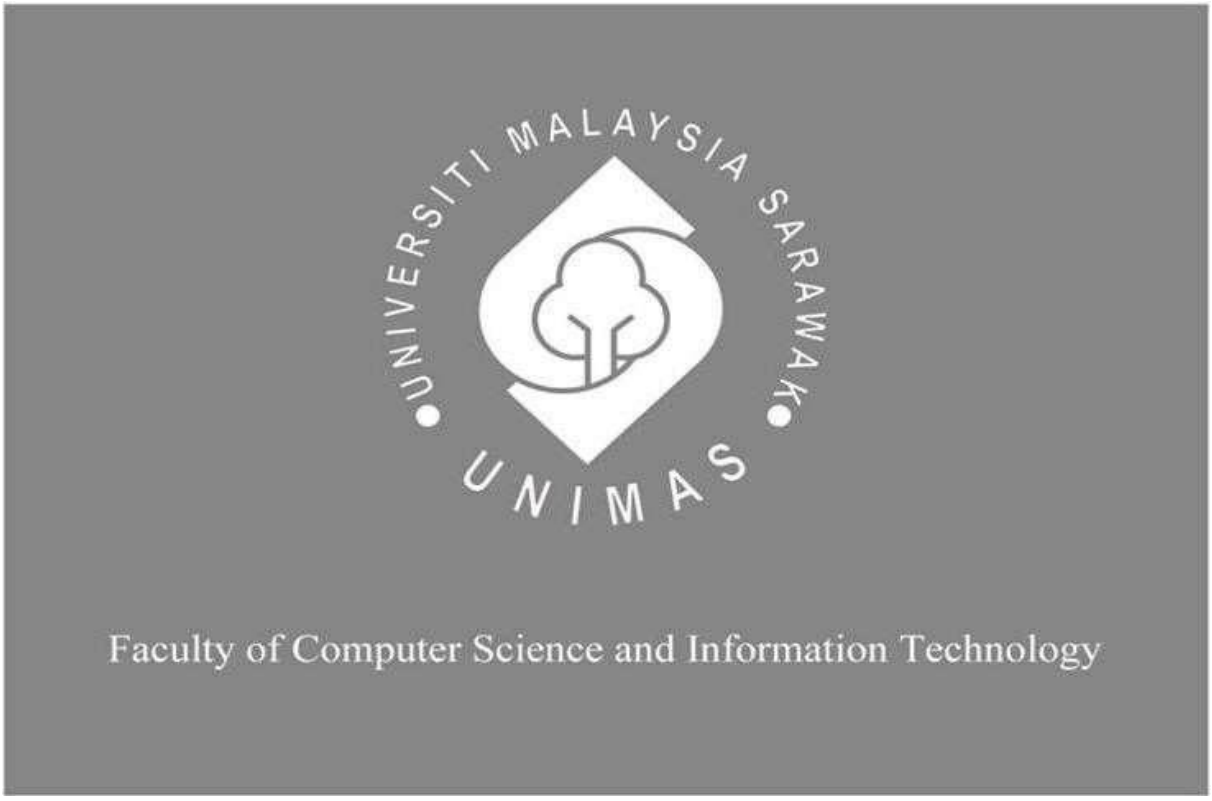

CYBERSECURITY SOCIAL ENGINEERING AWARENESS ASSESSMENT AMONG STUDENTS IN UNIMAS

Nurain Batrisyia Binti Mohamad Jaihan

Bachelor of Computer Science with Honours (Network Computing)

2023

CYBERSECURITY SOCIAL ENGINEERING AWARENESS ASSESSMENT AMONG STUDENTS IN UNIMAS

NURAIN BATRISYIA BINTI MOHAMAD JAIHAN

This project is submitted in partial fulfilment of the

requirements for the degree of

Bachelor of Computer Science and Information Technology (Network Computing)

