A STUDY OF AWARENESS OF CYBER SCAMS AND CYBERSECURITY AMONG UNIVERSITY STUDENTS IN MALAYSIA

BONG XU LIN

A RESEARCH PROJECT
SUBMITTED IN
PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE BACHELOR OF COMMUNICATION (HONS) BROADCASTING
FACULTY OF CREATIVE INDUSTRIES
UNIVERSITI TUNKU ABDUL RAHMAN

MAY 2023

A STUDY OF AWARENESS OF CYBER SCAMS AND CYBERSECURITY AMONG UNIVERSITY STUDENTS IN MALAYSIA

BONG XU LIN

A RESEARCH PROJECT
SUBMITTED IN
PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE BACHELOR OF COMMUNICATION (HONOURS) BROADCASTING
FACULTY OF CREATIVE INDUSTRIES
UNIVERSITI TUNKU ABDUL RAHMAN

MAY 2023

ACKNOWLEDGEMENTS

It would be impossible to complete this thesis without the assistance and cooperation of a host of individuals and organizations. I am therefore deeply thankful to Mr Anthony Gandolfo Miranti Jr (Head of Department of Media, and Dr Chong Eu Choong (Assistant Professor of the Department of Media).

I am deeply grateful to my parents for their warm and sweet encouragement as well as their understanding. Besides, I would also thank my supervisor Mr. Beh Chun Chee for the guidance on how to improve the contents of my final year project. A big thank you to all my family and friends who gave me moral support and encouragement throughout the whole process.

To every one of you, I would like to express my gratitude to everyone who gave me support. This thesis has been completed by having all of your efforts and contributions.

BONG XU LIN

Approval Form

This research paper attached hereto, entitled “A Study of Awareness of Cyber Scams and Cybersecurity Among University Students In Malaysia” prepared and submitted by “Bong Xu Lin” in partial fulfilment of the requirements for the Bachelor of Communication (Hons) Broadcasting is hereby accepted.

Date: 10 May 2023

Supervisor
Beh Chun Chee

ABSTRACT

The number of Malaysians using social media has grown. The availability of the infinite social network has been linked to a rise in the occurrence of cybercrimes in Malaysia. Based on the cases that have taken place, most cases are due to lack of awareness of cyber scams and cybersecurity. Therefore, this study aimed at measuring the awareness level of different cyber scams and discovering awareness of cybersecurity among Malaysian university students. In this study, quantitative online surveys were used during the data collection process. A total of 50 respondents have been involved in this survey. As a result, it showed that respondents had the highest level of awareness of merchant fraud. For awareness in cybersecurity, university students were more conscious of their privacy. A cybersecurity awareness program can be conducted as a suggestion in any tertiary institutions. Hopefully this study will reduce the number of cases of cyber scams and at the same time, strengthen the awareness of the major concern group, university students in Malaysia.

DECLARATION

I declare that the material contained in this paper is the end result of my own work and that due acknowledgement has been given in the bibliography and references to ALL sources be they printed, electronic or personal.

Name : BONG XU LIN

Student ID: 19UJB01979

Signed :

Date : 8th May 2023

TABLE OF CONTENTS

LIST OF TABLES

LIST OF GRAPHS

CHAPTER I

INTRODUCTION

1.0 Background of Study

Through innumerable websites and apps, social media has become a significant part of many people's lives, allowing them to interact with others and share their ideas, feelings and experiences. It has the potential to be a source of shopping and entertainment, and many companies have even found it useful for marketing and promotion (Sharma & ph social media, 2022). With this explanation, it seems as though people couldn't live without social media because of its enormous influence on society. According to Malaysia Digital Marketing, it stated that WhatsApp, Facebook and Instagram were the most used social media platforms in Malaysia (Malaysia Digital Marketing, 2022). The main pros of them are definitely that they can reach thousands of people from anywhere, this may ease the communication between people through social media platforms, the convenience that face-to-face is not necessarily anymore. Besides that, social media does benefit those online businesses. Since it can reach millions or billions of people on networking platforms such as Facebook, Instagram, Twitter etc. This makes the online businesses get attention from the users. In spite of that, there are also cons for social media. These days the public is handling a phone, clicking into social media platforms, and started checking on the latest posting, others' pages, accounts. Without realizing it, probably two out of ten were getting hacked by the fraudsters. This is called a 'cyber scam', refers to someone who uses software or online services to scam or exploit victims, usually for financial gain (Clare Stouffer, 2022). This problem occurred when there was a lack of awareness about cybersecurity among people. Social media scamming referring to an attack on social media platforms like Facebook, Instagram, Twitter, and others. According to CCID's Superintendent Madhavan Nair mentioned on New Straits Times that since 2020, 48,850 online

scams have been reported (David, 2022). Linked from this seriousness, the researcher has more concern on the university students in Malaysia which are known as the ‘Z generation’ in the society. They belong to the latest generation which uses social media platforms for one of their daily essentials, plus the study from a book titled ‘Cyberpsychology, Behavior, and Social Networking’ showed that more than one-third of 295 Malaysian students have fallen into social media scamming (Kirwan et al., 2018). This makes the researcher enthusiastic to figure out their awareness level for cyber scams. There are many websites, even postings that speak briefly of the happenings of social media scamming and how to notice them. For instance, Panda Dome website they have listed down 10 different social media scams that could take place to all of us (Security, 2020). Which are lottery and free gift card scam, gossip scam, healthcare scam, catfishing, photo of you scam, account cancelled scam, the 419 scam or Nigerian scam, stuck abroad scam, IQ scam and see you viewed your profile scam. But here to emphasize their content about scams could happen is the victims’ greed, curiosity, trust etc. We have been reminded many times but somehow, we still have people who have fallen into traps again. Based on a news article by New Straits Times, it says that the police predicted that young people, particularly students, would become scammers' newest prey (Basyir & Naz Harun, 2022). Occurrence of these problems make the researchers want to emphasize on this topic once again on Malaysian university students.

Mentioned about the cyber scam encounter affected by the cognitive of cybersecurity awareness. It belongs to the first step before it becomes a proper culture for all of us, as cybersecurity is an understanding security danger and acting responsibly to minimize risks are two components of cybersecurity awareness (Apps, 2023). As what a computer and informatics organisation from India they have mentioned that understanding the scope, application, and appropriate usage is crucial for cybersecurity. Many people don't realise that cybersecurity

extends beyond protecting online computers. To protect the hardware, software, data, and information found in an online system against any type of compromise is to practise cybersecurity. For individuals, privacy and access control are important for their cybersecurity awareness (Tirumala et al., 2019). Thus, cybersecurity as an independent variable that could affect the occurrence of cyber scams, it acts as a significant in this study as well. The research is going to figure out the cybersecurity awareness among Malaysian university students so that it could help them to prevent from cyber scams encountered.

1.1 Problem Statement

Presently, there is still a lack of studies about the level of awareness for specific fields of scams. Mostly placed to identify the factors that affect their awareness of social media or targeted on the general scamming instead of narrowing it down to certain scam. From the perspective of researchers, the main concern to avoid cyber scams is to increase the awareness of cyber scams among the target respondents, Malaysian university students. Hence, it is important to focus on the level of awareness for different cyber scams first before getting into the factors that affect the tragedy of scamming. There are many different scams that can be done by scammers on social media which include e-commerce, illegal loans, jobs, investment schemes and money mulling etc. However, this study focused on four cyber threats which are phishing scams, investment schemes, romance scams and merchant fraud based on our interest in the age of 18-26 years old Malaysian university students' perceptions of cybersecurity.

1.2 Research Objectives

The aim of undertaking this study is:

1. To measure the awareness level of different cyber scams among university students in Malaysia.

2. To discover the awareness of cybersecurity among Malaysian university students.

1.3 Research Questions

1. What is the awareness level of different cyber scams among university students in Malaysia?
2. How aware are the Malaysian university students in terms of cybersecurity?

1.4 Significance of Study

The study would be useful in detecting the awareness for cyber scams and cybersecurity among Malaysian university students. The goal of this study is to caution the community of students about the occurrence of cyber scams and also raise up their awareness on their cybersecurity. Besides, the study also aims to reduce the number of cases for cyber scam going to happen in Malaysia.

1.5 Summary

This chapter introduced the background of study, problem statement, research objectives, research questions and significance of study.

CHAPTER II

LITERATURE REVIEW

2.0 Introduction

This section highlights the key findings from previous or past studies that have been conducted on the awareness of cyber scams and cybersecurity. It will discuss the awareness level of different cyber scams which include phishing scam, investment scam, romance scam and merchant fraud respectively. Simultaneously, cybersecurity awareness will be talked through also by mentioning the basic knowledge for cybersecurity be made up of privacy, password management and trust.

2.1 Types of Cyber Scams

A higher-level awareness of cyber scams could reduce the occurrence of cyber scams. Yet, this awareness is depending on the person itself. According to a study from New York researchers, they had done an interview with five scammers to understand why they have the urge into Internet scamming (Claude Tambe Ebot & Siponen, 2014). The result shows it can be explained with an interaction between socioeconomic and dynamic thinking processes. For those scammers who are around 30 to 38 years old, they probably do it for revenge, or we can say payback. When a person does nothing while reaching their middle age, they have the urge to do something that is highly paid for their entire life. For example, they did Internet fraud which got a good reward especially financially as the most pragmatic way to accomplish that was through internet fraud. While for scammers who are between 20 to 24 years old, they stumbled into scamming because the opulent lifestyles of the more experienced fraudsters enticed them. Nevertheless, these results can’t be fixed for all scammers who commit cyber scams. There are thousands of tricks that could happen, however in this research we are going

to focus on the general four cyber scams that frequently come into being among us. First to explain details and knowledge about each scam before survey the awareness level for each scam among our targeted respondents, university students in Malaysia.

