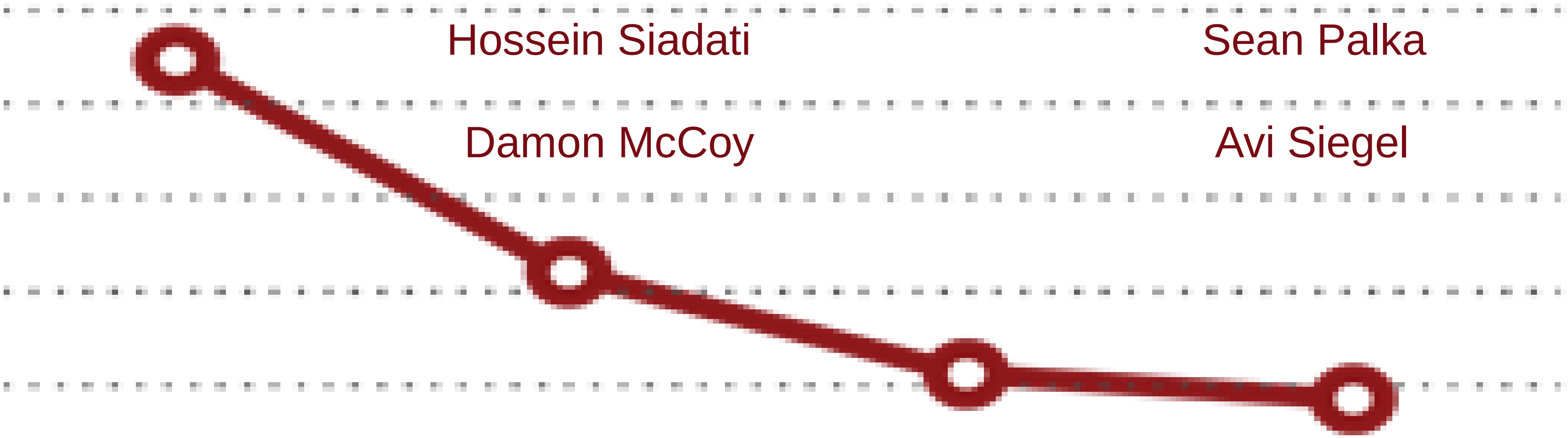
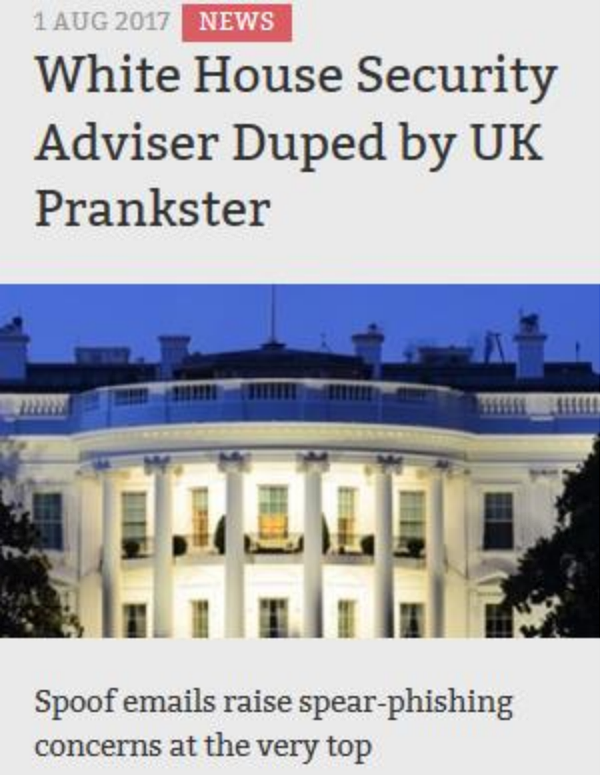
10th USENIX Workshop on Cyber Security Experimentation and Test