Faculty of Computer Science and Information Technology UNIVERSITI MALAYSIA

SARAWAK

2023

UNIVERSITI MALAYSIA SARAWAK

THESIS STATUS ENDORSEMENT FORM

TITLE **CYBERSECURITY SOCIAL ENGINEERING AWARENESS ASSESSMENT AMONG STUDENTS IN UNIMAS**

ACADEMIC SESSION: 2022/2023

NURAIN BATRISYIA BINTI MOHAMAD JAIHAN
(CAPITAL LETTERS)

hereby agree that this Thesis* shall be kept at the Centre for Academic Information Services, Universiti Malaysia Sarawak, subject to the following terms and conditions:

1. The Thesis is solely owned by Universiti Malaysia Sarawak
2. The Centre for Academic Information Services is given full rights to produce copies for educational purposes only
3. The Centre for Academic Information Services is given full rights to do digitization in order to develop local content database
4. The Centre for Academic Information Services is given full rights to produce copies of this Thesis as part of its exchange item program between Higher Learning Institutions [or for the purpose of interlibrary loan between HLI]
5. ** Please tick (√)

☐	CONFIDENTIAL	(Contains classified information bounded by the OFFICIAL SECRETS ACT 1972)
☐	RESTRICTED	(Contains restricted information as dictated by the body or organization where the research was conducted)
☒	UNRESTRICTED	

Validated by

_____ _____

(AUTHOR'S SIGNATURE) (SUPERVISOR'S SIGNATURE)

Permanent Address

No.22 Jalan Nova U5, Seksyen U5 Subang

Bestari, 40150 Shah Alam, Selangor.

Date: 30/06/2023 Date: 30/6/2023

Note * Thesis refers to PhD, Master, and Bachelor Degree
** For Confidential or Restricted materials, please attach relevant documents from relevant organizations / authorities

DECLARATION

I hereby declare that the work entitled, Student Course Registration Coordination System (SCRCS) is my original work. I have not copied from any other students' work or any source except where due reference or acknowledgment is made explicitly in the text, nor has any part been written for me by another person.

Nurain Batrisyia binti Mohamad Jaihan

Network Computing

Faculty of Science Computer and Information Technology

Universiti Malaysia Sarawak

Date: 23/1/2023

ACKNOWLEDGEMENT

First and foremost, I want to thank Allah for granting me the blessing to do my final year project. Alhamdulillah. Here, I'd want to express my gratitude to my supervisor, Dr. Tan Chong Eng, for the advice he gave me when I was working on this project. His assistance has made it easier for me to finish this project. Not to mention, a heartfelt thank you to my parents, Mohamad Jaihan Bin Suliman and Rena Nasreen Binti Ramli, for their unwavering support, which gave me the motivation to complete my final year project. Last but not least, thank you to my examiner, Dr Adnan Shahid Khan that has given me the opportunity to do this project. Everyone who offered to assist me in finishing my final year project was greatly appreciated. I'm grateful once more.

ABSTRACT

In this day and age, social engineering attacks are among the most dangerous dangers. It is now prevalent all across the world. A social engineering attack may result in financial loss, privacy breach, reputational harm, and many other negative outcomes. Thus, a study aimed at evaluating individuals' understanding and knowledge of social engineering tactics and their ability to protect themselves against such attacks is proposed. The study would summarize the key findings, such as the level of awareness and understanding of social engineering tactics among the population being studied. It would also suggest recommendations for improving cybersecurity awareness and knowledge based on the findings of the study. The overall goal of the study would be to improve individuals' ability to recognize and defend against social engineering attacks, thus reducing the risk of security breaches and other cyber threats.

ABSTRAK

Pada zaman ini, serangan kejuruteraan sosial adalah antara bahaya yang paling berbahaya. Ia kini berleluasa di seluruh dunia. Serangan kejuruteraan sosial boleh mengakibatkan kerugian kewangan, pelanggaran privasi, kemudaratan reputasi dan banyak hasil negatif lain. Oleh itu, satu kajian yang bertujuan untuk menilai pemahaman dan pengetahuan individu tentang taktik kejuruteraan sosial dan keupayaan mereka untuk melindungi diri mereka daripada serangan sedemikian adalah dicadangkan. Kajian ini akan merumuskan penemuan utama, seperti tahap kesedaran dan pemahaman taktik kejuruteraan sosial dalam kalangan populasi yang dikaji. Ia juga akan mencadangkan cadangan untuk meningkatkan kesedaran dan pengetahuan keselamatan siber berdasarkan penemuan kajian. Matlamat keseluruhan kajian adalah untuk meningkatkan keupayaan individu untuk mengenali dan mempertahankan terhadap serangan kejuruteraan sosial, sekali gus mengurangkan risiko pelanggaran keselamatan dan ancaman siber lain.

