GONE PHISHING: SURVEYING COLLEGE STUDENTS ON PHISHING AWARENESS AND COMPETENCY

Steven Vue
Undergrad Student
Information Systems
St. Cloud State University
St. Cloud, MN 56301
vust1001@stcloudstate.edu

Dr. Mark Schmidt and Erich Price
Information Systems
St. Cloud State University
St. Cloud, MN 56301
mbschmidt@stcloudstate.edu
eprice@stcloudstate.edu

Abstract

Technology trends are progressing towards mobility and ease of access from any source including BYOD (Bring Your Own Device) such as personal laptops and smartphones. These new trends are creating data vulnerabilities to enterprise networks in both the public and private sector, making them potentially vulnerable to external cyber-attacks. Of these potential attacks, phishing is one that a majority of organization's deal with every day. Once an email is a suspect of phishing, what are the immediate thought processes one should undertake and how should an individual address it? Recently, various forms of phishing attacks have targeted St. Cloud State University's students, staff and faculty. This paper will try and assess the levels of phishing awareness and recognition of IT college students and faculty to help further assess the study of this question.

1 Introduction

Mobility and ease of access to social media, emails, and daily use have received growing popularity due to the technology trend of mobile devices and BYODs (Bring Your Own Device). But it also presents low security issues that address information security. Whether it is a laptop, phone, or tablet, the potential vulnerabilities are often overshadowed by the convenience and level of use advancements created by these technologies. These devices contain a huge surmount of data that are vulnerable to phishing attacks and potential risks to networks and personal information. Phishing is defined as "sending an e-mail to a user falsely claiming to be a legitimate enterprise in an attempt to scam the user" [Volonino 7].

Each organization and individual has its shared number of email phishing attacks, but what are the success rates? Of the top-ten types of information breached, email addresses are number eight on the list [Symantec 2014]. Phishing attacks compromised about .2 percent of all email [Symantec 2010]. Is this due to the results of human behavior, or lack of awareness and knowledge in the subject? According to a Norton global survey of end-users, 38 percent of mobile users are victims of mobile cybercrime already and poor user behavior dictates self-inflicting problems; yet only half of them invest in the most basic security precautions [Symantec 2014]. The results of this study aims to compare and evaluate the security awareness levels of St. Cloud State University IT graduates, undergraduates, and a small pool of non-IT students.

The layout of this research includes: the methodologies of the research and recent phishing attacks and outcomes of those attacks. Followed by a thorough analysis of the survey data collected from the participants. With the data, a study will be presented on their potential cognitive awareness and knowledge and their resulting interactions when faced with several examples of phishing emails and a non-phishing emails.

2 Methodology

The primary goal of this research is aimed to study the awareness and competency of St. Cloud State students in the Herberger Business School of Information Systems. In order to achieve the best results for the research survey we had to consider the best deliverable to implement, an electronic survey or a hard copy. Electronic or online surveys are less likely to receive a response as compared to paper surveys that are administered and distributed on site. The scope of the survey pool is fairly small and un-highly diversified, therefore distributing the surveys to individual classes would yield a significant turnout of participant results.

In the design of the survey, questions and concepts are revolved around phishing and emails usages of each participant. By conducting a survey with the students of one common department, poses potential biases to the results of the survey, as a student may or may not have taken the survey twice or the awareness of being tested on phishing competency may influence their result. The steps to acquiring the research data included preliminary approvals. In the process of acquiring our data, mandatory approval of compliance by the campus Institutional Review Board (IRB) was required before we

were granted the privilege to conduct our survey research. Once approved by the IRB, necessary steps were taken to distribute the surveys and completed surveys were stored securely according to IRB standards. The results of the survey were entered into a spreadsheet template for thorough analysis of the data. Overall, the goal of the analysis will aid the researchers conclusion on the examination of students when handling emails.