Measuring the Effectiveness of Embedded Phishing Exercises



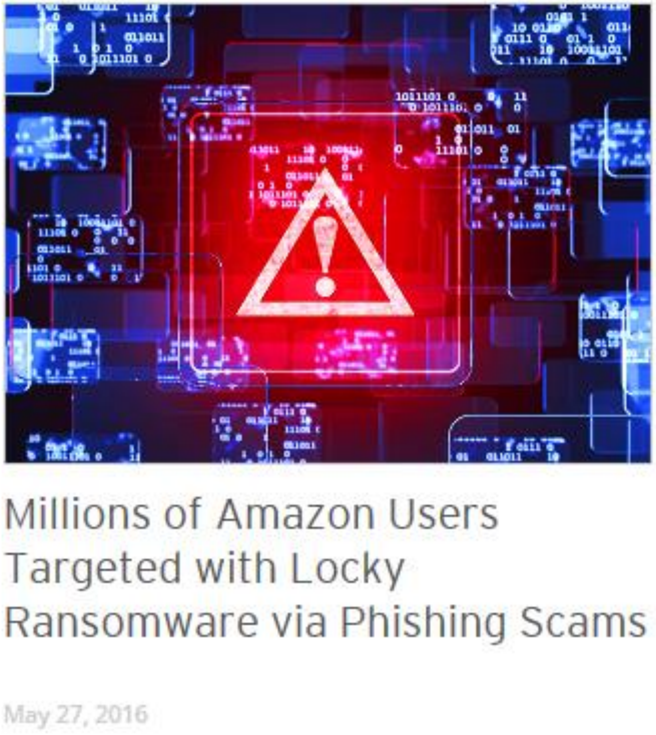
Hossein Siadati
Sean Palka
Damon McCoy
Avi Siegel



1 AUG 2017 NEWS

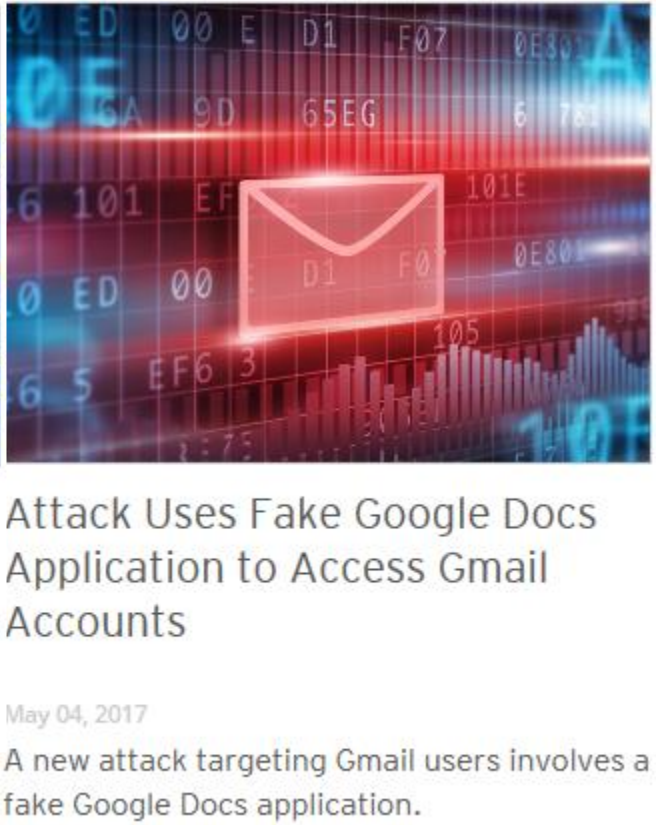
White House Security Adviser Duped by UK Prankster

Spoof emails raise spear-phishing concerns at the very top



Millions of Amazon Users Targeted with Locky Ransomware via Phishing Scams

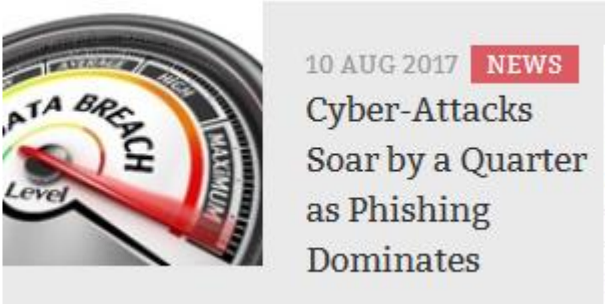
May 27, 2016



Attack Uses Fake Google Docs Application to Access Gmail Accounts

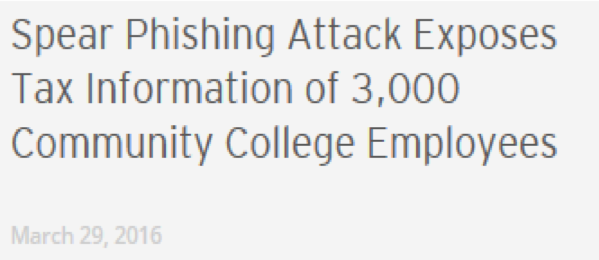
May 04, 2017

A new attack targeting Gmail users involves a fake Google Docs application.



