Phishing Susceptibility and Analysis Study

Te Ming Tiong, Kristin DiMichele, Abdulla Alhamer, Abdullah Alsaadi
Professor Gino Manzo, Dr. Kathryn Laskey, James Lee
Cyber Security Engineering Department, George Mason University, Fairfax, Virginia, United States

Abstract

Phishing is a social engineering tactic that utilizes email and other forms of electronic communication that a malicious actor can use to trick people into giving their personal information, login credentials, bank account information, etc. Phishing is the number one cause of data breaches.

Breaches that started with a phishing email:

- Operation Phish Phry ($1.5 million)
- Walter Stephan ($47 million)
- Target/FMS Scam (over $200 million, 110 million users, 41 credit cards)
- Ukrainian Power Grid Attack (a whole country)
- Facebook/Google (over $100 million from 2013 to 2015)
- FACC ($61 million)
- Crelan Bank ($75.8 million)
- Ubiquiti Networks ($46.7 million)

Since phishing poses an imminent threat to everyone, our senior design project is to simulate a phishing attack for George Mason University (GMU). This attack will target undergraduate students above the age of 18, and use emails that manipulate different psychological factors that may affect students' susceptibility to a phishing attack.

Introduction

This research project is based on a study previously conducted by our customer, Dr. Kathryn Laskey, SEOR, using GMU faculty and staff as the test subject. The prior study focused on the susceptibility due to the demographics of the test audience whereas this study is adapted to see what aspects of a phishing email is more appealing to the subject to convince them to click on a link.

Four major parts are essential for the success of this study:

- Experiment design
- IRB approval
- Environment set up and testing
- Execute experiment and analyze de-identified data

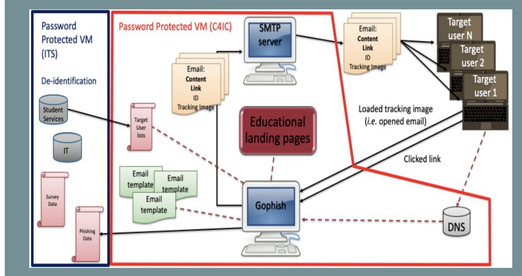
Goals of this study:

- Understand which psychological aspects will make a student more likely to click on a link.
- Seeing how many students will detect and report illegitimate emails.
- Determine whether incentive or punishment measure is more effective in combating phishing.
- Provide remediations to better educate students at GMU.

Methodology

Architecture Design

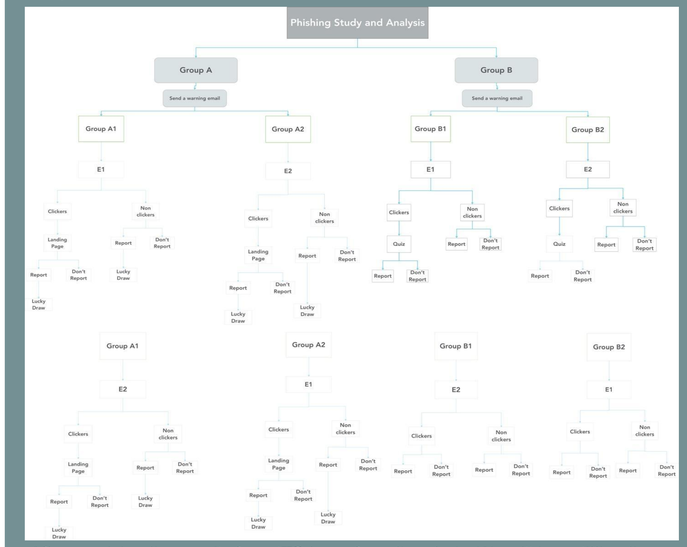
Mainly, the design outlines our methods and steps that must be followed to complete the project successfully.



This architecture demonstrates how each component interacts with each other via Gophish software.