3 Phishing attacks on St. Cloud State

Recently St. Cloud State University (SCSU) campus has seen a noticeable number of unfiltered phishing attacks on SCSU emails and attempted phone scams. In a case, one of the international students was targeted by a phone scam on January 23, 2015, reported by the SCSU campus Public Safety department. The caller attempted to extort $1, 945.00 worth of taxes as he claimed to be a representative from the Internal Revenue Service (IRS). The student was also threatened with deportation and confiscation of his passport. Although under the threats of the anonymous caller who went by "Steven Jones", the student was aware of the fraud and did not provide any personal information or credentials to the caller.

In another case, students were exposed to an email "easy money" scam, also known as Money Mule scams. In this type of attack, scammers send out emails claiming to have job offers that require little to no work. SCSU officials have seen campus emails that may have been compromised and are being piggybacked to send spam emails to other students with fraudulent job offers. An actual email message a student received: "Work at your convenience a Personal Assistant and earns weekly. Click here for further details or to sign up." The scammers will often ask for support towards a non-existent orphanage, when they've obtained your donations, scammers will promise you a check with tracking information to keep you interested, but behind the scenes your cash is being wired to a different account. The SCSU campus banks TCF and Affinity Plus were notified and are aware of the scam and have made stops to fraudulent check deposits. Not all of those scams made it through, but a few have and students have fall victim to this type of scam. These types of phishing attacks can damage the student's financials and lead to vulnerabilities amongst the campus' network system.

So far none of the attacks have been proven to cause unsustainable damages. But since some of those attacks presented victims, this research will evaluate the current awareness of the Herberger Business School, Information Systems students to potentially determine if they are competent of phishing attacks. The Information Technology Services (ITS) and Public Safety departments are continuously collaborating to halt any phishing threats against the campus community, but there is no guarantee that human error can be predicted. Email is an essential part of communicating issues and recent news. Although all students receive the email updates from ITS staff concerning important technical issues, what causes outcomes of successful attacks? How often do the students read emails sent by the ITS department? All of these questions were inducted in the survey and the results will be discussed in the evaluation of portion of this research.

4 Survey Results

The survey results yielded a total of 118 participants and their data from each of the targeted sectors of the research. There were a total of 76 male and 40 female participants, of which included 30 non-IT students whose results were erratic in the opinion questions of the survey. We observed that the graduate students in the Master of Science in Information Assurance displayed a refined view of what security measure should be taken, but did not always make the correct decision on the email examples. The Undergraduates data were uncorrelated and presented different data measures all around the board. Nonetheless we were able to collect sufficient data to produce our research study.

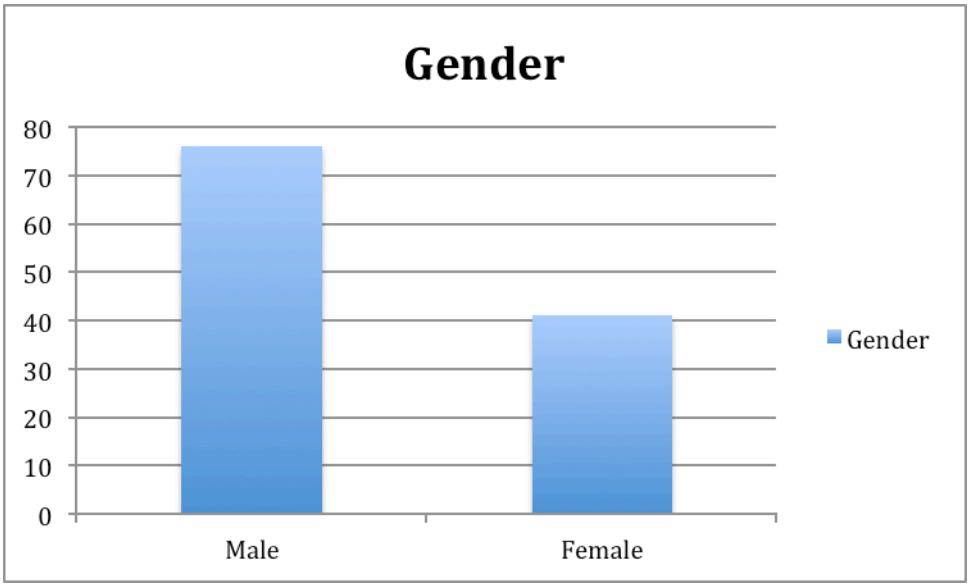

Figure 1. Chart displaying total number of male and female participants in the survey