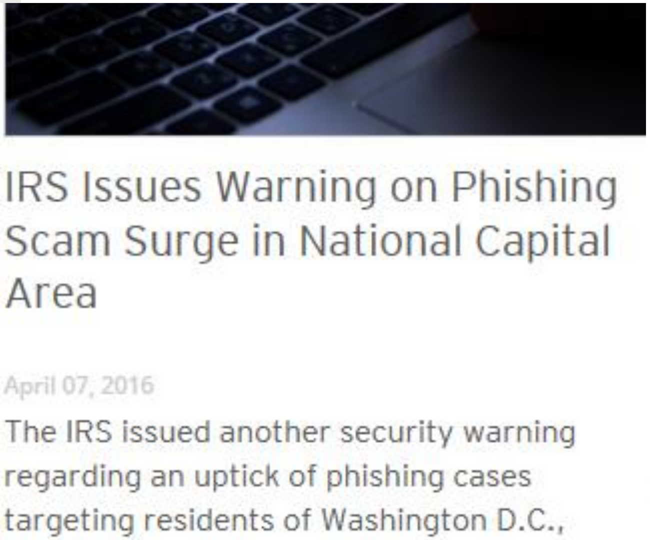
10 AUG 2017 NEWS

Cyber-Attacks Soar by a Quarter as Phishing Dominates



Spear Phishing Attack Exposes Tax Information of 3,000 Community College Employees

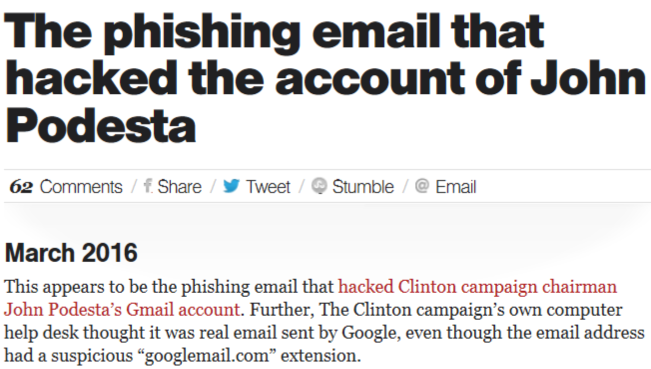
March 29, 2016



IRS Issues Warning on Phishing Scam Surge in National Capital Area

April 07, 2016

The IRS issued another security warning regarding an uptick of phishing cases targeting residents of Washington D.C.,



The phishing email that hacked the account of John Podesta

62 Comments / Share / Tweet / Stumble / Email

March 2016

This appears to be the phishing email that hacked Clinton campaign chairman John Podesta's Gmail account. Further, The Clinton campaign's own computer help desk thought it was real email sent by Google, even though the email address had a suspicious "googlemail.com" extension.

Embedded Phishing Exercises Overview

- Content Creation
  - A limited set of phishing emails are manually or automatically generated by subject matter experts for each embedded phishing exercise.
- Grouping
  - Users are partitioned into cohorts or exercise groups, and exercise content is determined for each cohort.
- Execution
  - Users are sent e-mails.
  - Clicking links results in some action, typically static or interactive training
  - Multiple rounds of testing are typical
- Evaluation
  - Effectiveness measures are evaluated to determine improvement metrics
  - This is the perhaps most important phase, with the least established approach

THE PROBLEM

Untrained users are a significant exploitable weakness of many modern IT systems.

Anti-phishing measures such as user awareness training try to prevent phishing attacks from succeeding.

Determining whether the anti-phishing measures are effective presents significant difficulties.