2.1.1 Phishing Scam

People communicate through social media, while phishing assaults cannot be avoided in online communication. Phishing attacks are usually used when an attacker who poses as a reliable source tries to trick the recipient to click into malicious links (McKeever et al., 2020). They could be using email or short message service (SMS) to send those ransomware attacks. Ransomware is a sort of malware attack in which the attacker locks and encrypts the victim's data, critical files, and then demands money in exchange for the decryption and unlocking of the data (McKeever et al., 2021). Whenever the recipient clicks into it, it may cost them data loss, even financial loss as their user data and card number could be stolen by a hacker. For instance, we received an email or text from an unknown sender and at the moment we clicked into the malicious link, our device could be hacked immediately, and we would lose our privacy and data. By focusing on university students, a study from Purdue University mentioned that younger participants (18 to 25 years old) were more subject to such attacks, mostly because they have less exposure to technological expertise, are less comfortable with the internet, and have not had any phishing training (Kancherla, 2017). However, their result shows students with higher education would be less likely to be involved in phishing attacks because of their wisdom and information about phishing. They have also brought up the number one reason why phishing scams keep happening is due to lack of training and awareness about this issue. As students, they use email to check messages and information ordinarily. Leading phishing scam to occur more often in email receiving. In order to reduce the cases of this scam, either to improve the security system of school authority or to enhance the cybersecurity attentiveness

of students themselves. From this research we are going to observe a degree of awareness among university students in Malaysia so that phishing scams can be taken into the attention of related authorities such as school and government as well.

2.1.2 Investment Scam

Owing to the fact of coin depreciation, people start working on investment nowadays. It could be the easiest and fastest way to earn money. Bringing investment fraud to happen, which apparently scam for the purpose of monetary gain. ‘The victims' desire to enhance their income, lack of resources in life, susceptibility to persuasion, faith in their own abilities, and carelessness contributed to their involvement in investment fraud’, a thesis by PhD in Criminal Justice mentioning that actually the origin of investment scams is all from the victims themselves (Badua, 2020). Greater vulnerability results from a desire for money. How does this investment fraud work? The most common gimmick that we see is ‘pyramid schemes. It works by promising to pay the members if they are able to recruit more members to join the investment package. Other than that, a ‘gold investment scam’ is even worse than a ‘pyramid scheme’ because the victim will have to pay an amount to the company before they get their promised money back. This will cost them financial loss. Basically, the company would try to bother them with advantages and rewards. In order to compromise them to join the investment package which is fake. An online information from Ariel Chew has provided lots of wisdom about investment scams and the way to prevent them, and it has also given advice to all investors saying that ‘prevention is better than cure’(Chew, 2016). Along with changes with time, we are now living in the golden age of financial technology (FinTech), ‘money game’ has come about as a talking point around people. According to knowledge instructions from Greaterthan, money games required 8-15 people to ‘play’ (The Money Game Experience, n.d.). It indicates the participants will be asking to let go of a meaningful sum of money that they feel

comfortable letting go of. The amount will be around RM10-RM500. Literally, RM10 can be only a small amount. However, after a few rounds the accumulation of the amount could be up to RM1000 or even higher. This is why people get tricked in money games. This kind of investment is suitable for people who do not have a high income or resources, especially students. The awareness of getting scammed from money games should blaze up among them. Although there are benefits from investment which receive extra salary, at the same time they should watch out for scammers as well. Therefore, their awareness about investment scams is significant in this research.

2.1.3 Romance Scam

For the age of a student around 18 to 26 years, to be loved by a lover is blessed. They desire a sense of romance to happen to them. Normally, people get into a relationship by meeting face-to-face, either they get to know each other well from friend to couple; or love at first sight. According to an expert blogger Sylvia Smith, stated people get to be in a relationship, it is due to there being someone who clearly understands you, who makes you feel romantically happy and an all-time accountability partner etc. reasons that make people craving for a romance relationship (Smith, 2021). It seems like people who fall in love are able to fulfill their needs. However, if all these actions can be done on the internet, which means online, what's the possibility that people could fall in a romance scam? As we know, nowadays masking on social media is normal. Sometimes, we chat with anonymous people online without really realizing who the actual person looks like in reality. During the MCO lockdown period, we can't hang out with friends nor meet new acquaintances. This led to dating apps such as Tinder, TanTan, Bumble etc. becoming well known around youngsters (The ASEAN Post, 2020). "Not just to find love, but for some sort of human connection". On the authority of an article by Universiti Kebangsaan Malaysia which did an analysis about the steps and strategies of an online romance

scam that happened in Malaysia, it concluded that a scammer's strategies include three stages: initial, pre-attraction and hooked (Shaari et al., 2019). Firstly, initial stage cover 'trust' between scammers and their potential victim. Their relationship establishes and contacts with formal conversation. After that, scammers begin to involve a more personal level of communication by sharing their profiles like culture background, education, images and friends in the pre-attraction stage. In this phase, scammers may be using fake profiles just like masking, and strengthen the relationship by using words or phrases that are similar to the victim. For instance, religious connotations such as 'Allah God bless you' and trustworthy words 'I'm very honest' to victims. To make victims believe that scammers have the same feelings as them. In the final hooked stage, scammers start to create a more flexible, casual conversation with their victims. It could be telling victims that they have financial problems or any possible situations that money is needed. Just because the relationship has been developed, the victim falls into the trap. Since our target respondents are university students, romance scam has been listed down to get their attention in sequences to reduce the number of romance scam victims in Malaysia.

2.1.4 Merchant Fraud

When a fraudster pretends to be a merchant in order to handle transactions and steal money, it is known as merchant fraud (Gurus, 2021). In short, scammers use fake identity to create a business account in order to trick the buyers' money, which is what happened to merchant fraud. How's normally a merchant fraud could happen? It is due to online shopping. During two years of MCO lockdown, people have been restricted from stepping out of home to in-store shopping. The use of electronic shopping (e-shopping) has begun to sprout among us. It was mainly for crowd avoidance at that time, yet it still continues to be used by the majority for its convenience, cheaper price etc. that made people addicted to it. Official e-shopping platforms like Shopee, Lazada, Taobao etc. are popular in utilization rate. While there are also

some unofficial websites that operate business online. For the reason of technological advancement, scammers use the internet to commit crime. In this case, they normally belong to unverified merchants and shady their front store products so as to trick their potential victim into traps (Love, 2022). Referring to wisdom authored by Dhruv written in a website called PayU Blog, there are three different types of merchant fraud. First and foremost, bust-out fraud is the common fraud where the criminals dupe their victim by selling things on a fake store and processing fraudulent transactions, vanishing after that. Secondly, transaction laundering refers to some kind of 'structuring' their business by handling credit card transactions using a legitimate company's merchant account. Through the use of a low-risk merchant category code, they are able to obtain normal merchant processing while also taking advantage of lower rates and fewer restrictions. Lastly belongs to identity swap in which the criminals manage a real store online but with no actual sales. Usually, they use it for illegal activities' transaction such as drug cartels (Dhruv, 2022). Focus point on university students, research by Global Business and Manage Research had shown that nowadays university students are loyal customers to e-commerce (Abdullah et al., 2022). They will prefer platforms that give them the highest value such as satisfaction like web design, system availability and contact services. In the case when those fraudsters fulfilled all these factors, users track into the trap easily as well. Hence, this study is going to investigate university students' awareness of this merchant fraud in order to reduce scam cases.

2.2 Cybersecurity Awareness

It is connected after mentioning the awareness of cyber scams. The tragedy of cybercrimes can be reduced if cybersecurity is being taken. According to a case study from Universiti Teknologi Malaysia, they found out that the university students in Nigeria lacked the basic knowledge of cybersecurity (Garba et al., 2020). Surprisingly, 346 out of 367 respondents strongly would

like to learn more about cybersecurity. From this research, there is a need to conduct a similar case study for Malaysian university students in order to understand their cybersecurity awareness and whether any of the cybersecurity awareness programs are considered in tertiary institutions. Lack of awareness of cybersecurity has some negative effects. Fundamentally, internet users will be easily influenced by the scammers due to their uninitiated experience in cyberspace and it is a high probability to get involved in cybercrime (Kamalulail et al., 2022). The basic knowledge of cybersecurity including privacy, password management and trust. The knowledge factors are way more significant than any demographic, social media attitudes and environment factors (Kamalulail et al., 2022). As social media users, it is critical that they have the knowledge and ability to control their social media (Saizan & Singh, 2018). In fact, since awareness of cybersecurity is very important, a conference from Barcelona, Spain had proposed for increasing public understanding and awareness of cybersecurity via necessary steps and researchers from University of Belgrade mentioning that educational institutions could take a more active approach to improving students' cybersecurity knowledge in order to protect themselves from cyber-attacks (Al-Mohannadi et al., 2018) (Kovačević & Radenković, 2020).

2.2.1 Privacy

First and foremost, sharing something on social media means parting ways with your privacy (Privacy on Social Media, n.d.). We are free to use and post anything on our social media platforms. For example, before creating an account on Facebook, we were required to fill up our personal information such as full name, date of birth, contact details, etc. which were already in the situation of possible consequences of being scammed. From the case study from UiTM Negeri Sembilan, they had reviewed that every user on the internet had to know privacy refers to keeping personal information private and away from people with bad intentions is

crucial (Kamalulail et al., 2022). Besides that, the willingness to share personal information with others should be reserved for people who can be trusted, and any information shared by others should be checked and verified. Anyhow, getting scammed is unavoidable when the fraudsters were the major-league and expert on how to swindle a person perfectly. As a user can only do their part of privacy management well. For instance, set the security model of "visible only to me" as default option on any social media platforms. In spite of that, posting daily stuff on social media seems to be accustomed to. Hence, as users we can't really keep everything private unless we are the one who is disconnected from social media, also known as a 'lurker' to others. As stated by an author Megan Ellis, a lurker is someone who does look at social media, social media profiles, and forums but does not interact or post anything (ELLIS, 2019). One of the slang terms used in social media. This makes us have a contradiction that we have to care for privacy at the same time as using social media for our daily essentials. However, we still have to be aware of privacy cybersecurity so that cybercrime can be prevented.

