Human Hacking in Students

**Project Objective**

The objective of this study is to determine the students’ awareness and ability to recognize phishing emails as a form of cyber-attacks. Evaluate if the students are capable of determining if an email is phishing, or if it is trustable. The study will also analyze how frequently students fall victim to phishing attempts. Based on the findings, the study will propose possible solutions to engage cybersecurity awareness on campus, which may include educational campaigns or the development of a cybersecurity fundamental course to better prepare students against social engineering threats.

**Project Background and Significance**

Attacking humans and exploiting their vulnerabilities has existed throughout history. In today’s technological era, these attacks have developed into modern cyberattacks that increasingly target human behavior rather than technological weaknesses. For many years, such attacks lacked proper conceptualization. However, Sun, Wang, and Zhu define these crimes as "a type of attack wherein the attacker(s) exploit human vulnerabilities by means of social interaction to breach cyber security, with or without the use of technical means and technical vulnerabilities." In other words, attackers manipulate human susceptibility and lack of cybersecurity awareness to gain unauthorized access to sensitive data.

There are various motivations behind these attacks, such as financial gain, destabilization of institutions, political interference, or causing social disruption. A particularly common method is phishing. As Abdullah and Mohd explain, “Phishing is an attack that uses social engineering techniques to steal users' confidential information like passwords and banking information. It happens when cyber criminals, disguised as a trusted entity, deceive users into clicking on fake links in emails.” Phishing emails often attempt to extract sensitive information by imitating trusted organizations or individuals, exploiting the victim’s trust and lack of vigilance.

Despite ongoing awareness campaigns by banks, government institutions, and cybersecurity firms that educate users on recognizing phishing attempts, phishing remains an effective attack method. Steves et al. propose that two major factors contribute to a victim’s likelihood of falling for phishing: (1) the cues contained within the message itself, and (2) the alignment of the message's premise with the target audience's expectations and context.

This research points to evaluate how susceptible college students are to phishing attacks by analyzing their responses to different phishing email designs. Specifically, this study will assess:

1. Whether specific email components (such as language, urgency, or sender identity) influence the likelihood of the target audience falling for the phishing attempt.
2. Whether the student's major and educational background affect their ability to recognize and resist phishing attacks.

The findings of this research may help institutions better tailor cybersecurity education programs to target specific vulnerabilities of different student populations.

**Research Methods**

To effectively execute this study and investigate any potential relationship between a student’s major, their background in technology, and their ability to recognize phishing emails. I will collect and analyze quantitative data to store the number of students which didn’t recognize the fake email. This approach will allow for statistical analysis and a deeper understanding of students' awareness regarding cyber-security threats.

First, I will develop a phishing email trying to imitate an official university email. The structure and content of the message will be as close as possible to an authentic message that could come from the university; However, the email address won’t be an official university domain. Then, the same email will be distributed to 400 undergraduate students, ensuring this population will be equally split into four colleges: the College of Engineering & Computer Science, College of Business, the College of Communication, and College of Health Science.

The phishing email will contain a survey on the topic of how well diversity is on campus. Will be a social topic where most students will be interest and engage to participate. As part of the phishing simulation, students will be asked to answer a few questions and then provide sensitive information, such as their student ID, date of birth, and full name. This design will test students’ vulnerabilities, which Albladi and Wier define as “the set of user attributes that incline that particular user (rather than other individuals) to be a victim of social engineering attacks.” Their awareness of phishing tactics, their ability to verify the legitimacy of the request, and their willingness to disclose personal information.

Prior to distribution, all emails must be reviewed and approved by the appropriate university departments and each participating college to ensure ethical standards are met. Since sensitive data may be submitted, all responses will be encrypted and securely stored. The analysis will focus on the number of students who responded to the phishing email and submitted personal information; individual responses will not be manipulated or reviewed in detail.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Write Phishing email | Get Approvals to send email | Distribute Email | Analyzed Data | Prepare final report |
| Week 1 |  |  |  |  |  |
| Week 2-3 |  |  |  |  |  |
| Week 4-6 |  |  |  |  |  |
| Week 7 |  |  |  |  |  |
| Week 8-10 |  |  |  |  |  |

By collecting the data, this study will provide insights into which college should implement additional cybersecurity education. Also, the findings may help the university develop targeted awareness campaigns to strengthen students’ ability to recognize and avoid phishing attempts. Ultimately, contributing to a more cyber-aware student body and better-prepared future professionals.

**Expected Outcome**

Once the study is concluded, I plan to prepare a research paper summarizing the study’s methods, data analysis, results, and conclusions. I intend to submit this paper to UCF’s Office of Undergraduate Research. And with their approval I want to participate in a symposium to present my research work to other students and faculty. I will develop a poster presentation to facilitate audience participation and focus on the study.

Also, based on the outcome of the study, I will plan to propose practical applications. If the data reveals significant gaps in students’ ability to recognize phishing emails, i will recommend that the university implement an educational campaign across campus to raise awareness and improve students’ cybersecurity knowledge. However, if the results are dramatically high, it shows a high vulnerability rate. I will propose the development of a required course on cybersecurity fundamentals, applicable to all undergraduate students regardless of major. As Dupuis suggest the following “the goal of increasing cyber security hygiene for an important segment of the population—college undergraduates... The need for improved cyber security hygiene from the average everyday person is of equal importance” He proposed an introductory course elective for undergrad students to increase their awareness of cybersecurity. Proposing a general course to ensure future professionals will be also prepared to face cybercrimes.

While many studies have focused on technological vulnerabilities, this research emphasizes the human side of cybersecurity, specifically examining how background knowledge and academic discipline influence susceptibility to phishing attacks. For the UCF community, the study has the potential to guide curriculum development, improve student safety, and better prepare graduates to navigate an increasingly complex digital world.

**Preliminary Work and Experience**

As a computer Science student, I am taking a Computing Security class, where I learned the fundamentals of Security. Including key concepts related to system vulnerabilities, attack methods, and security protocols. Also, through the last several months, I have been independently studying to earn a cybersecurity certificate through Google. This program has expanded my understanding of technical terminology, threat analysis, and real-world applications of cybersecurity principles.

In addition to my technical preparation, my coursework in English Technical Writting has provided me with valuable experience in composing professional emails and understanding how to replicate the structure and formatting of an official university communications. This skill will be essential for designing a phishing email that imitates a UCF email, ensuring accurate assess to student awareness and susceptibility to phising attacks.

Finally, these combined experiences have equipped me with the technical knowledge, research skills, and communication abilities necessary to successfully complete this research project.

**IRB/IACUC statement**

This proposal will require IRB approval, since it involves indirect human contact via email. And the administration of a survey. Although the individual responses won’t be analyzed in detail, the study still involves human interaction and data collection.

**Budget**

This research study requires minimal funding, as the survey will be conducted online and campus library computers can be used to create and send simulated phishing emails. As well as analyzing the data. The primary anticipated expense would be needed if the study is approved for presentation at a symposium, in which case it may be needed to print a poster for the presentation.