Phishing Training For The Layperson

University of Findlay

Matthew Wilkins

Master of Science in Applied Security and Analytics

ABSTRACT

Cybersecurity is a constant arms race between people seeking to exploit potential weaknesses for profit or for ideological reasons, and those attempting to construct as close to perfect defenses as is possible. One of the constants within this arms race has been the fact that the system is only as strong as the "weakest" user. If one person who is inside the system that is being defended opens a phishing link, either through ignorance or malicious intent, the system can collapse. This project aims to develop and test data-based training focused on the layperson. Backed by data to focus on common issues and presented in a simple and engaging manner, this training intends to reduce the occurrence of ransomware incidents, especially via the vector of phishing emails. This training will lay the foundation for expanded training material, either into other specific areas, or into a broader training field.

INTRODUCTION

This training can provide businesses with a way to reduce the amount of phishing occurrences each year. To develop the training, I focused on the two extremes of training, one side is accurate, in-depth, and often far too dry or complex for the layperson to stay engaged with or properly understand, the other is far too patronizing and low-level to be effective for anyone above a fourth-grade level.

While developing a fully interactive web-based training program was beyond the scope of this project, I was able to create a PowerPoint presentation that covered the information that I wanted to convey. Phishing and ransomware were chosen as the topics for training based on being the most common issue faced by the clientele of the company I am working with. As phishing is a method of gaining access, I decided to focus my efforts on reducing the likelihood of successful phishing attempts.

DEVELOPMENT PROCESS

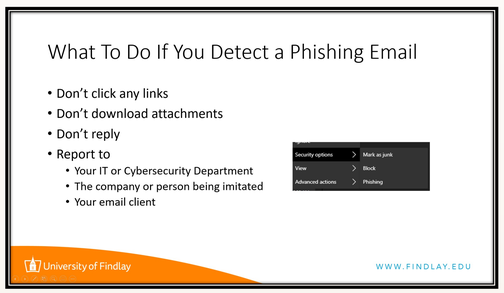
Training Material Development:

- Met with mentor
- Collected information on prominent issues
  - Shown to be ransomware delivered by phishing
- Met with committee
- Planned phishing knowledge test
  - Used Google Forms and attached PDF to allow roll-over of links to display URL
- Decided to use narrated PowerPoint in place of website for main training material

TRAINING MATERIALS

My training materials are in the form of a narrated PowerPoint, with the plan being to present the training between a pre- and post-test.

The training was designed with a business environment in mind, but has been modified some to fit the academic environment that the testing is taking place in.



The materials aim to be understandable by non-cybersecurity professionals without becoming patronizing and emphasizes the consequences of phishing on the individual and the organization, as well as how to avoid falling for a phish, and how to react to a phishing attempt.

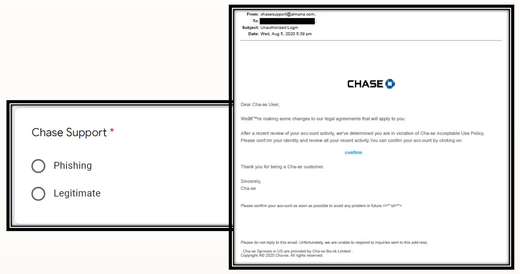
END-USER TESTING

Simulating non-cybersecurity experts:

- Computer Science students
- Test provided after receiving phishing-related training
- Test presented via Google Forms with accompanying PDF of emails

Test layout

- Five "phishing" emails
- Five "legitimate" emails
- Students identify which are which
- Students are told which they got correct and what they should have been looking for in each email, regardless of their answer



DISCUSSION

Lessons Learned:

- Any form of testing done with people is complex
- Always start early, and make plans based on the longest time estimates
- Prepare backup plans

Changes Made:

- Originally planned on utilizing pre- and post-testing, and training materials with a control group
- Used one group and a single test to create benchmark for analysis of training materials in the future

CONCLUSIONS

Training is important in any aspect of business. As it is developed, training must be outcome-oriented and thoroughly tested to ensure that it is usable and effective.

When testing the effectiveness of training, there are three stages that should be tested to be truly thorough, as well as dividing tests into a primary test group and a control group. The three test stages are a pre-test to gauge the level that a group is at prior to the training being delivered, an immediate post-test to gauge the short-term efficacy of the training, and a second post-test some weeks or even a month later to determine how well the information from the training sticks.

Cybersecurity and the related training are often overlooked in the business world as the effects of good security are rarely seen, and many people only notice when something goes wrong. The phishing and "cyber hygiene" training are usually part of the onboarding process, and are frequently done as quickly as possible, which can lead to poor retention and problems further down the line.

With proper training, we can help to reduce the number of user-caused security incidents and focus on developing more effective responses to the ever-growing threat of cybercriminals.

REFERENCES

Firch, J., & Swanagan, M. (2021, March 25). How to create a successful phishing campaign in 8 steps. Retrieved March 28, 2021, from https://purplesec.us/phishing-campaign/

How to recognize and avoid phishing scams. (2021, February 19). Retrieved March 28, 2021, from https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

KnowBe4. (n.d.). What is phishing? Retrieved March 28, 2021, from https://www.phishing.org/what-is-phishing

ACKNOWLEDGEMENTS

I would like to thank Drs. Schneider and Leventhal, my mentor Loren Wagner, the company that provided data, and all the instructors and students who assisted with my project.