2.2.2 Password Management

Every social media account needs a password to login. Normally, the password manager suggested users to create a strong password with at least 8 characters long and use a combination of upper- and lower-case letters, symbols and numbers. However, such a strong password is difficult to remember, so users were forced to write them down, making them more vulnerable to cybercrime. Research by Mohammed A. Alqahtani had also revealed that 11.5 percent of users generate their passcodes using their username and email, while over 12 percent use their birthdays and mobile phone numbers. People created passwords with numbers that they are familiar with in order to remember well (Alqahtani, 2022b). According to a review by the same author also, a survey discovered 80% of users kept using their current passcodes wherever possible. The hackers could just try the same password to log into their multiple

accounts at once, this might easily result in a cyber scam. Hence, there are few other ways to replace passwords or to concrete the users' password security, which also means password alternative. There are multi-factors authentication (MFA), biometrics password, etc. that we can often find from any website. The MFA approach requires two or more pieces of evidence to authenticate the login user. The common form of MFA that we used was two-factor authentication (2FA). 2FA strengthens the authentication process' security by making it more difficult for hackers to access a user's devices or online accounts (Rosencrance et al., 2021). It added the second layer for login to an account. Normally, after entering the password the user will have to answer a simple question such as 'What is your favourite fruit?', something that only the user self-knows. Otherwise, one-time password (OTP) is used, in which the user will receive a unique password or 8-digit code thru short message service (SMS) on their actual phone number. The OTP will basically only be valid for 30 seconds to 1 minute duration. If the user failed to enter the code on time, the login failed automatically. Besides that, biometrics approaches include facial recognition, fingerprint scanning, voice authentication, etc. which require any parts of the users' DNA to unlock. This password alternative approach is considered as the strongest way of login since the user has to present tangible identification to access their account. Password as the major element before entering an account. Even if the MFA approach is functioning, there still could be a possibility of cyberpunk trying to hack users' passwords. Thus, password management is listed among the cybersecurity awareness to inform users to be defensive with it.

2.2.3 Trust

A connection between a trustor and a trustee is referred to as a trust (Tang & Liu, 2015). When it comes to trust, we take the easy route or shortcut by asking trustees or other reliable sources for information directly by considering that we have faith in what the trustee stated. In this

research, we focus trust on social media and cyber scam. How does trust affect cybersecurity of the users? How and why did the users believe information or people in the media easily? Social media provides information sharing and communication. When it comes to information sharing, trust is needed. As a user, we have to make ourselves believe in the fact that is given by the sender, before we take it into consideration. However, a blunder trust or we say mistrust, could bring consequences such as cyber scam, phishing attacks etc. Normally, cyberpunks or we know as hackers use it to fulfill their goal, which aims to bother their target sufferer. As mentioned above, social media provided information sharing and communication thus people nowadays relied on it to satisfy their needs. In spite of that, it can be risky to seek information on social media. From the literature by Ingrid Hsieh-Yee, she has identified that trust and risk as two related factors that influence social media behavior (Hsieh-Yee, 2021). In order to avoid consequences from mistrust, these trusting beliefs of Integrity, Ability and Benevolence can be assembled by users to define if trust is warranted. Firstly, Integrity is the conviction that the person or thing to be trusted is trustworthy, honest, and will act morally. Ability defines the trusted party's capacity to carry out their responsibilities effectively. It can be said as the “Authority” standard used to evaluate web resources and scholarly resources. Finally, Benevolence refers to the dependable party who cares about the user's interests, is well-intentioned, and prioritizes the user over the party's interests (McKnight et al., 2002). In short, Users must determine whether the source of the information is reliable and honest. Losses of time, money, safety, privacy, and other personal damage could result from trusted parties providing misleading information. Since trust is all controlled by users’ self, it is significant to let them understand the possibility of cyber scamming from mistrust. Hence, this is why trust has been listed among cybersecurity.

2.2.4 Awareness

No matter who we are, awareness of cyber scams and cybersecurity is significant for us as in this technological era the internet is kind of necessities. Users' ignorance of the hazards in cyberspace could lead to security problems. Hence, a suitable setting for educating people about the risks and periodically reminding them of them is cybersecurity awareness. As a solution, completing a brief online cyber security awareness course as a requirement for orientation has been proposed by research of American Institute of Physics. The students should be made aware of this from their very first day of college, and they may use it when they begin working (Ramakrishnan et al., 2022). However, it would be asked in this study also for the target audiences' decision whether to wish cybersecurity awareness as a course in their academic semester.

2.3 Summary

In this chapter, the research literature review has been discussed about each scam in details. Especially about its scam process. Besides, the section in cybersecurity awareness involved ways to improve each of the essentials of cybersecurity including privacy, password management, trust and awareness.

CHAPTER III

RESEARCH METHODOLOGY

3.0 Introduction

This section is going to highlight the research design, data collection method and research instrument used by the researcher. First of all, in order to obtain results, a quantitative approach was used as a method in this research. A quantitative research method deals with quantifying and analyzing variables. It entails the use of numerical data and statistical tools to analyze that data in order to provide answers to queries like who, how much, what, where, when, how many, and how (Apuke, 2017). The topic of this research is related to awareness, the researcher has to find out either higher or lower and statements explaining the statistics of Malaysian university students about cyber scams and cybersecurity consciousness. Hence, a quantitative approach had been used. Secondly, since the researcher was studying awareness among university students. Therefore, the target population goes to students as well. Simple random sampling used in the sampling method, which refers to each person in the population having the same chance of being chosen. The entire population should be included in the sampling frame.

3.1 Research Design

When the participants first clicked into the Google Form produced by the research, there are a total a of 4 questions asking for the demographic information of the respondents in Section A. After that, straight away to the next Section B contained 8 questions asking about the level of awareness for each scam including phishing scam, investment scam, romance scam and merchant fraud by using Likert scale measurement for rating. The lowest rate represents they are not aware of the scam at all while the highest rate representing, they are extremely aware

of the scam. After their rating, along with asking them whether they have encountered a certain scam before, to understand the victimization rate. A total of 2 questions for each scam, one for rating and one for encountering. A further study on the next Section C to understand their behavior when using social media sites and to discover how aware they are of cybersecurity. There are 14 questions for the overall cybersecurity awareness. Each 5 questions for questions about privacy and password management while the other 2 questions each for the trust and awareness questions. After completion of the questionnaire, a word of thanks was to be expressed to the participants.

3.2 Data Collection Methods

For the findings, the researcher had spread to 50 participants that aged 18 to 26 years to complete the survey online via answering on Google Form. Targeted Malaysian university students through social media platforms such as Instagram story, Facebook story and WhatsApp.

3.3 Research Instrument

This study using correlational research attempts to use statistical data to quantify the strength of a link between two or more variables (Key Elements of a Research Proposal Quantitative Design, n.d.). Variables are measurable qualities that are typically divided into dependent and independent variables based on the instrumentation. This study using correlational research attempts to use statistical data to quantify the strength of a link between two or more variables.

i) Dependent Variables

The main and only dependent variable belongs to the awareness of cyber scams of the Malaysia university students.

ii) Independent Variables

Several of independent variables were considered: the behaviors using social media sites with cybersecurity awareness for *(1) privacy, (2) password management, (3) trust and (4) awareness.* Besides, the encountered experiences could also be one of the independent variables to affect the awareness of cyber scams.

3.4 Summary

This chapter involved the research design of the questionnaire with data collection methods and the research instrument with dependent and independent variables respectively.

CHAPTER IV

FINDINGS & DATA ANALYSIS

4.0 Introduction

The awareness of cyber scams is the main significant outcome to study for in this research. In this chapter is going to analyze the results from the questionnaire that has been distributed to audiences aged 18 to 26 years to understand the level of awareness for each scam of Malaysian university students and their cybersecurity awareness. The data will be analyzing the acquired data by using tables and graphs.

4.1 Findings

4.1.1 Participants

Count of Age			Educati			
Age	Ethnicity	Gender	Bachelor's Degree	Diploma	Foundation	Grand Total
18 - 20	Chinese	Female	1		2	3
21 - 23	Chinese	Female	29			29
		Male	12			12
	Malay	Male	1			1
24 - 26	Chinese	Female	2	2		4
		Male		1		1
Grand Total			45	3	2	50

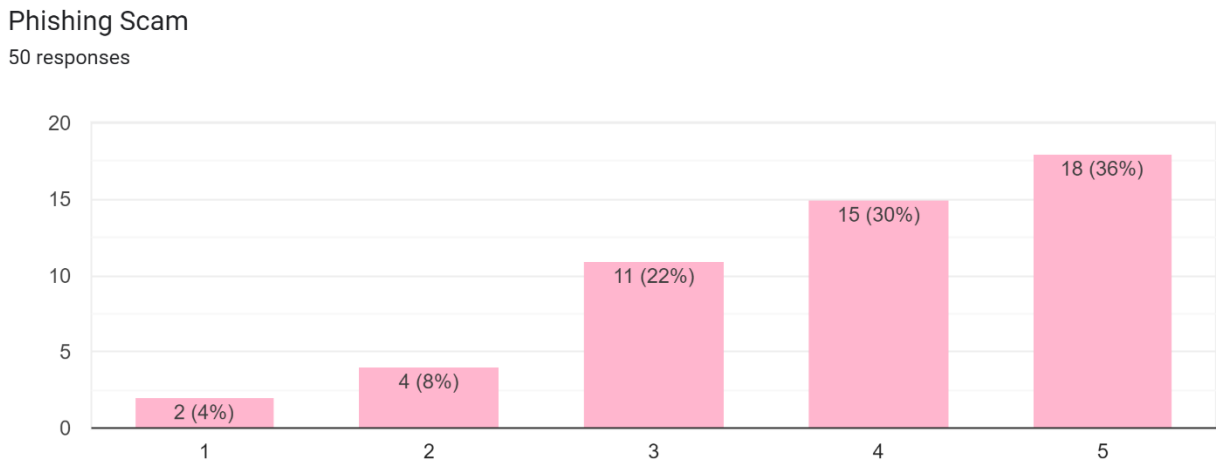
Table 4.1 *Total participants with analysis*

The researcher obtained data from the age of 18 to 26 university students in Malaysia of both genders regardless of race who are still studying whether in Foundation, Bachelor's Degree, Master's Degree, Doctorate or others. According to the data from (Ruby, 2023), the Internet User Statistics 2023 found out that the age group of 18 to 29 years old belongs to 99% of internet users. In the questionnaire having a total of 50 respondents. According to Table 4.1 it showed that the most participated in the questionnaire age range were around 21 to 23 years old which with 42 participants. The majority of respondents were female (n=36; 72 percent)

and left out (n=14; 28 percent) of male respondents. They were Chinese Malaysian in ethnicity (n=49; 98 percent). The one remaining participant was Malay ethnicity. For their education background, most of the respondents had their bachelor's degree at the moment (n=45; 90 percent), while three participants in Diploma and two in Foundation study.