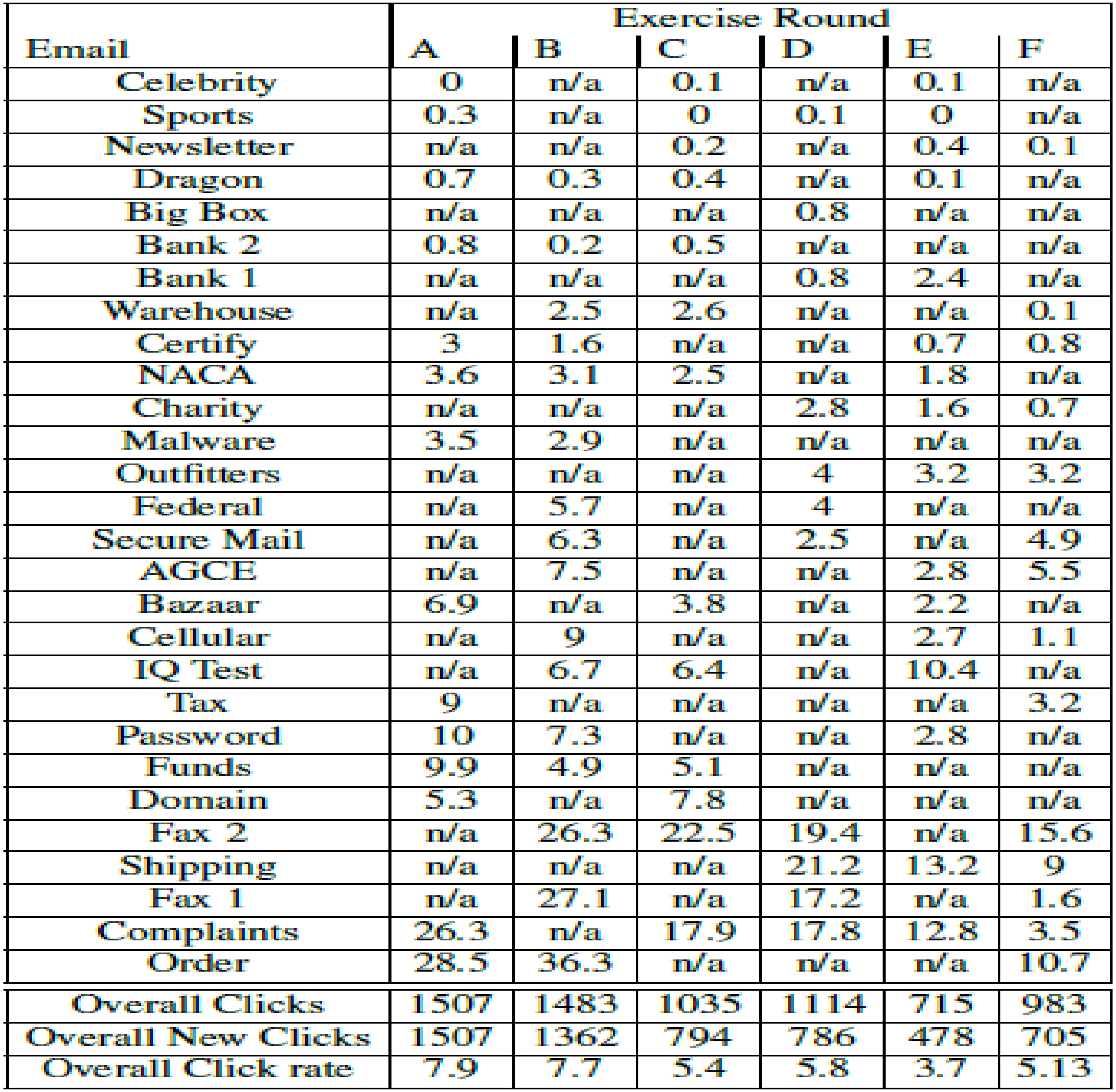
THE GOAL

Develop methodologies for correcting possible sources of bias in exercise analysis, which would enables more sound evaluation of the effectiveness of embedded phishing exercises.