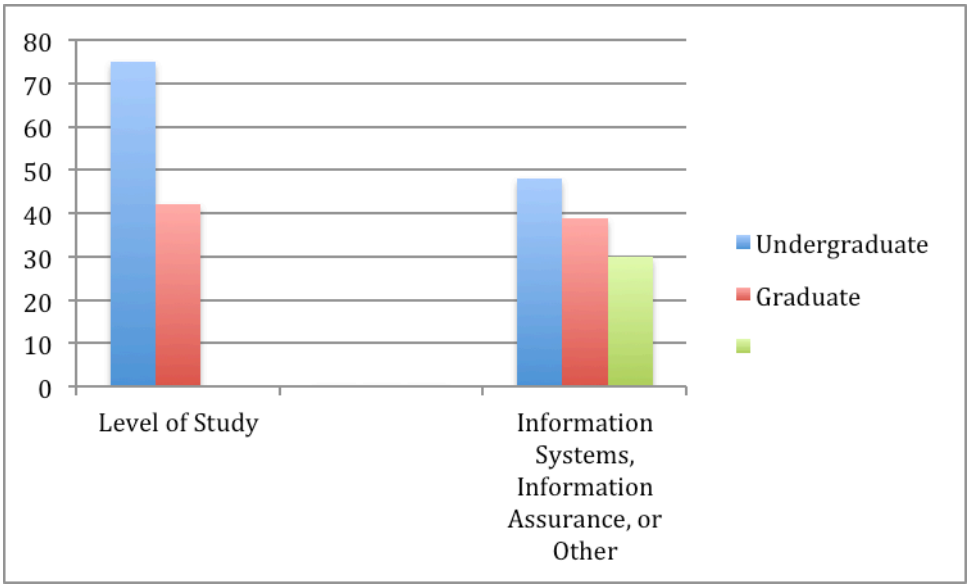

Figure 2. Chart displaying current level of study and area of studies.

To address the continuing concerns of phishing vulnerabilities and awareness levels of our IT students, we attempted to measure their current state of awareness. In the survey we asked the students for their opinion that will reflects their current awareness level and knowledge of phishing. Below is a chart figure that displays the student's selection to the opinionated question.

4.1.1 Awareness and Knowledge of participants

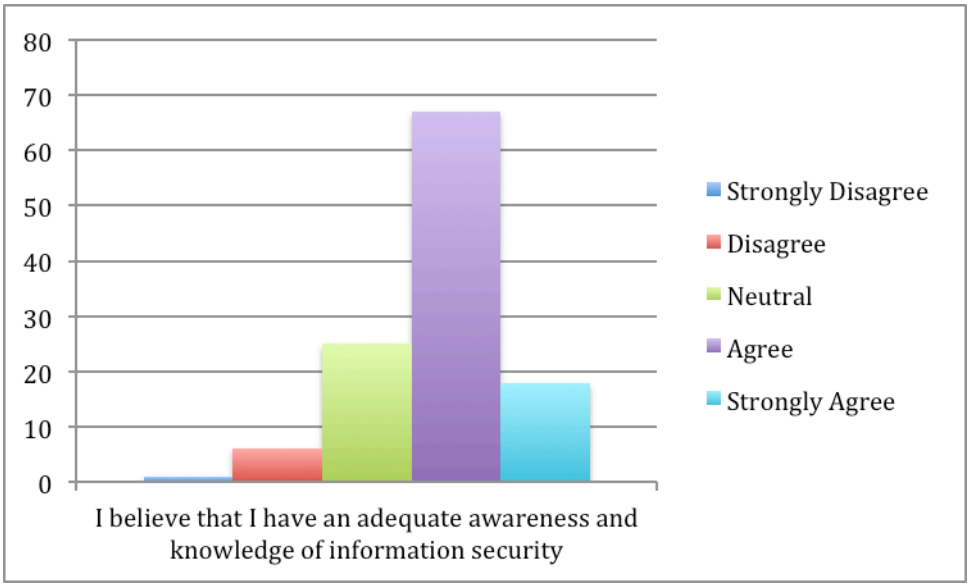

Figure 3: This chart is displaying the survey data results from Question 2 of the survey