4.1.2 Level of Awareness

Phishing Scam



Graph 4.2.1 *Phishing Scam*

First and foremost, we analyze phishing scam. The level of awareness for phishing scam among 50 university students in Malaysia conforming to Graph 4.2.1 shows that a total of (n=18; 36 percent) of them were extremely aware of this scam while (n=2; 4 percent) were not aware at all of this phishing scam. The data analyze that Malaysian university students having a quite high awareness in phishing scam as it has already crossed the half value standard of awareness of the overall. Since some phishing scams such as fake URLs and emails gradually become a common fraud among the society, we could saw those anti-phishing ads around us to warn people about phishing scams. They usually offer advice on how to recognize and avoid

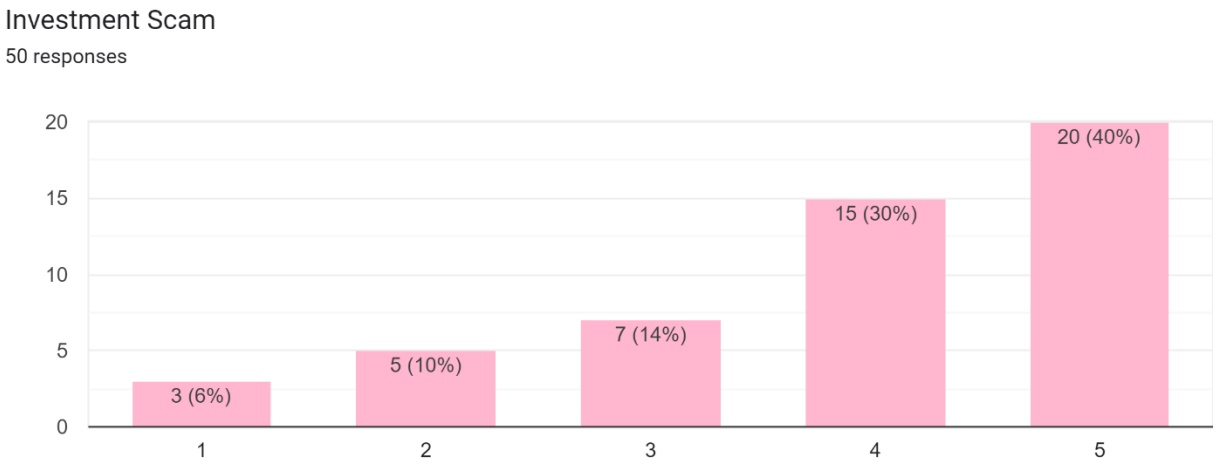
phishing emails, such as looking for misspellings or suspicious links. Hence, the awareness of getting phishing scam increased.

Gender	Have you encountered phishing scam before?	Age	Ethnicity	Count of Gender
Female	Yes	21 - 23	Chinese	14
		24 - 26	Chinese	2
	Yes Total			16
	No	18 - 20	Chinese	3
		21 - 23	Chinese	15
		24 - 26	Chinese	2
	No Total			20
Male	Yes	21 - 23	Chinese	6
			Malay	1
	Yes Total			7
	No	21 - 23	Chinese	6
		24 - 26	Chinese	1
	No Total			7

Table 4.2.1 *Have you encountered phishing scam before*

According to Figure 4.2.1 there are a total of 23 over 50 respondents that have encountered phishing scam before regardless male or female. We can obviously see that the age around 21 to 23 years belongs to the age for getting either a YES or NO when encountered in a phishing scam. Which means the people around this age especially females are most vulnerable to scams. For the remaining 27 respondents, they have not encountered a phishing scam before. In summary, for phishing scam, although the awareness level is high. However, the amount of victim fall in this scam is also quite a number. Therefore, it can conclude that phishing scam still needs attention for nip in a bud among university students in Malaysia.

Investment Scam



Graph 4.2.2 *Investment Scam*

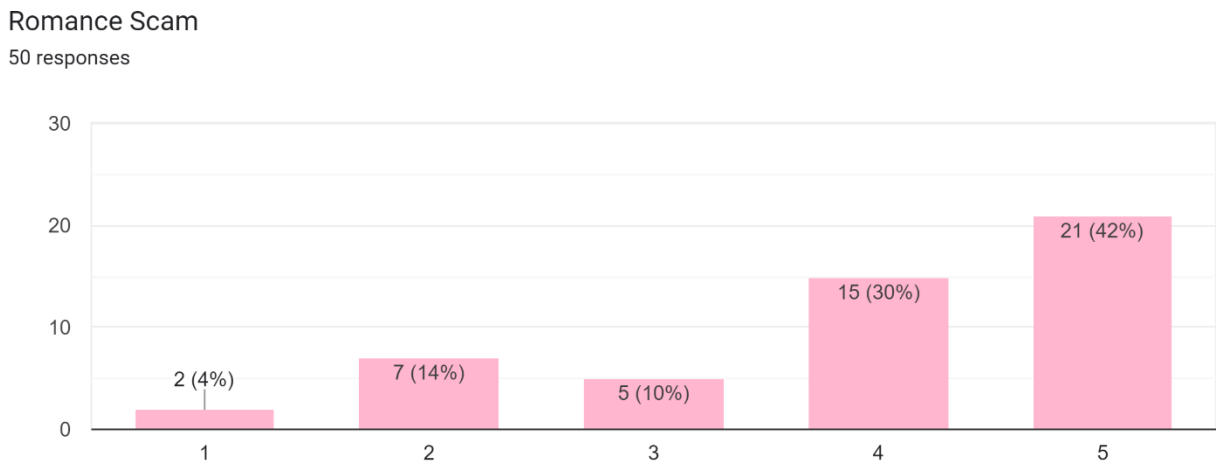
50 participants having quite high awareness in investment scam as the data from bar graph Graph 4.2.2 showed that (n=20; 40 percent) of them were rating 5 over 5 of awareness. However, (n=3; 6 percent) respondents were not aware of this investment scam. This may be because currently there are quite a lot of postings about preventing investment scams on social media platforms hence people get higher awareness for this scam.

Gender	Have you encountered investment scam before?	Age	Ethnicity	Count of Gender
Female	**Yes**	21 - 23	Chinese	5
		24 - 26	Chinese	1
	Yes Total			**6**
	No	18 - 20	Chinese	3
		21 - 23	Chinese	24
		24 - 26	Chinese	3
	No Total			**30**
Male	**Yes**	21-23	Chinese	2
			Malay	1
	Yes Total			**3**
	No	21-23	Chinese	10
		24-26	Chinese	1
	No Total			**11**

Table 4.2.2 *Have you encountered investment scam before*

Table 4.2.2 showed that of a total of 41 respondents, they were not encountered to any investment scam before, but the remaining 9 respondents were trapped before. In details we can see that, actually the amount of female participants that have encountered to investment scam before (6/36 = 16.6%) is lower than male participants (3/14 = 21.4%). It may be because of males are more interested and willing to invest in high-risk. In spite of that, it could not draw a conclusion for this general analysis. Research by (Lokanan & Liu, 2021) found out that the proportion of female victims' economic losses through investment is higher than males. It may also speculate that there are factors that cause women trapped into investment scam with unknown tricks.

Romance Scam



Graph 4.2.3 *Romance Scam*

For romance scam, Graph 4.2.3 showed that there are (n=7; 14 percent) of respondents only slightly aware of this scam. However, also (n=21; 42 percent) of them were extremely aware of romance scams too and (n=15; 30 percent) were moderately aware. We can see that a great majority of respondents have a rating of 4 to 5 for high awareness. However, there are still

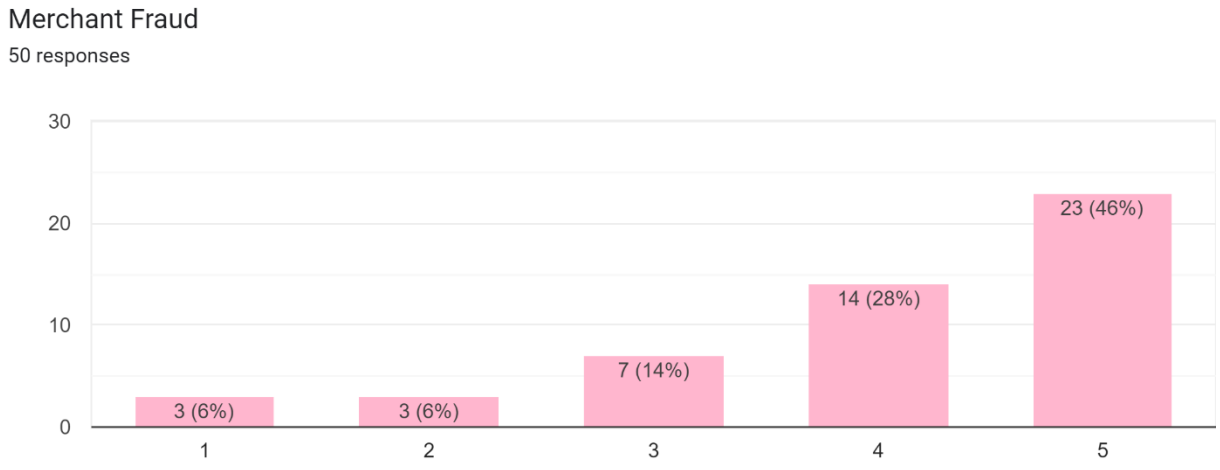
some of them only slightly aware of the romance scam. It may be because nowadays there are still lack of knowledge about this scam.

