“Categorizing human phishing difficulty: a Phish Scale”

By M. Steves, K. Greene, and M. Theofanos

Article Review

Jeremiah Price

CYSE 201S

Prof. Leigh Armistead

March 31, 2022

Introduction

Corporations and businesses will often put their employees to the test to determine adequate training and precautions. As technology progresses, many corporations are now including the new-generation “Phishing” scams into these tests. The company will send out a phishing email and the employee is supposed to recognize the phish and report it. If it is not reported or it is clicked out, additional training will be required. This has shown success on many occasions during the last decade.

When many CISOs reported high numbers, a flaw was recognized in the phishing email test. It was not put into account that there would be obvious different levels of difficulty within these phishing emails. Different wording and topics may be harder to spot than others, resulting in many different click rates. Research has shown that if the topic of the email was aligned with the users work, click rates would be higher (Steves et al., 2020).

This is an article summary and review of “Categorizing human phishing difficulty: a Phish scale” by M. Steves, K. Greene, and M. Theofanos.

Research

Research of this journal was collected through many studies and papers aligned with phishing emails.

For one of these sources, phishing exercise data was collected over 4 ½ years to study the correlation between the type of email and the responses. This study found that:

- Context of the user was a large variable in the users susceptibility
- Out-of-context emails were often much easier to spot
- If the email had to do with their direct line of work, it was likely to gain clicks

Method

The authors of this journal have created a method known as the “Phish Scale” to determine level of difficulty within phishing training exercises. This method is intended to be used by large audiences to help the process of these exercises and expose hidden variables.

The method organized many examples of emails and cues, as well as a rating system to determine email difficulty. These emails were put to the test within many different settings and it showed much success when results got back.

Analysis

All exercises having a very difficult rating got much higher click rates ranging from 19.4% to 49.3%. All exercises with a lower difficulty only had click rates ranging from 3.2% to 11.6%. This scale was applied to many different groups being tested and it showed proper rankage immediately. Emails with very few cues (hints to show it is phishing) were ranked more difficult and thus showed much higher clicks. Emails with many cues were clicked on less, and were ranked as less difficult. However, some of the emails still had clicks because the context of the email was in line with the context of the user.

Contributions to Society

This journal had quite a few significant achievements and advances.

- This is the first difficulty scale created and publicly used
- It is a big step for cyber-awareness training
- Many companies and businesses may quickly inherit this scale
- Training percentages can be rightfully determined and studied

Relation to the Social Sciences

Phishing has become a large problem in the last decade. Many common scams are recognized and joked about by the public. However, many of the scams work and become recognized by people learning them the hard way. Even if the success percentage is 1 in 100, it would not be hard to send 10,00 emails.

These scammers manipulate and target individuals to steal money, information, or assets. Commonly, scammers will target older users to manipulate. They are seen as socially and technologically unaware and they are less likely to spot a scam. Psychologically, they are the easy targets for the scammers to pick on.

Corporations use these connections to the social sciences to carefully construct tests to deploy against the employees. These tests question human error factors, training success percentages, and help collect data for future research.

As a bigger relation to the social sciences, social science is the pure reason this table ranking method needed to be created in the first place. Scamming success percentage could solely depend on the context of the email, context of the user, and the user's current situation. An invoice manager is more likely to respond to an email asking about an unpaid invoice.

Human error will always be one of the biggest factors in cybersecurity, but with proper ranking and variable statistics, it can be thoroughly analyzed and evolve.

References

Michelle Steves, Kristen Greene, Mary Theofanos, Categorizing human phishing difficulty: a Phish Scale, *Journal of Cybersecurity*, Volume 6, Issue 1, 2020, tyaa009, https://doi.org/10.1093/cybsec/tyaa009