Study Campaign Design

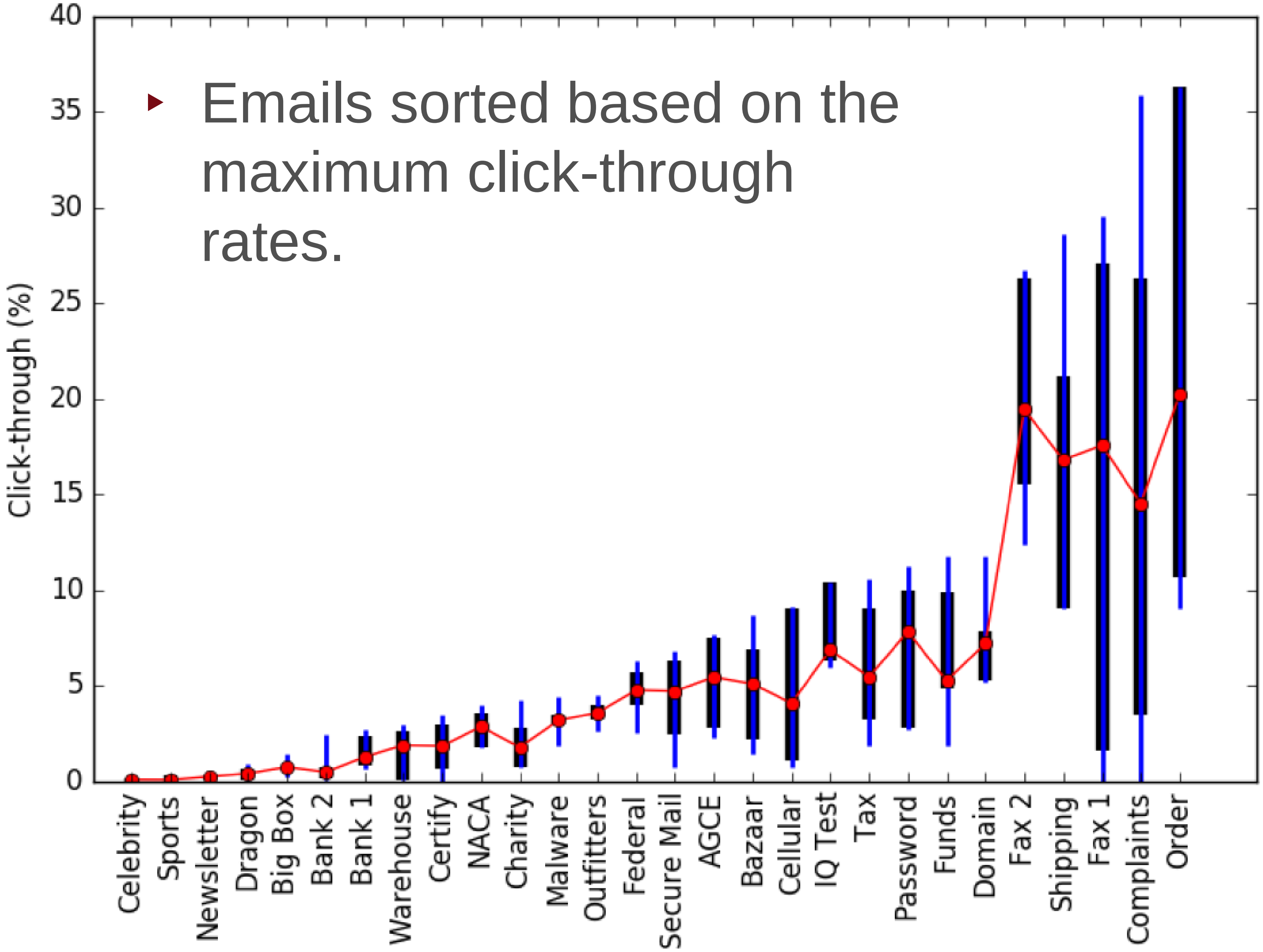
- This study is based on data acquired from a large-scale phishing training campaign conducted in a medium-size company.
  - 19,180 participants
  - 32 unique exercise groups/cohorts
  - 28 unique test e-mails varying in persuasiveness
  - 6 rounds of testing over 8 months
  - 115,080 test phishing emails distributed
- Exercise design highlighted difficulties and lack of best practices for structuring large-scale phishing exercises.