Gender	Have you encountered romance scam before?	Age	Ethnicity	Count of Gender
Female	Yes	21 - 23	Chinese	1
	Yes Total			1
	No	18 - 20	Chinese	3
		21 - 23	Chinese	28
		24 - 26	Chinese	4
	No Total			35
Male	No	21-23	Chinese	12
			Malay	1
		24-26	Chinese	1
	No Total			14

Table 4.2.3 *Have you encountered romance scam before*

According to Table 4.2.3 a high total of 49 respondents have not encountered any romance scam before, only one over 50 of them encountered before. The only one was female and she aged between 21 to 23 years. This indicated that there were very few of victim among Malaysian university students that have been run into romance scam.

Merchant Fraud



Graph 4.2.4 *Merchant Fraud*

Figure 4.2.4 showed that (n=23; 46 percent) respondents were extremely aware of the merchant fraud. There are only (n=3; 6 percent) respondents who are not aware of this scam. In between, (n=14; 28 percent) of them being moderately aware of merchant fraud while half of the respondents (n=7; 14 percent) were somewhat aware of this scam only. Overall, university students in Malaysia are still having a high awareness to merchant fraud.

Gender	Have you encountered merchant fraud before?	Age	Ethnicity	Count of Gender
Female	**Yes**	21 - 23	Chinese	9
		24 - 26	Chinese	2
	Yes Total			**11**
	No	18 - 20	Chinese	3
		21 - 23	Chinese	20
		24 - 26	Chinese	2
	No Total			**25**
Male	**Yes**	21-23	Chinese	2
			Malay	1
	Yes Total			**3**
	No	21-23	Chinese	10
		24-26	Chinese	1
	No Total			**11**

Table 4.2.4 *Have you encountered merchant fraud before*

Conforming from Table 4.2.4 we can notice that a total of 36 participants have not encountered merchant fraud before while 14 participants have been confined to merchant fraud before. If calculate in detail, we can know that the percentage of female respondents encountered to merchant fraud (11/36; 30.5 percent) is higher than male respondents (3/14; 21.4 percent). This can predict that because online shopping is more obsessive to females, most of the time males are not so into cybershopping. Thus, merchant fraud less likely happen on males.

4.1.3 Cybersecurity Awareness

Privacy

What is the privacy setting of your social media accounts?				
Gender	Age	Private	Public	Grand Total
Female	18 - 20		3	3
	21 - 23	22	7	29
	24 - 26	2	2	4
Female Total		**24**	**12**	**36**
Male	21 - 23	8	5	13
	24 - 26	1		1
Male Total		**9**	**5**	**14**
Grand Total		**33**	**17**	**50**

Table 4.3.1 *What is the privacy setting of your social media accounts*

The first question in the privacy section asking about the respondents' privacy setting of their social media accounts. From Table 4.3.1 we can see that overall, people are more tend to private their social media accounts as there are 33 out of 50 respondents chose to private instead of public their social media accounts. This can be understood as respondents are more care about their privacy, and control over who can see their content.

Do you accept friend request from strangers?				
Gender	Age	Yes	No	Grand Total
Female	18 - 20	3		
	21 - 23	4	25	
	24 - 26		4	
Female Total		**7**	**29**	**36**
Male	21 - 23	2	11	
	24 - 26		1	
Male Total		**2**	**12**	**14**
Grand Total		**9**	**41**	**50**

Table 4.3.2 *Do you accept friend request from strangers*

Accepting friend requests from strangers could bring online harassment and stalking. Followed by scams and phishing attempts. As advice we do not simply accept strangers' friend request. From the questionnaire, there are 41 out of 50 respondents that felt the same also as shown in Table 4.3.2. They do not accept friend requests from strangers except for people well-known.

Do you reveal your location on your social media?				
Gender	Age	Yes	No	Grand Total
Female	18 - 20		3	
	21 - 23	8	21	
	24 - 26	1	3	
Female Total		**9**	**27**	**36**
Male	21 - 23	4	9	
	24 - 26		1	
Male Total		**4**	**10**	**14**
Grand Total		**13**	**37**	**50**

Table 4.3.3 *Do you reveal your location on your social media*

Conforming from Table 4.3.3 total of 37 respondents that do not reveal their location on social media while 13 of them chose to show up their location. For privacy purpose, it is not recommended to reveal our location on social media which that means we are sharing our location on social media and can make it easier for cybercriminals to hack into accounts or steal personal information. The analysis showed most of the respondents are concerned about their privacy on social media.

It is not a problem to post your basic personal information on social media.				
Gender	Age	TRUE	FALSE	Grand Total
Female	18 - 20	2	1	
	21 - 23	12	17	
	24 - 26	2	2	
Female Total		**16**	**20**	**36**
Male	21 - 23	6	7	
	24 - 26	1		
Male Total		**7**	**7**	**14**
Grand Total		**23**	**27**	**50**

Table 4.3.4 *It is not a problem to post your basic personal information on social media*

Through Table 4.3.4 we can see that the number of respondents that decide to post or not post their basic personal information on social media is about the same. However, there is possibility that the 23 of them only posting necessary and appropriate personal information on social media such as name, date of birth and gender. No including any contact information. The data

analyse that posting personal information on social media mostly depending on the person, personal opinion will do.

Are you aware of posting private photography such as selfie could lead to scamming?				
Gender	Age	Yes	No	Grand Total
Female	18 - 20	1	2	
	21 - 23	21	8	
	24 - 26	3	1	
Female Total		**25**	**11**	**36**
Male	21 - 23	8	5	
	24 - 26	1		
Male Total		**9**	**5**	**14**
Grand Total		**34**	**16**	**50**

Table 4.3.5 *Are you aware of posting private photography such as selfie could lead to scamming*

We can obviously observe that respondents are aware of posting private photographs could lead to scamming as 34 out of 50 of them answered yes in Table 4.3.5. Despite that, people still getting selfie and post on social media as selfie has become the common routine among society nowadays.

Password Management

Do you use the same password for multiple accounts?				
Gender	Age	Yes	No	Grand Total
Female	18 - 20		3	
	21 - 23	20	9	
	24 - 26	4		
Female Total		**24**	**12**	**36**
Male	21 - 23	11	2	
	24 - 26		1	
Male Total		**11**	**3**	**14**
Grand Total		**35**	**15**	**50**

Table 4.3.6 *Do you use the same password for multiple accounts*

Most of the respondents are using the same password for multiple accounts as Table 4.3.6 shows 35 over 50 of them voted for yes. This action may be convenient for the user, yet it poses a security risk as if one account is compromised, all your other accounts could also be at risk. In this analysis we noticed that respondents have less awareness about their password usage which using same password for multiple accounts.

Do you change passwords periodically?				
Gender	Age	Yes	No	Grand Total
Female	18 - 20	1	2	
	21 - 23	5	24	
	24 - 26		4	
Female Total		**6**	**30**	**36**
Male	21 - 23		13	
	24 - 26		1	
Male Total			**14**	**14**
Grand Total		**6**	**44**	**50**

Table 4.3.7 *Do you change passwords periodically*

Table 4.3.7 obviously shows that most of the respondents do not change their passwords periodically as the amount of 44 over 50 of them. Usually, people do not simply change password as they may forgot the latest password that they have set. Hence, this result showed is acceptable. Nevertheless, changing password periodically does really enhance our password security.

You don't mind sharing passwords with your friends.				
Gender	Age	TRUE	FALSE	Grand Total
Female	18 - 20	1	2	
	21 - 23	2	27	
	24 - 26	1	3	
Female Total		**4**	**32**	**36**
Male	21 - 23	2	11	
	24 - 26		1	
Male Total		**2**	**12**	**14**
Grand Total		**6**	**44**	**50**

Table 4.3.8 *You don't mind sharing passwords with your friends*

Data from Table 4.3.8 showed that 44 out of 50 respondents are minded sharing passwords with their friends. In this stage, we can see that most of them have awareness of their password privacy, which is good. For the reason that password belongs to our very private information as it can login to platforms of us, it should not being share with others than ourselves.

Do you use previously or used passwords whenever needed to create a password?				
Gender	Age	Yes	No	Grand Total
Female	18 - 20		3	
	21 - 23	25	4	
	24 - 26	3	1	
Female Total		**28**	**8**	**36**
Male	21 - 23	10	3	
	24 - 26		1	
Male Total		**10**	**4**	**14**
Grand Total		**38**	**12**	**50**

Table 4.3.9 *Do you use previously or used passwords whenever needed to create a password*

A total of 38 respondents uses their previous passwords whenever needed to create a password while the remaining 12 do not, data obtained from Table 4.3.9. It may be because their previous password is easier to remember. Additionally, people may believe that their previous password was strong and secure, so they feel comfortable using it again. However, reusing passwords can pose a security risk because if one password is compromised, then all accounts that use that same password can also be compromised. At this point, people are less aware about their password management.

Do you think two-step verification passcode should be compulsory whenever login?				
Gender	Age	Yes	No	Grand Total
Female	18 - 20	2	1	
	21 - 23	22	7	
	24 - 26	3	1	
Female Total		**27**	**9**	**36**
Male	21 - 23	11	2	
	24 - 26	1		
Male Total		**12**	**2**	**14**
Grand Total		**39**	**11**	**50**

Table 4.4.0 *Do you think two-step verification passcode should be compulsory whenever login*

From the data obtained from Table 4.4.0 there are (n=39; 78 percent) respondents that think two-step verification passcode should be compulsory whenever login. While the remaining (n=11; 22 percent) do not think so. This analysis depends on the person, two-step verification passcode is good for our password management but for those choosing not to have, they may be thinking that it takes time during login.