According to the results, about 70 percent of the students agree that they have adequate awareness and knowledge of information security. Comparing these results with Fig. 2 of Question 8 from the survey, there is a noticeable difference in the responses collected.

4.1.1.1 Experience handling phishing emails and scams

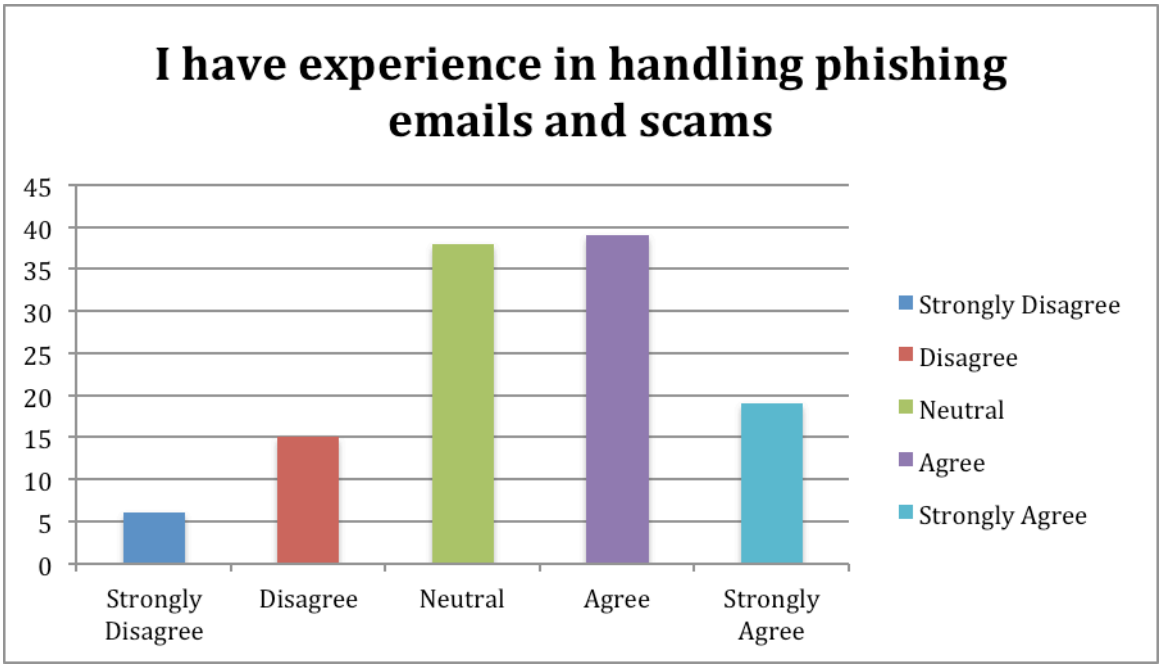

Figure 4: This chart is displaying the survey data results from Question 8 of the survey

The student's responses were highly correlated from Neutral to Agree. Just about half the data would count towards little to no knowledge of what a phishing email is and how it should be dealt with. By analyzing and comparing the two Figures, we will produce a question as to whether the students have the experience and awareness of security issues that they may or may not claim to have.

As mentioned in the earlier context of the research, the students were given a phishing email and non-phishing email quiz to test their decision process. Of the four given examples, all of them were pulled from actual St. Cloud State phishing emails and scams. Some students had noticeable troubles with first example in the quiz.