Study Campaign Results



Email	Exercise Round					
	A	B	C	D	E	F
Celebrity	0	n/a	0.1	n/a	0.1	n/a
Sports	0.3	n/a	0	0.1	0	n/a
Newsletter	n/a	n/a	0.2	n/a	0.4	0.1
Dragon	0.7	0.3	0.4	n/a	0.1	n/a
Big Box	n/a	n/a	n/a	0.8	n/a	n/a
Bank 2	0.8	0.2	0.5	n/a	n/a	n/a
Bank 1	n/a	n/a	n/a	0.8	2.4	n/a
Warehouse	n/a	2.5	2.6	n/a	n/a	0.1
Certify	3	1.6	n/a	n/a	0.7	0.8
NACA	3.6	3.1	2.5	n/a	1.8	n/a
Charity	n/a	n/a	n/a	2.8	1.6	0.7
Malware	3.5	2.9	n/a	n/a	n/a	n/a
Outfitters	n/a	n/a	n/a	4	3.2	3.2
Federal	n/a	5.7	n/a	4	n/a	n/a
Secure Mail	n/a	6.3	n/a	2.5	n/a	4.9
AGCE	n/a	7.5	n/a	n/a	2.8	5.5
Bazaar	6.9	n/a	3.8	n/a	2.2	n/a
Cellular	n/a	9	n/a	n/a	2.7	1.1
IQ Test	n/a	6.7	6.4	n/a	10.4	n/a
Tax	9	n/a	n/a	n/a	n/a	3.2
Password	10	7.3	n/a	n/a	2.8	n/a
Funds	9.9	4.9	5.1	n/a	n/a	n/a
Domain	5.3	n/a	7.8	n/a	n/a	n/a
Fax 2	n/a	26.3	22.5	19.4	n/a	15.6
Shipping	n/a	n/a	n/a	21.2	13.2	9
Fax 1	n/a	27.1	n/a	17.2	n/a	1.6
Complaints	26.3	n/a	17.9	17.8	12.8	3.5
Order	28.5	36.3	n/a	n/a	n/a	10.7
Overall Clicks	1507	1483	1035	1114	715	983
Overall New Clicks	1507	1362	794	786	478	705
Overall Click rate	7.9	7.7	5.4	5.8	3.7	5.13

Study Campaign Results



- Emails sorted based on the maximum click-through rates.

Key Questions

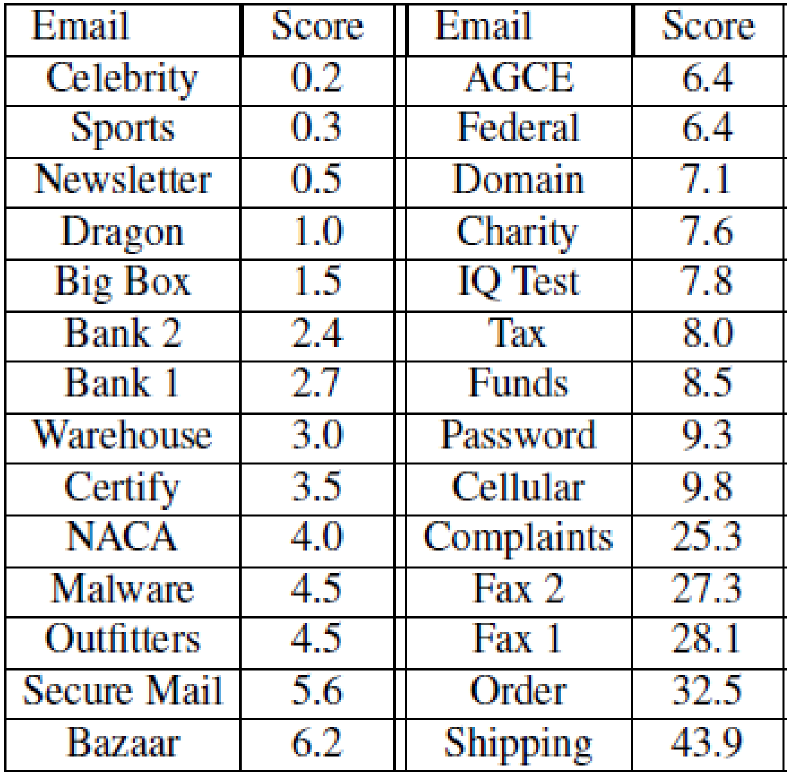
- Did the organization become more resilient to phishing attacks?
- Did the individuals involved become more resilient to phishing attacks?
- How much improvement was measured?
- What were the major influences on click-through rate increases or decreases?