Trust

Are you aware that we could be scammed by SMS or emails?				
Gender	Age	Yes	No	Grand Total
Female	18 - 20	2	1	
	21 - 23	27	2	
	24 - 26	3	1	
Female Total		**32**	**4**	**36**
Male	21 - 23	11	2	
	24 - 26		1	
Male Total		**11**	**3**	**14**
Grand Total		**43**	**7**	**50**

Table 4.4.1 *Are you aware that we could be scammed by SMS or emails*

Table 4.4.1 showed 43 out of 50, most of the respondents were aware that they could be scammed by SMS or emails. At this point this question can be a reminder to respondents that

do not trust people easily as any receiving from strangers could lead to a scam. Fortunately, they have a sense of trust when dealing with outsiders.

Did you filled up any form with personal information that was given by a stranger?				
Gender	Age	Yes	No	Grand Total
Female	18 - 20		3	
	21 - 23	12	17	
	24 - 26		4	
Female Total		**12**	**24**	**36**
Male	21 - 23	5	8	
	24 - 26		1	
Male Total		**5**	**9**	**14**
Grand Total		**17**	**33**	**50**

Table 4.4.2 *Did you filled up any form with personal information that was given by a stranger*

Table 4.4.2 showed that 33 compared to 17 respondents do not fill up any form with personal information that was given by a stranger. Which means they are still concerned about their own privacy and do not simply trust any requests from others unknown person.

Awareness

Were you aware of any cyber scams before this?				
Gender	Age	Yes	No	Grand Total
Female	18 - 20	1	2	
	21 - 23	27	2	
	24 - 26	4		
Female Total		**32**	**4**	**36**
Male	21 - 23	11	2	
	24 - 26		1	
Male Total		**11**	**3**	**14**
Grand Total		**43**	**7**	**50**

Table 4.4.3 *Were you aware of any cyber scams before this*

Cyber scams are aware by most of the respondents as 43 out of 50 of them showed in Table 4.4.3 voted yes. The cyber scams type is not specifically mentioned in this question thus no matter what scams, they would also be careful of it. Which is great for them to having such an awareness about any cyber scams from their understanding.

Do you wish cybersecurity awareness as a course in your academic semester?				
Gender	Age	Yes	No	Grand Total
Female	18 - 20	1	2	
	21 - 23	26	3	
	24 - 26	3	1	
Female Total		**30**	**6**	**36**
Male	21 - 23	7	6	
	24 - 26		1	
Male Total		**7**	**7**	**14**
Grand Total		**37**	**13**	**50**

Table 4.4.4 *Do you wish cybersecurity awareness as a course in your academic semester*

Statistics from Table 4.4.4 show that (n=37; 74 percent) of the respondents wished cybersecurity awareness as a course in their academic semester. While there are also some of them who do not support this action with (n=13; 26 percent) respondents. Having such a course in the academic semester is good for a student while it can also be thinking it is very extra from their major subject in the semester.

CHAPTER V

DISCUSSION AND CONCLUSION

5.0 Introduction

In the last chapter, a series of outcomes have been produced from this research. The research's limitations and potential future intensifications highlighted along with the study's condensed results and discussion.

5.1 Results

This study aims to measure the awareness level of cyber scams and discover the cybersecurity awareness among university students in Malaysia. First and foremost, the main result of the study indicate that merchant fraud has the highest-level awareness among the others cyber scams. It contained of total of 23 respondents; 46 percent of them have an extremely aware about such scam. Which followed by romance scam with 42 percent, investment scam with 40 percent and phishing scam with 36 percent. As mentioned in literature review section before, usually a merchant fraud happens when there is an attraction of the web design, system availability and contact services. Consequences simply a transaction fraud, fake front store or even online shopping scamming to happen. Explaining by using the elements of cybersecurity in terms in this study, the 14 encountered respondents may have trust issue in their cybersecurity awareness. When we getting online transaction, personal information and banking information are essential during pre-purchase. With the lower trust awareness in their cybersecurity, they trusted the sellers, leading merchant fraud to the second highest number of students encountered the scam before. However, the number of students who encounter merchant fraud is lower than phishing scams. Therefore, they may have learned from experience. One of the independent variables, experiences have gave them a lesson on

merchant fraud. Oppositely, although the phishing scam having the highest number of students had been trapped into the scam before, it still resulted in the lowest level awareness among all with only 36 percent. This could mean that experiences still did not pay a lesson on them. Reason for that is because phishing scam is over random. Plenty of phishing types could be happen such as sending fraudulent documents link as an education purpose to the students. Hence, the encountered rate is higher with a number of 23 students. Illustrate using the awareness among cybersecurity, the trust issue also will be the main concern when explaining this result. There were 43 over 50 respondents that having aware of they could be scammed by SMS or emails. Nevertheless, students still getting lower awareness level for it. Therefore, this also indicates the need to strengthen in the phishing scam area among university students in Malaysia. After discussed each scam for highest level and lowest level awareness, left over romance scam and also the investment scam. Romance scam having 42 percent respondents having extreme aware of it. When talking about romance scam, it is about a scam between two person's relationship. Which trust and privacy will be the essential elements of the independent variables. Firstly, they going to accept a friend request from any stranger that requested, reveled their location on the social media and posting their personal information on it. Whenever the victim trusted the fraudster, who called for dating scammers. Usually, they willing to share their personal information such as name, age, home address or even bank number. Apart from that, even worse they could share the passwords to their 'lover'. This is linked to password management in cybersecurity awareness. Although from the results showing that most of the respondents have high privacy awareness and password management awareness, it can't be determined that they are not going to fall into any of the scams anymore. It depends on their perception of the moment as a romance scam involved emotions of love. Love is sometimes emotional and not rational (Segal, 2023). Lastly, investment scam having 40 percent of extreme awareness from the respondents. The result showing that still the same, trust will be the main

issue that a victim had fallen into the scam trap. The reason why is because a stock trader may need a sense of trust from the investors, which can be considered as the fraudster of investment scam need the certainty of victim on them. When the investors trusted their stock trader, they may have to submit their personal information such as name, age and bank number to them, in order to proceed with their investment package purchasing. At this moment, the victim has gradually fallen into the investment trap. Other than trust, password management could also important when facing this. If the victim was using the same password for multiple accounts, their bank could hack easily. For example, the stock trader could use the same password as their victim has set on their investment account, and try on their other accounts such as bank, e-wallet and social media sites as well. As showed from the result there were 35 over 50 respondents using the same password for their multiple accounts. Hence, this could have risk for them to encounter investment scam either.

For cybersecurity awareness, results show that respondents have quite a high awareness of each specific element including privacy, trust and awareness. Except for password management. In password management, respondents use the same password for multiple accounts, do not change password periodically and they use the previous password whenever needed. This can be concluded that password management becoming the most serious issue in cybersecurity awareness, and it should be improved among Malaysian university students, so that they could be aware of their password management, and any of the cyber scams could reduce as well.

5.2 Limitations

In this study, there is a data limitation. Since there is no restricted amount for each age group and gender group to fill up the questionnaire, it is not accurate to understand the awareness level for each specific age group. For instance, the mostly respondents belong to the

age group of 21 to 23 while the other two age groups were not much of them. Besides, the simple bias where the participants may not be representative of the general population. The researcher had only relied on self-reported data from individuals who are willing to participate in surveys or studies. With also the rapidly evolving threats. The field of cybersecurity is constantly evolving, with new threats emerging on a regular basis. This makes it challenging for the researcher to keep up with the latest trends and to design studies that accurately reflect the current cybersecurity landscape.

5.3 Recommendation

Further research should attempt more of independent variables on the cybersecurity awareness in more detail such as different types of interventions, as well as the factors that influence scams and cybersecurity awareness over time. Other than that, a qualitative study such as interviews or focus groups, could also provide insights into the motivations and attitudes of individuals who engage in risky online behaviours or fall for scams. These studies could identify the underlying factors that influence scams and cybersecurity awareness, such as cognitive biases or social pressures. As well as the patterns and trends in cybercrime, the characteristics of individuals who are most vulnerable to scams and cybersecurity threats. Which could understand the study in details.

5.4 Conclusion

Overall, in this research, there are scams and cybersecurity awareness among university students in Malaysia. However, do not consider higher or lower awareness in the midst of them as it depends on different level awareness for each different type of scam. The knowledge of cybersecurity should irrigate into the scope of universities so that students could be aware of

the issues and be defensive. This study benefits the target population, which Malaysian university students get to alert about the existence of these scams that are mentioned, including phishing scam, investment scam, romance scam and merchant fraud. Other than these few frauds, at least they have a concept that scam exists. Hopefully this study will raise the awareness of fraud issues among university students and reduce the number of scam cases that happen in Malaysia at the same time.

REFERENCES

Abdullah, M. Z., Othman, A. K., Wong, M. B., Anuar, A., & Mokthar, M. Z. (2022). Determinants of Consumer Loyalty toward Online Shopping Platforms among Malaysian Part-Time University Students. *Global Business & Management Research, 14*, 187–196.