Table of Contents

List of Figures

List of Tables

CHAPTER 1: INTRODUCTION

1.1 Introduction

Scammers are attempting to steal user personal details by employing new techniques. The approaches may be made in person, on social media, through email, phone call, text message, and so on. Scammers use the most recent advanced technologies to obtain personal information and money. Vast areas of younger users, notably college students, have significant financial shortfalls that are receiving progressively more attention. The importance of making wise financial decisions that affect a variety of living circumstances has increased as a result of recent economic conditions. The financial knowledge of users, particularly university students, appears to be less prepared to address these financial issues as the requirement for essential financial knowledge rises. The university population (18 to 25 years old) seems to be particularly affected by this (Williams & Oumlil, 2015). There are many ways for university students to fall victim to scam, whether they are negotiating financial aid or scholarships, jobs, or even on social media.

The purpose of this study is to assess the likelihood of UNIMAS students being exposed to cyber threats. As financial services increasingly become the primary target of continuing attacks in the global cyber security business, the assessment will be centered on social engineering attacks in this sector. A set of questionnaires will be distributed to students on campus from various backgrounds to collect datasets prior to developing the evaluation. The datasets will be used to design a few scenarios of cyber-attack which will then be spread to the students to study how they will respond to suspicious senders. A statistic will be accomplished by utilizing the evaluation data to examine and assess the number of students who were duped by suspicious senders. The statistic

collected will be analysed for the formulation of effective countermeasure recommendations against social engineering attacks among campus students.

1.2 Problem Statement

The financial industry is one of the main targets for cybercriminals using cyber security attacks. Although internal and user banking websites and applications are designed with safety mechanisms, it is frequently the human factor that fails to recognize the scam, leading to robberies of all sizes. Due to their technological focus on psychological manipulation and ongoing increase in frequency, social engineering assaults may be among the most harmful types of security and privacy threats.

Social engineering is the practise of phishing in which the victim is led to divulge their login information, which is subsequently utilised to access networks or accounts. Human are thought to be the weakest links in the chain, into providing information. Due to their heavy reliance on the internet, students are more vulnerable to many types of cybercrimes, particularly when interacting with banks. These attacks take place because students themselves are dangerously unaware of social engineering, not because bank security systems are lacking. Essentially, the idea behind social engineering is to use psychological trick to get data out of users and then use that information to compromise a system (Elsadig Adam et al., 2011).

The number of social engineering attacks that have been carried out, the most of which have been successful, has been continuously rising in quick succession for some time, and it has become an exceedingly serious security issue(Indzhov Ognyan & Axel, n.d.). Numerous attackers achieve success in various ways by altering the beliefs of many people on a variety of issues. They may give their victims fake information that is similar to that which prevents proper thought and

confusion. They also profit from the fact that in times of need and emergency, people might ignore procedures. In order to get clients to respond fast, the social engineer may employ the techniques of urgency and intimidation. Cybercriminals may trick their victims using a variety of techniques, such as encouraging impulsive clicking on specific websites (Dawabsheh et al., 2021b).

1.3 Aims and Objectives

- To propose effective countermeasure recommendation against social engineering attack based on student response pattern in cybersecurity assessment related to online financial services.
- To design a comprehensive phishing assessment related to online financial services using open-source software.
- To conduct an effective and controlled phishing assessment for the purpose of assessing UNIMAS students' awareness level on social engineering attacks related to online financial services.
- To analyze and perform comprehensive review on the state of readiness of students towards cybersecurity threats focusing on online financial services.