Persuasiveness and Normalization

- Looking at the data, there appeared to be some interesting features.
- E-mail persuasiveness appears to be a key factor in measuring effectiveness.
  - Example: Group 20 started out with 35.9% of participants being phished in exercise A. The rate then dropped to 1.9% and 2.4%, respectively, in exercise B and C, before increasing to 19.4% in exercise D.
  - Same individuals, but dramatically different click-through rates per e-mail
- This observation suggests that the click-through rate should be normalized based on the persuasiveness of the content of phishing email text to produce a sounder analysis.

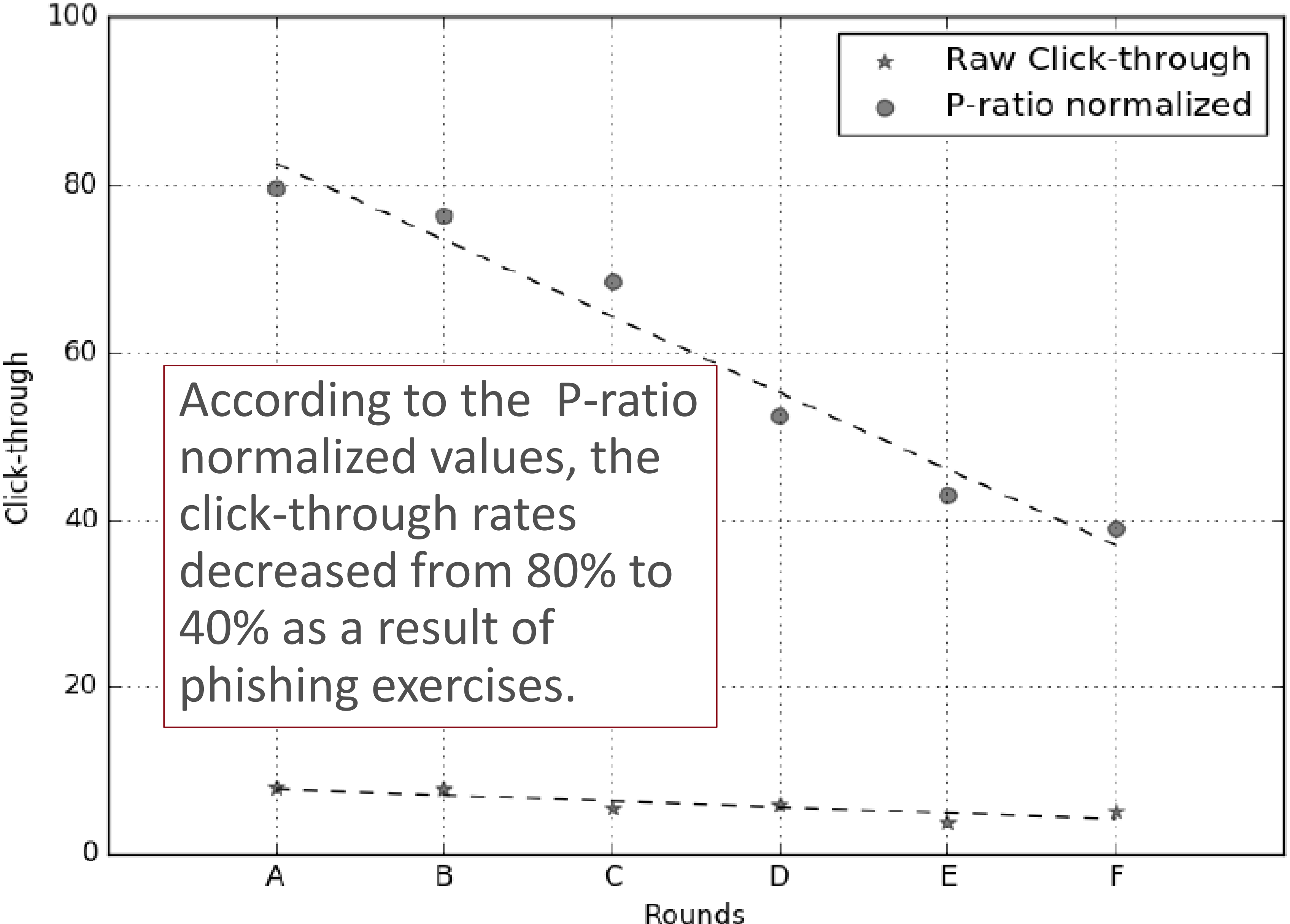
Persuasiveness and Normalization

- We used linear regression analysis over click-through rates to compute “email persuasiveness” scores.
- The calculations of these scores took into account bias for the exercise round of the e-mail.
- Multiple normalization approaches were then evaluated
- We determined that a P-ratio normalization scheme was most appropriate for normalization.