Al-Mohannadi, H., Awan, I., Al Hamar, J., Al Hamar, Y., Shah, M., & Musa, A. (2018). Understanding Awareness of Cyber Security Threat among IT Employees. *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. https://doi.org/10.1109/w-ficloud.2018.00036

Alqahtani, M. A. (2022b). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences*, *12*(5), 2589. https://doi.org/10.3390/app12052589

Apps, S. C. (2023, February 21). *Cybersecurity awareness: Definition, Importance & More*. Spanning. Retrieved May 4, 2023, from https://spanning.com/blog/cybersecurity-awareness/

Apuke, O. D. (2017b). Quantitative Research Methods : A Synopsis Approach. *Kuwait Chapter of Arabian Journal of Business & Management Review*, *6*(11), 40–47. https://doi.org/10.12816/0040336

Badua, J. (2020). The Nature and Victimization of Investment Frauds. *PhD in Criminal Justice W/ Specialization in Criminology*. https://doi.org/10.13140/RG.2.2.11077.06888

Basyir, M., & Naz Harun, H. (2022, September 26). *Online scam cases increasing in Malaysia*. New Straits Times. https://www.nst.com.my/news/nation/2022/09/834531/online-scam-cases-increasing-malaysia

Chew, A. (2016). *Protecting Yourself From Investment Scams*. Feature. https://sidrec.com.my/wp-content/uploads/2020/01/Protecting-Yourself-From-Investment-Scams-Smart-Investor-Magazine.pdf

Clare Stouffer (2022, September 16). Retrieved from: https://us.norton.com/blog/emergingthreats/internet-scams

Claude Tambe Ebot, A., & Siponen, M. (2014). Towards a Rational Choice Process Theory of Internet Scamming: The Offender's Perspective. *International Conference on Information Systems 2014*. https://www.researchgate.net/publication/271527329

David, A. (2022, August 4). *RM5.2b in losses through online scams since 2020*. New Straits Times. https://www.nst.com.my/news/crime-courts/2022/08/819331/rm52b-losses-through-online-scams-2020

Dhruv. (2022, May 30). *Types Of Merchant Frauds And Ways To Tackle It*. PayU Blog. https://payu.in/blog/types-of-merchant-frauds-and-ways-to-tackle-it/

ELLIS. (2019, March 4). *25 Social Media Slang Terms You Need to Know*. WUO.com. https://www.makeuseof.com/tag/social-media-slang-terms/

Garba, A., Maheyzah Binti Sirat, Siti Hajar, & Ibrahim Bukar Dauda. (2020). Cyber Security Awareness Among University Students: A Case Study. *Science Proceedings Series*, *2*(1), 82–86. https://doi.org/10.31580/sps.v2i1.1320

Gurus, C. (2021, October 30). *Getting Familiar with Merchant Fraud*. https://www.chargebackgurus.com/blog/merchant-fraud

Hsieh-Yee, I. (2021). Can We Trust Social Media? *Internet Reference Services Quarterly*, *25*(1–2), 9–23. https://doi.org/10.1080/10875301.2021.1947433

Kamalulail, Abdul Razak, Aisyhah Omar, & Mohamed Yusof. (2022). Awareness of Cybersecurity: A Case Study in UiTM Negeri Sembilan Branch, Seremban Campus. *Academia Journal*, *11*(1). https://doi.org/10.24191/e-aj.v11i1.18266

Kancherla, J. (2017). Effects of Phishing Emails on College Students. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3794938

Key Elements of a Research Proposal Quantitative Design. (n.d.). Retrieved April 25, 2023, from https://www.wssu.edu/about/offices-and-departments/office-of-sponsored-programs/pre-award/_Files/documents/develop-quantitative.pdf

Kirwan, G. H., Fullwood, C., & Rooney, B. (2018). Risk Factors for Social Networking Site Scam Victimization Among Malaysian Students. *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 123–128. https://doi.org/10.1089/cyber.2016.0714

Kovačević, A., & Radenković, S. D. (2020). SAWIT—Security Awareness Improvement Tool in the Workplace. *Applied Sciences*, *10*(9), 3065. https://doi.org/10.3390/app10093065

Lokanan, M., & Liu, S. B. (2021). The demographic profile of victims of investment fraud: an update. *Journal of Financial Crime*, *28*(3), 647–658. https://doi.org/10.1108/jfc-09-2020-0191

Love, J. (2022, June 28). *Merchant Fraud: How Fake Businesses Hurt Real Merchants*. Chargebacks911. https://chargebacks911.com/merchant-fraud/

Malaysia Digital Marketing 2022 | Insight | AsiaPac - Digital Marketing Agency Asia. (2022, August 3). AsiaPac. https://www.asiapacdigital.com/digital-marketing-insight/malaysia-digital-marketing-2022

McKeever, G., Rossi, E., Hewitt, N., Rossi, E., Hewitt, N., Hasson, E., Hewitt, N., & Hasson, E. (2021, June 15). *What is Ransomware | Attack Types, Protection & Removal | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/ransomware/

McKeever, G., Rossi, E., Hewitt, N., Rossi, E., Hewitt, N., Hasson, E., Hewitt, N., & Hasson, E. (2020, June 17). *What is phishing | Attack techniques & scam examples | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/phishing-attack-scam/

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research*, *13*(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81

Privacy on Social Media | This is How You Protect Your Socials. (n.d.). VPNoverview.com. https://vpnoverview.com/privacy/social-media/

Ramakrishnan, K., Yasin, N. M., & Periasamy, J. (2022). Digital divide on cybersecurity awareness among the Malaysian higher learning institution students. In *Nucleation and Atmospheric Aerosols*. American Institute of Physics. https://doi.org/10.1063/5.0092796

Ruby, D. (2023, March 20). *Internet User Statistics In 2023 — (Global Data & Demographics)*. Demand Sage. https://www.demandsage.com/internet-user-statistics/#:~:text=Internet%20User%20Demographics&text=In%20the%20year%202021%2C%2099,of%2018%20to%2029%20years.

Saizan, & Singh. (2018). Cyber Security Awareness among Social Media Users: Case Study in German-Malaysian Institute (GMI). *Asia-Pacific Journal of Information Technology &Amp; Multimedia*, *07*(02(02)), 111–127. https://doi.org/10.17576/apjitm-2018-0702(02)-10

Security, P. (2020, October 13). *10 Social Media Scams and How to Spot Them*. Panda Security Mediacenter. https://www.pandasecurity.com/en/mediacenter/panda-security/social-media-scams/

Segal, J. (2023, February 27). *Your trusted guide to mental health & wellness*. HelpGuide.org. Retrieved May 4, 2023, from https://www.helpguide.org/articles/mental-health/emotiohttps://www.helpguide.org/articles/mental-health/emotional-intelligence-love-relationships.htmnal-intelligence-love-relationships.htm

Shaari, A. H., Kamaluddin, M. R., Paizi@Fauzi, W. F., & Mohd, M. (2019). Online-Dating Romance Scam in Malaysia: An Analysis of Online Conversations between Scammers and Victims. *GEMA Online® Journal of Language Studies*, *19*(1), 97–115. https://doi.org/10.17576/gema-2019-1901-06

Sharma, P. & ph social media. (2022, July 18). *Social media has changed the lives of modern society*. Summit News. https://summitpsnews.org/2020/03/24/social-media-has-changed-the-lives-of-modern-society/

Smith, S. (2021, July 29). *15 Reasons to Be in a Relationship*. Marriage Advice - Expert Marriage Tips & Advice. https://www.marriage.com/advice/relationship/reasons-to-be-in-a-relationship/

Tang, J., & Liu, H. (2015). Trust in Social Media. *Synthesis Lectures on Information Security, Privacy, and Trust*, *10*(1), 1–129. https://doi.org/10.2200/s00657ed1v01y201507spt013

The ASEAN Post. (2020, May 15). *Love Under Lockdown*. https://theaseanpost.com/article/love-under-lockdown

The Money Game Experience. (n.d.). https://www.greaterthan.works/moneygame

Tirumala, S. S., Valluri, M. R., & Babu, G. A. (2019). A survey on cybersecurity awareness concerns, practices and conceptual measures. *2019 International Conference on Computer Communication and Informatics (ICCCI)*. https://doi.org/10.1109/iccci.2019.8821951

Appendix A

Survey Questionnaire

Awareness of Cyber Scams and Cybersecurity among University Students in Malaysia.

Dear respondents,

I am Bong Xu Lin, a Y3S3 student studying Bachelor of Communication (HONS) Broadcasting from University Tunku Abdul Rahman (UTAR), Sungai Long Campus. I am currently working on my Final Year Project (FYP), entitled "Awareness of Cyber Scams and Cybersecurity among University Students in Malaysia". I would like to invite you to participate in this research study and help me to complete this simple questionnaire.

This questionnaire consists of **THREE** sections:

Section A: Demographic profile (4 questions)

Section B: Level of Awareness (8 questions)

Section C: Cybersecurity Awareness (14 questions)

Please answer **ALL** the questions listed in this questionnaire.

Objective:

To identify the awareness level of cyber scams and cybersecurity among Malaysian university students.

Estimated time for completing this questionnaire: *5 - 10 minutes*

Please note that the **CONFIDENTIALITY** of your responses is meticulously assured. The data collected will only be used for educational and research purposes only. If you have any inquiries or doubt, please do not hesitate to contact me through
email: xulinbong828@1utar.my (Bong Xu Lin).

Greatly value your co-operation. Thank you for your time and consideration.

Section A: Demographic Profile

1. Gender
    - Male
    - Female

2. Age
    - 18 - 20
    - 21 - 23
    - 24 - 26

3. Ethnicity
    - Chinese
    - Malay
    - Indian
    - Other (please specify)

4. Education
    - Foundation
    - Bachelor’s degree
    - Master’s degree
    - Doctorate
    - Other (please specify)

Section B: Level of Awareness

This section proceeding to study your level of awareness for different types of scamming. Rate the awareness level of each scam with your acknowledgement, from:

1 - Not aware of at all
2 - Slightly aware of
3 - Somewhat aware of
4 - Moderately aware of
5 - Extremely aware of

a) **Phishing Scam**

Examples: Fake Email, False URL.

- 1
- 2
- 3
- 4
- 5

ai) Have you encountered phishing scam before?

- Yes
- No

b) **Investment Scam**

Examples: Money Game, Real Estate, Cryptocurrency, Investment Packages.

- 1
- 2
- 3
- 4
- 5

bi) Have you encountered investment scam before?

- Yes
- No

c) **Romance Scam**

Example: Online Dating, Request for Money, Nude Photo Scam.

- 1
- 2
- 3
- 4
- 5

ci) Have you encountered romance scam before?

