NAME: AVISHEK MUKHERJEE

EMAIL: amukherjee3@albany.edu

DATE: 4/5/2019

PAPER TITLE: Unpacking spear phishing susceptibility

1. What is the main problem or issue that the authors are addressing?

Ans: The study assesses the vulnerability of people against phishing attack through Facebook and/or E-Mail messages.

1. Provide a short summary of the authors’ approach/argument.

Ans: The study is based on a previous study Benenson, Z., Girard, A., Hintz, N., Luder, A.: Susceptibility to URL-based Inter- net attacks: Facebook vs. email. In: 6th IEEE International Workshop on SEcurity

and SOCial Networking (SESOC). pp. 604–609. IEEE (2014). They paid special attention to recruit people in the study under the disguise of studying their Internet Habits, once they clicked on a phishing link their name was registered on the database. They replicate the above study with 1255 users, receiving the same message with suspicious link. Firstly, they made accounts with the most common German names based on the demographic characteristic of the dataset, like the probable birth year. In this case it was the 1990s. Facebook messages and E-Mails were not personalized.

Sample Characteristic: We recruited 280 Facebook users (80 male, 200 female) and 975 email users (265 male, 710 female). Groups have a comparable gender structure with 27% and 29% of male participants, respectively.

Research Question 1: Do people react to a “suspicious” link differently depending on whether the link was received via Facebook or via email?

Hypotheses: The following factors will be correlated to the higher success rate of the attack:

1.Message reception via Facebook

2.Friend Request from the sender

3.Message sent from an open Facebook profile

4.Female gender of the sender

5.Female gender of the recipient

Research Question 2: How people explained their behavior?

They designed a follow-up survey after the experiment.

The main reason for not clicking was the name:

1.Unknown Sender

2.Suspicion of Fraud

3. Situation context

4. Life Context

5. rule of conduct

6.privacy

7. message context

8. Message from

9. Link from

10. Bad Experience

and the most common reason for clicking on the link was that.

1. Curiosity
2. Context
3. Investigation
4. Known-sender
5. Technical Context
6. Fear
7. Automatic Response

42.5% of Facebook users and 20% of email users, compared to 38% in the study.

Conclusion: Users are susceptible to phishing in very high rate.

1. What are the main strengths and/or weaknesses of the approach?

Ans: The approach is strong enough in which they didn’t let the users know that they were being approached to study phishing attacks, and thus emulated a close to real scenario. The main strength is that the attacks were not personalized, but still they were better at fooling the users.

1. Provide at least 1 question regarding the paper that you’d like to address during class discussion.

Ans: I’d like to discuss the effect of such attacks on other sources like the one’s at a job. Where the effects may be more pronounced. 42.5% implies that ½ of the people do make the mistake of clicking the link.