Email	Score	Email	Score
Celebrity	0.2	AGCE	6.4
Sports	0.3	Federal	6.4
Newsletter	0.5	Domain	7.1
Dragon	1.0	Charity	7.6
Big Box	1.5	IQ Test	7.8
Bank 2	2.4	Tax	8.0
Bank 1	2.7	Funds	8.5
Warehouse	3.0	Password	9.3
Certify	3.5	Cellular	9.8
NACA	4.0	Complaints	25.3
Malware	4.5	Fax 2	27.3
Outfitters	4.5	Fax 1	28.1
Secure Mail	5.6	Order	32.5
Bazaar	6.2	Shipping	43.9

Normalized Results



According to the P-ratio normalized values, the click-through rates decreased from 80% to 40% as a result of phishing exercises.

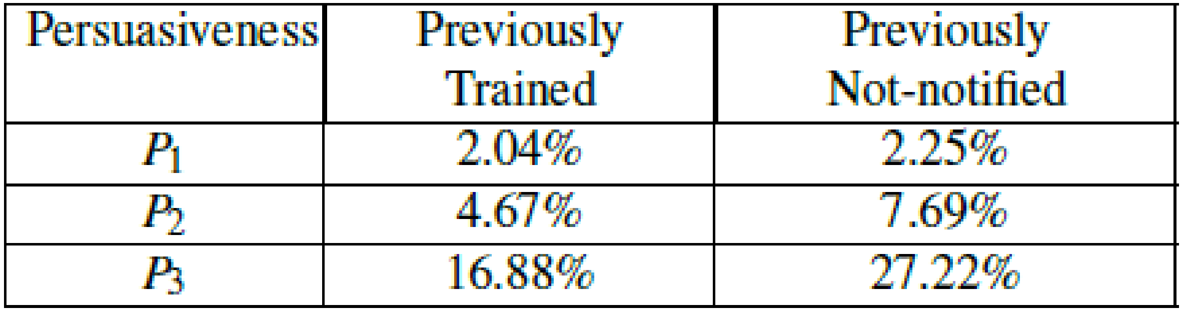
Recidivism Analysis

- The mere fact that the overall performance of the participants has improved as a result of phishing exercises does not fully validate the effectiveness of the training on individuals.
- If the training is effective, it should be much less likely that trained participants will fall for a phishing e-mail.
- Comparing the percentage of recidivism for users who were not trained vs. users who were trained shows that 25.94% of not trained participants fall for phishing compared to only 15.57% of trained participants. (p-value < 0.01)

Persuasiveness and Training

- Previous works did not look at whether training is equally useful for phishing emails of different levels of persuasiveness.
- We analyzed 3 classes of e-mails from our study:
  - (P1) includes emails with persuasiveness score below 5%
  - (P2) includes emails with score between 5% and 20%
  - (P3) includes emails with score above 20%
- We computed the probability of participants falling for such email after being trained in the previous round and also computed the probability for participants who were not trained or notified after the previous round.

Persuasiveness and Training



Persuasiveness	Previously Trained	Previously Not-notified
P_1	2.04%	2.25%
P_2	4.67%	7.69%
P_3	16.88%	27.22%

- The results show that training makes a more significant difference for email types that are initially more persuasive (i.e., P3).
- The improvement on click-through rate of less-persuasive phishing emails is not significant (i.e., P1).
- Highly susceptible users fall for even unpersuasive phishing emails, which suggests it might be more difficult to educate this type of user at all.

Conclusions

- Embedded phishing exercises can be useful, but require solid exercise design protocols rather than ad hoc testing.
- Post-analysis is critical for evaluation and requires normalization.
- The improvement from training seems to be limited to more persuasive phishing emails and that there is no improvement for unpersuasive phishing emails.
- Unfortunately, some users will fall for obvious phishing e-mails, and it is unlikely that they will benefit from such exercises or training.