- Email templates and landing pages are both loaded into the C4I server that hosts Gophish software.
- Gophish sends out the phishing emails to the students who are in the target user lists obtained from GMU ITS.
- Gophish automatically keeps track of who opened and clicked on the phishing emails.

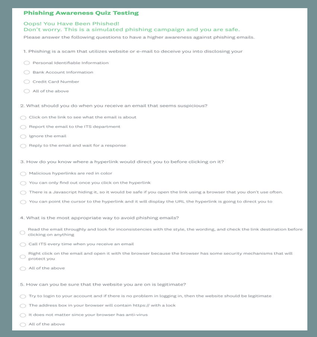
Experiment Process Breakdown



After receiving the emails from ITS to perform the study. We will be splitting the emails into two main groups (Groups A & B).

- Group A & B will receive a general warning email from ITS about phishing email tips.
- We used 2 different email templates (E1 & E2) which are based on curiosity and fear psychological factors respectively.
- Each group will be divided into 2 subgroups that will receive each email template.
- In Group A, clickers and non-clickers will enter a lucky draw if and only if they report the phishing emails.
- The same procedure will also be repeated on Group B.
- But for Group B, clickers will receive a quiz to educate them about phishing scams to enhance their awareness about phishing.
- During the second round, all of the things will be the same except we will switch the email templates for each sub group.

Landing Pages



We have created two different landing pages for clickers from different groups:

- The landing page on the left informs clickers that they were a victim of a fake phishing attack (Group A).
- The second landing page is a quiz about phishing to raise user awareness about phishing attacks (Group B).

Email Templates

Email templates are created based on our hypothesis:

- Hypothesis states that fear-based emails will have more clicks than curiosity-based emails.
- The first template (on the left) is based on fear and it is a notification about unpaid balance in student account.
- The second template (on the right) is based on curiosity and it is about a first time virtual career fair due to COVID-19 outbreak..
- Measure the effectiveness of each template after gathering data.

Verification and Validation

- For verification, we had weekly stand up meetings with our customer to ensure the design was to her standards via Agile model.
- For validation, with the help of our SME, we set up the Gophish environment with all the templates. We then sent testing emails to ourselves to see how they looked on various platforms. Adjustments were made as needed.

Results

For the results, we intended on looking at a few different factors:

- which group had more students click on the phishing link.
- which round of emails had more clicks on the phishing link.
- which template is more effective.
- which group would have more phishing reports to GMU ITS.

Due to restrictions from COVID-19, we were unable to send emails out to students and were unable to conduct the experiment. Without collecting data from our rounds of intended emails, there was no analysis of data to show results or validate and verify our hypotheses.

Conclusion

From this experiment, we projected that:

- Group A would report more emails to GMU ITS.
- There would be less clicks in the second round versus the first round
- An email template based on fear is more likely to receive a click than the template based on curiosity.

Dealing with sensitive information, the experiment could only be done on campus. Since we were not able to conduct the experiment, we were not able to draw any concrete conclusion.

References

[1] "The Dirty Dozen: The 12 Most Costly Phishing Attack Examples," *Hashed Out by The SSL Store™*, Jun. 07, 2019. https://www.thesslstore.com/blog/the-dirty-dozen-the-12-most-costly-phishing-attack-examples/ (accessed Apr. 13, 2020).

[2] Brad, "The Top 5 Phishing Scams in History – What You Need to Know," *PhishProtection.com*, Jul. 24, 2018. https://www.phishprotection.com/blog/the-top-5-phishing-scams-in-history-what-you-need-to-know/ (accessed Apr. 13, 2020).

Acknowledgements

Our team would like to express many thanks and gratitude to Dr. Kathryn Laskey for leading our senior design project, James Lee for helping us through the technical aspect of our project, and Professor Manzo for guiding us through the senior design process. Even though we have experienced some difficulties along the way, but we are still very grateful for having this as an opportunity to collaborate as a group and gain some insight on what does an industrial project looks like.

27 April 2020