1.4 Scope

This project is conducted among the students in UNIMAS from various backgrounds which will solely focuses on phishing through social engineering attacks to analyse how they react to various social engineering attack scenario including malicious link seemingly legitimate phishing email focusing on online financial services. The evaluation data will be used to create a statistic that counts the number of students that fell for the malicious attack. In order to develop effective recommendations for countermeasures against social engineering attacks among university students, the statistics gathered will be analysed.

1.5 Research Question

1. What is the state of cybersecurity social engineering awareness in online financial services among undergraduate students in UNIMAS?
2. Do undergraduate IT students have higher level of awareness on cybersecurity social engineering compared to undergraduate non-IT students?

1.6 Significance of The Project

The significance of this project is to assist regular users in better understanding of social engineering and to educate them about the attack. Notwithstanding efforts to increase awareness of this cyber threats issue, numerous people keep falling victim to these kinds of attack every year even though they are very simple and that many people are still vulnerable to these threats because of a variety of different causes (Indzhov Ognyan & Axel, n.d.). The finding demonstrated the methods a cyber attacker could use to scam the victim. Additionally, this also aids in preventing exposure to and defending against this kind of threat.

1.7 Chapter Outline

Chapter 2 presents a literature review that includes introduction to literature review, theoretical framework, review on individual characteristics affecting social engineering awareness, types of financial frauds, review on methods of social engineering attacks, countermeasures against social engineering and summary of the chapter.

Chapter 3 review on the methodology of this project. The first part of the chapter discusses on the introduction to methodology. The methodology is divided into three phases including information gathering, threat modelling and simulation and vulnerability analysis. The last part of the chapter discusses the summary.

Chapter 4 focuses on implementation, analysis and discussion. This chapter includes introduction, survey questions, survey analysis, simulation process, simulation result, discussion and recommendation and summary.

Chapter 5 discusses on conclusion and future work where it includes introduction to the chapter, objective achievements, project limitations, future enhancements and improvements and summary.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

A literature review is an objective, brief, critical overview of published research literature pertinent to a topic being explored in an article. It is also known as a "relevant review of the literature". In this chapter, there are a few subsections that make up this literature review which consists of theoretical framework, review on individual characteristic affecting social engineering awareness, types of financial scams, review on methods of social engineering attack and countermeasures against it and comparison between Phising-As-A-Service (PHAAS) frameworks.

2.2 Theoretical Framework

The development of numerous software tools has been facilitated by the accessibility and availability of the Internet. Through the Internet, a lot of challenges have been made simpler and more adaptable to handle. It is now impossible to ignore the continuous availability of services offered online by several organisations and businesses. The most crucial issues that organisations face today are information and data. Despite the numerous safeguards and procedures that businesses implement, information and data are occasionally breached and taken. Humans are therefore regarded as the weakest link (Dawabsheh et al., 2021a).

Social engineering is the practise of persuading a victim to join a fake connection through the use of behaviour and skills. Social engineering attacks can be either technology-based or human-based. Human-based social engineering is accomplished based on relevant relationships and human-to-human interaction. Contrarily, technology-based social engineering is carried out through an electronic connection like a web, email, or social media connection (Dawabsheh et al., 2021a).

Based on Dawabsheh et al., 2021, table below describes the definition of different types of social engineering.

Table 1 Social Engineering Attacks

	Types of Social Engineering	Definition
Human-based social engineering	Dumpster diving	It is the process of sorting trash for individuals and businesses to locate any discarded things that could contain sensitive information, including such usernames and passwords, that requires to be used.
	Shoulder surfing	The intention is to observe and immediately receive information, such as when a person is staring at a keyboard or machine screen from behind.
	Baiting	Attackers may leave malware-containing storage media in a location that is accessible to victims. The material is similar to "road

		apples," such as laying a USB drive with a Trojan horse at a company's gate to lure any employee to enter it into the organization's computer.
Technology-based social engineering	Phishing	Phishing is the act of sending fake emails or other forms of electronic connection to obtain data and information. Typically, the electronic communication looks to be coming from a trustworthy and legitimate source. The problem arises when the victim is instructed to click on a fraudulent link intended to steal their private and confidential information.
	Pretexting	Typically, this is based on the basic scenario principle. The victim is given a hazy piece of writing that