- Yes
- No

d) **Merchant Fraud**

Examples: Online Shopping Scam, Fake Storefronts, Transaction Fraud.

- 1
- 2
- 3
- 4
- 5

di) Have you encountered merchant fraud before?

- Yes
- No

Section C: Cybersecurity Awareness
This section is use to understand the behaviour of the respondents while using social media sites and to discover how aware they are for cybersecurity.

Privacy

1. What is the privacy setting of your social media accounts?
   - Public
   - Private

2. Do you accept friend request from strangers?
   - Yes
   - No

3. Do you reveal your location on your social media?
   - Yes
   - No

4. It is not a problem to post your basic personal information on social media.
(Example: full name, date of birth, contact details)
   - True
   - False

5. Are you aware of posting private photography such as selfie could lead to scamming?
   - Yes
   - No

Password Management

1. Do you use the same password for multiple accounts?
   - Yes
   - No

2. Do you change passwords periodically?
   - Yes
   - No

3. You don’t mind sharing passwords with my friends.
   - True
   - False

4. Do you use previously or used passwords whenever needed to create a password?
   - Yes
   - No

5. Do you think two-step verification passcode should be compulsory whenever login?
(Enter a code that will send you via text or voice message upon signing in.)
   - Yes
   - No

Trust

1. Are you aware that we could be scammed by SMS or emails?
   - Yes
   - No

2. Did you filled up any form with personal information that was given by a stranger?
   - Yes
   - No

Awareness

1. Were you aware of any cyber scams before this?
   - Yes
   - No

2. Do you wish cybersecurity awareness as a course in your academic semester?
   - Yes
   - No

Thank you for your participation.

Faculty of Creative Industries

Research Project Evaluation Form

Supervisor / Reviewer: Beh Chun Chee

Student's Name : Bong Xu Lin

Student ID : 19UJB01979

Programmme : BACHELOR OF COMMUNICATION (HONS) BROADCASTING

Research Project Title: A Study of Awareness of Cyber Scams and Cybersecurity Among University Students In Malaysia

Instruction:
Please score each descriptor based on the scale provided below:
(1 = very poor, 2 = poor, 3 = average, 4 = good and 5 = very good)

Abstract (5%)	**Score**	**Convert**
1. Adequately describes the entire project		
2. States clearly the research problem		
3. Describe briefly and clearly the approach/methodology of the study		
4. Highlights the outcomes/significance of the study		
Sum		
Subtotal (sum / 4)		
Remark:		

Introduction (10%)	**Score**	**Convert**
1. Fitting introduction to the subject of the study		
2. Concepts/definitions well explained		
3. Scope of study well described		
4. Statement of the research problem/research questions		
Sum		
Subtotal (sum / 2)		
Remark:		

Literature Review (15%)	**Score**	**Convert**
1. Latest research/work done in the area of study		
2. Explication of theories used		
3. Constructive discussion on publications in relation to the topic of study		
Sum		
Subtotal (sum *1)		
Remark:		

Methodology (10%)	**Score**	**Convert**
1. Research method explained clearly(inclusive of clear explanation of sampling techniques used, where applicable only)		
2. Appropriate research design/framework/questionnaire		
Sum		
Subtotal (sum * 1)		
Remark:		

Findings & Analysis (20%)	**Score**	**Convert**
1. Data analysis is appropriate		
2. Data analysis is detailed		
3. Pertinent use of diagrams/tables/graphs, correlated with content/Analysis supported by evidence		
4. Clear interpretation, well explained		
Sum		
	Subtotal (sum * 1)	
Remark:		
Discussion & Conclusion (15%)	**Score**	**Convert**
1. Appropriate; related to the objective of the study		
2. Shortcomings of the study & recommendations for future study		
3. Conclusion is apt, clear		
Sum		
	Subtotal (sum * 1)	
Remark:		
Language & Organization (15%)	**Score**	**Convert**
1. Correct use of English and technical language		
2. APA format is followed		
3. Comprehensiveness of content and presentation		
Sum		
	Subtotal (sum * 1)	
Remark:		

Presentation (10%)	**Score**	**Convert**
1. Ability to answer questions from the panel (4 Marks)		
2. Presentation delivery is clear (4 Marks)		
3. Body language (2 Marks)		
Subtotal (sum * 1)		
Remark:		
	TOTAL	**100%**
Penalty: maximum 10 marks for late submission or poor attendance for consultation with supervisor		
	FINAL MARK	**100%**

****Overall Comments:**

Signature: _____ Date:_____

FYP Evaluation Form
(Literature-based projects)

Supervisor: Mr Beh Chun Chee

Name : Bong Xu Lin

Student ID : 19UJB01979

Program : BACHELOR OF COMMUNICATION (HONS) BROADCASTING

ProjectTitle: A Study of Awareness of Cyber Scams and Cybersecurity Among University Students In Malaysia

Abstract I. Adequately describe the entire thesis II. State clearly the research problem III. Describe briefly the approach to the research/ work/study IV. Highlight the outcome/significance of the study (impart sufficient depth in argument/discussion)	5 marks	
Context/Background I. Background of author and text II. Information about genre and/or historical time period of the text III. Information about theory/theories used to analyze the text e.g. feminist/Marxist/etc. if any IV. Awareness of academic debates/discussions of text or theories used	15 marks	
Close Reading/Analysis I. Original close reading that extends and expands our understanding of the text II. Analysis that is precise and well-supported by textual evidence III. Adheres to objectives of the project	30 marks	
Relationship of issues/themes to the entire text I. Relating close reading analysis to the text as a whole	10 marks	

II. Looking at broader issues/themes in the text and their significance		
Relationship of text to other works by the same author (if any) or in the same genre I. Able to relate text to other works or similar themes/issues explored by same author II. Able to relate text to works in the same genre	10 marks	
Organization I. Ideas well organized and flow smoothly II. Ideas in each chapter are coherent and self-contained. III. Relationship of chapter analysis to the thesis as a whole is well-elaborated and logical	10 marks	
Language I. Correct use of grammar and punctuation II. Correct use of technical language	15 marks	
Presentation of Project I. References/appendices correctly cited II. Thesis handed in on time and complete	5 marks	

TOTAL **100 MARKS** _____

Comments:

_____

_____

_____

_____

Signature: _____ **Date: _____**

Checklist

Whole the project	**Done**
1 Font size = 12 points	[ ]
2 Font type = Times New Roman	[ ]
3 No bold	[ ]

4	Italic for statistical symbols	[ ]
5	Margins = the left, top and bottom margins should be 1 inch.	[ ]
6	Spacing = double-spaced	[ ]
7	A4 paper	[ ]
8	No justification for APA; Justification for M LA ETC.	[ ]
9	Number of words = 6,500 to 10,000words (exclude reference and appendices)	[ ]

Abstract

1	Not more than 200 words	[ ]
2	No tab and in one paragraph	[ ]
3	Include the following information	[ ]

a. Statement of the problem,
b. A concise description of participants, the research method and design
c. Summary of major findings
d. Conclusions and suggestion

Level of writing

1	Level one (title of each section) = CENTERED in uppercase	[ ]
2	Level two = flush left, italicized, Title case	[ ]
3	Level three = indented, italicized, sentence case, ending with a period	[ ]

Appendix

	Appendix materials should be grouped by type, e.g. Appendix A:	
1	Questionnaire; Appendix B: Original Data; Appendix C: Result	[ ]
2	Every appendix group starts from a new page	[ ]

Table

1	Tables are numbered consecutively (with Arabic numerals) throughout the research paper (including text and appendices), such as Table 1, Table 2	[ ]
2	Format:	
	a. Type the word Table and its Arabic numeral	[ ]
	b. Flush left at the **top** of the table.	[ ]
	c. Double-space	[ ]
	d. Begin the table title flush left,	[ ]
	e. Sentence case	[ ]
	f. Italicizing the title.	[ ]
	g. Insert into text,	[ ]
	h. Not more than 1 table in a page	[ ]

Figure

1	Figures are numbered consecutively (with Arabic numerals)	[ ]

throughout the research paper (including text and appendices), such as Figure 1, Figure 2…

2 Format:
- a. Type the word Figure and its Arabic numeral [ ]
- b. Flush left at the **bottom** of the Figure. [ ]
- c. Follow by the Figure caption flush left, [ ]
- d. Sentence case [ ]
- e. Italicizing the caption. [ ]
- f. Insert into text, [ ]
- g. Not more than 1 figure in a page [ ]

Page header

1 First two or three words from the title [ ]
2 Upper right-hand corner [ ]
3 Sentence case [ ]
4 12 points times new roman [ ]
5 After page header, leave 2-5 spaces, follow by page number [ ]
6 Start from introduction to the last page of appendices [ ]

Pagination

1 Blank leaf, title page, acknowledgement and approval sheet = No pagination [ ]
2 Abstract, declaration, table of contents, list of tables, list of graphs, list of plates and list of abbreviations = To be paginated as i, ii, iii… [ ]
3 Introduction, Literature Review, Methodology, Findings & Analysis, Discussion & Conclusion, References and Appendices = To be paginated as 1, 2, 3 [ ]

Table of content

1 Blank leaf, title page, acknowledgement and approval sheet = not be listed [ ]

Research spine

1 12-point, Times New Roman [ ]
2 Lettered in gold [ ]
3 Include the followings: [ ]
- a. Project/Research title (abridged version);
- b. Faculty and
- c. Year of submission

Project cover

1 12- point, Times New Roman [ ]
2 Lettered in gold [ ]
3 ALL in UPPER CASE [ ]
4 Include the followings: [ ]
- a. University logo

b. Title of thesis
c. Name of candidate;
d. Degree;
e. Faculty
f. Name of university
g. Month and year of submission.

Submission

1	Two bound copies of research project to supervisor	[ ]
2	A soft-copy in the form of a compact disc to supervisor	[ ]
3	Signed the declaration	[ ]
4	Signed the approval sheet by supervisor	[ ]