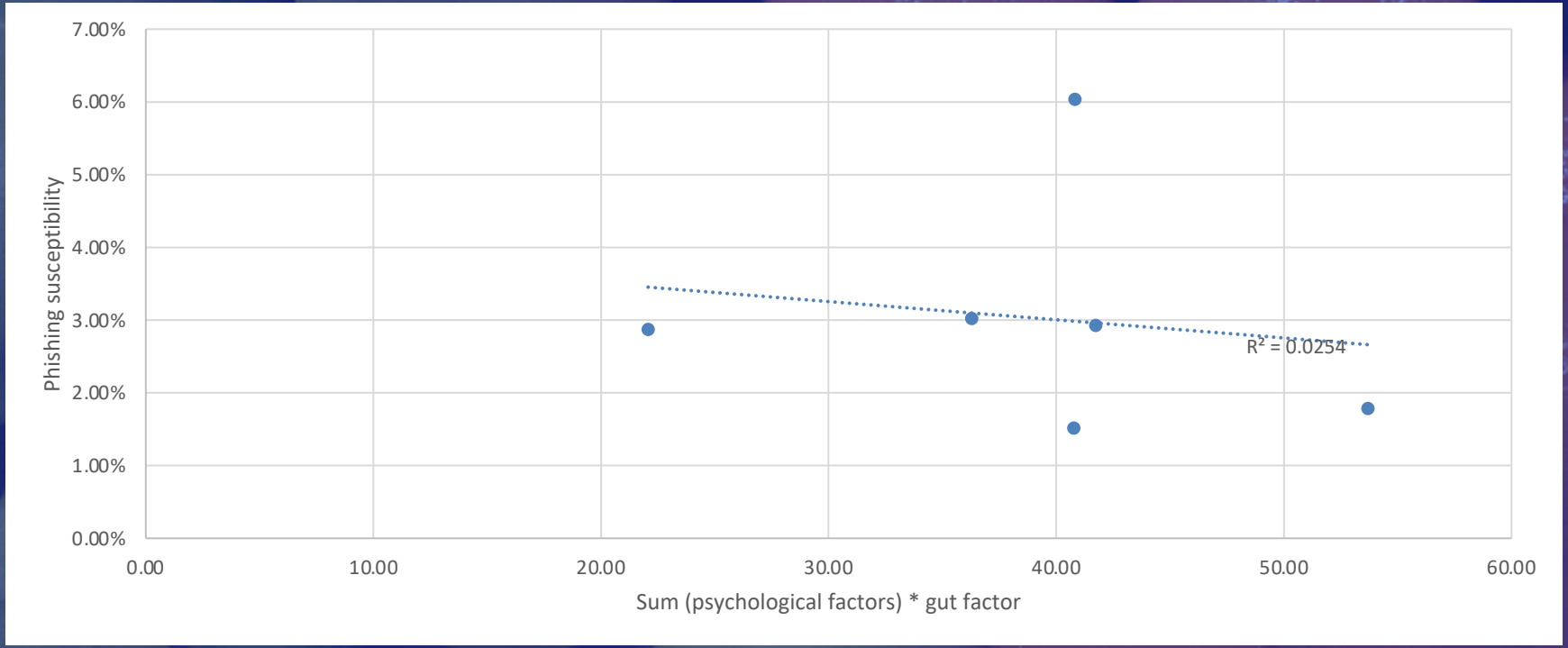
Phishing susceptibility rates

Phish 01	SIMPLE Urgent help needed	0.00%
Phish 02	SIMPLE Governor Request	0.00%
Phish 03	BASIC Check CV	3.02%
Phish 04	BASIC Contact Info	0.00%
Phish 05	INTERMEDIATE Secure email	6.03%
Phish 06	INTERMEDIATE Compromised Account	1.52%
Phish 07	DIFFICULT discussed link	2.87%
Phish 08	DIFFICULT Spam mail removal	0.00%
Phish 09	COMPLEX GDPR Breach	1.78%
Phish 10	COMPLEX Information Leak	2.92%

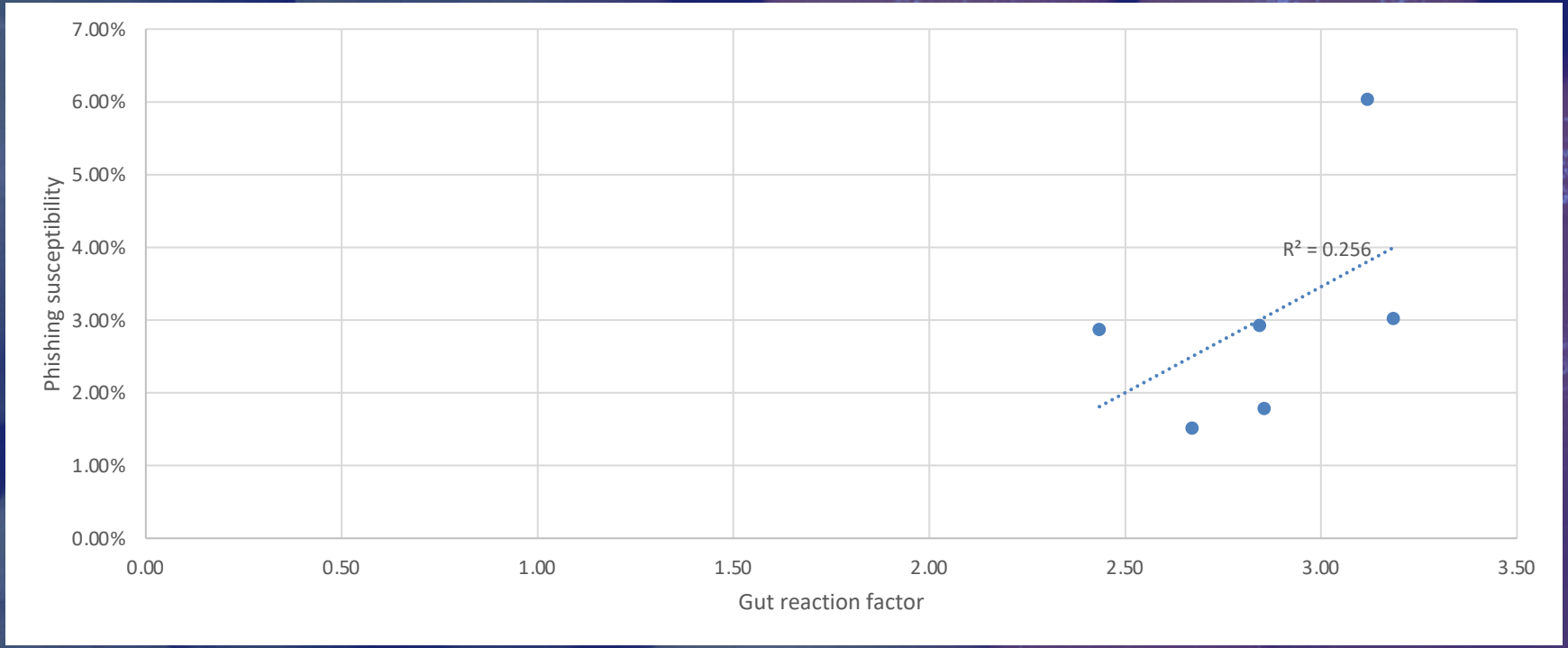
The results – Method 1



The results – Method 2



The results – Method 3



3 takeways

- Gut feel is important, but not just your own gut feel.
- Running the same phishes against a different organisation would be interesting
- If this doesn’t work, how do we measure the different susceptibility levels?

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