		encourages them to assist indirectly in disseminating free information such as date of birth, legal name, social security number and other personal data. Typically, this scenario is planned out and properly thought out.
	Vishing	a kind of phishing attack that typically uses VoIP over Internet Protocol (IP) to trick the target and persuade them to reveal private and sensitive data
	Pop-up Windows	This kind of attack refers to pop-up windows that display on the victim's monitor to report a failed connection in order to remotely launch malware on the victim's device with the victim's knowledge and permission. Sometimes they take the

		form of text messages sent to the victim informing them of viruses or other threats in an effort to get them to interact, download hazardous programmes, and run those programmes on their computer with their own assistance.
	Spoofing	There are multiple ways to access the source machine in this type of penetration and fraud attacks. Through email or other electronic contact, attackers may present themselves in a cunning way to conceal the victim. Attackers may use a variety of techniques, including changing and forging DNS and IP addresses, to carry out such attacks.

The basic idea behind social engineering is to employ psychological ploys to get information out of individuals and then use that information to compromise a system (Elsadig Adam et al., 2011). The attackers can also readily take advantage of psychological elements by manipulating the emotions of their victims and inducing fear or desperation in them. A target's emotional response prompts them to act without thinking things through and subtly prompts users to click a dangerous link. (Hanis Binti Tuan Kob et al., 2020). Based on Dawabsheh et al., 2021, this research project will be focusing on technology-based social engineering solely on phishing attack.

The majority of phishing attacks use emails that contain links to dangerous websites(Bullee & Junger, 2020). Sending an email that needs the recipient to do more than only interact with it but also submit their credentials is one technique to test the human side of security vulnerability. When the target interacts with the phishing email for research purposes, it will ping back to a site to indicate that the scam message was clicked. The fake email sent must make use of excuses that entail greed, fear, surprise, or sadness in order to achieve this objective. Since the target's attention is needed at these stages in order to view the email attachment and log in with credential, the emotional triggers must be more potent (Hadnagy, n.d.).

2.3 Review on Individual Characteristics Affecting Social Engineering Awareness.

A study by Elsadig Adam et al., 2011 that were done among students in IIUM University shows a high number of respondents that has been exposed to social engineering attack through emails. Overall, results showed that 50% of IT students were aware of the word "Social Engineering", compared to only 28% of non-IT students. This difference reflects a higher awareness rate among IT students. Postgraduate IT students had a higher knowledge of social engineering than undergraduate IT students, with a percentage of 61% versus 45.5% at that time. One of the most

common social engineering scams is exploitation of individuals to obtain their bank accounts and other relevant information. Compared to non-IT students, IT students had a lower victimization rate (4.4% against 7.3%). After receiving an email from "friends," respondents also showed some certain awareness level. Nevertheless, some students still lacked awareness, which was found to be between 23% and 16% among non-IT students and IT students, correspondingly. Based on result of phishing phone scam made in this study, one out of twelve students that were engaged in the experiment fell for the trap and revealed a personal information.

In research by Hanis Binti Tuan Kob et al., 2020 two types of phishing attacks simulation on social medias were done among undergraduate students in Malaysia. Based on the study, both attack simulations showed that although more women open emails than men, males had higher tendency to follow the suspicious link, which could expose them to such attacks. As the respondents of the study were divided to two group of ages, 17 to 20 and 21 to 30, findings result revealed that the older group being more vulnerable to phishing scams. The findings also shows that undergraduates are easily being deceived by phishing scams with the highest percentage of diploma and bachelor's degree students being the victims. The percentage of IT students being deceived by the attack were also quite high which is 25% given that they may have learned about these security exploits in their lectures. However, the percentage of non-IT students were still higher compared to IT students on both attacks. According to the findings, given that the majority of the undergraduate students had opened the emails provided to them from the very first day, it can be inferred that the students may have felt some urgency or curiosity regarding something they had just received. There are some students even carelessly clicked the links that were attached. This demonstrates how undergraduate students are particularly vulnerable to falling victim to phishing attacks.