4.1.1.1 Phishing Email Examples Quiz

The first example incorporated into the test was an actual phishing email. The Subject line included an urgent header stating, "Please Check". In the context, the sender, Julie Miller claims to be a staff of the St. Cloud State University library requests that the recipient confirms his access to the library services. Julie Miller also provides a SCSU

email appearing legitimate to the purpose. The signature incorporated a phone number, email, and position (SCSU library). The original factor that would truly determine the validity of this email was the original sender's email. Although it contained a legitimate SCSU school email, it did not match up with the original email appearing by the sender.

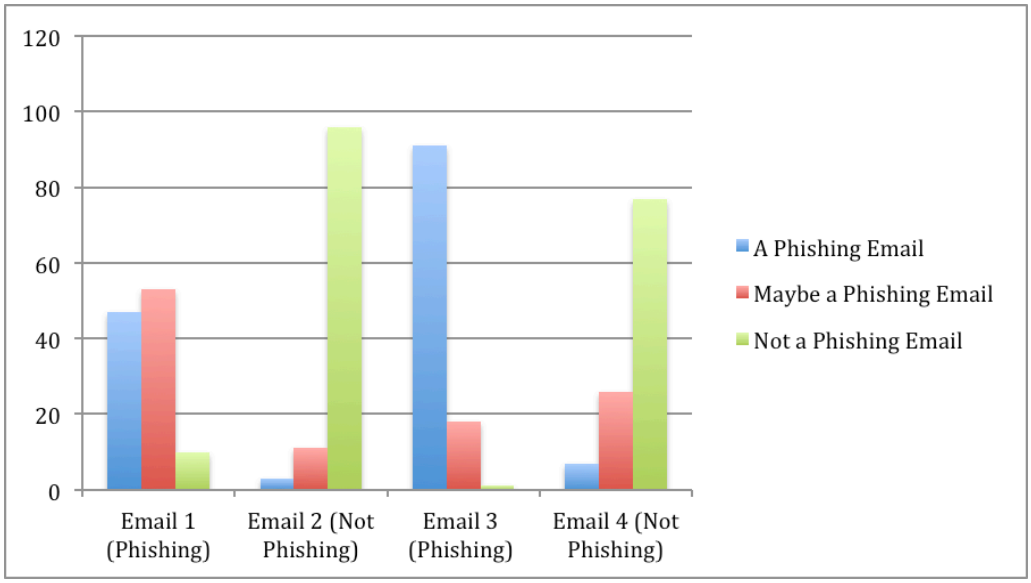

Figure 5: Phishing email examples test results

Referring to Figure 3 above, Email 1, which was determined as a phishing email yielded lower response levels compared to the other three email examples that were more obvious. Students were a little unsure, about 45 confirmed it to be an actual phishing email, and about 10 decided that it was a legitimate email. The 10 student responses accumulate about 8 percent of the total responses for that example, which is a fairly low percentile.

5 Analysis

How did the students perform? Overall, the students were able to determine the validity of the other three email examples. There are several reasons that could've contributed to these results. One, they checked their emails and read the news sent by the Public Safety and ITS departments that contained the phishing alerts. Another reason being that they had the knowledge and experience of the format a phishing email takes. With the following results, the analysis of their decision making process when dealing with phishing emails is at an adequate level. There is still a possibility that students could use more awareness and continued knowledge on phishing scams.

References

[1] McDowell, Mindi. "Security Tip: Avoiding Social Engineering and Phishing Attacks." *Avoiding Social Engineering and Phishing Attacks*. United States Computer Emergency Readiness Team, 22 Oct. 2009. Web. 25 Feb. 2015.
[2] Volonino, Linda, Reynaldo Anzaldua, and Jana Godwin. *Computer Forensics: Principles and Practices*. Upper Saddle River, NJ: Pearson/Prentice Hall, 2007. Print.

[3] Symantec Internet Security Threat Report 2014. Mountain View: Symantec Corporation, Apr. 2014. PDF.

[4] Jakobsson, Markus. The Human Factor in Phishing. Bloomington: Indiana University, n.d. PDF.