THE CYBER SECURITY AWARENESS OF ISLAMIC DIGITAL BANKING AMONG UMK CITY CAMPUS STUDENTS

AMIRAH FADHLINA BINTI AZAHAR

NUR HIDAYAH BINTI MOHD ZAKI

NURUL AFIQAH BINTI MAZENEE

NURULAIN AQILAH BINTI HALIZAN

DEGREE OF BUSINESS ADMISTRATION (ISLAMIC BANKING AND FINANCE) WITH HONOURS

2024

The Cyber Security Awareness Of Islamic Digital Banking Among UMK City Campus Students

by

Amirah Fadhlina Binti Azahar

Nurul Hidayah Binti Mohd Zaki

Nurul Afiqah Binti Mazenee

Nurulain Aqilah Binti Halizan

A thesis submitted in fulfillment of the requirements for the degree of Business Administration (Islamic Banking and Finance) with Honours

Faculty of Entrepreneurship and Business
UNIVERSITI MALAYSIA KELANTAN

2024

THESIS DECLARATION

I hereby certify that the work embodied in this thesis is the result of the original research and has not been submitted for a higher degree to any other University or Institution.

☑	**OPEN ACCESS**	I agree that my thesis is to be made immediately available as hardcopy or on-line open access (full text).
☐	**EMBARGOES**	I agree that my thesis is to be made available as hardcopy or on-line (full text) for a period approved by the Post Graduate Committee. Dated from _____ until _____.
☐	**CONFIDENTIAL**	(Contain confidential information under the Official Secret Act 1972)*
☐	**RESTRICTED**	(Contains restricted information as specified by the organization where research was done)*

I acknowledge that Universiti Malaysia Kelantan reserves the right as follows:

1. The thesis is the property of Universiti Malaysia Kelantan.
2. The library of Universiti Malaysia Kelantan has the right to make copies for the purpose of research only.
3. The library has the right to make copies of the thesis for academic exchange.

NAME: Amirah Fadhlina Binti Azahar

NAME: DR Ahmad Ridhuwan Abdullah
Date: 12 January 2024

NAME: Nurul Hidayah Binti Mohd Zaki

NAME: Nurul Afiqah Binti Mazenee

NAME: Nurulain Aqilah Binti Halizan

Date: 12 JANUARY 2024

ACKNOWLEDGEMENT

First and foremost, thanksgiving to God, the Almighty, for showered us with blessings while we worked on completing this research.

We'd want to congratulate and thank ourselves and our team members for fully committing to this study. From daylight till night, we worked hard to discuss and complete this study. We were afraid to make contact from the beginning until it was easy to share, what we sought could not be saved, and the cries of the hustle, the deadlock of ideas, being unwell, and so on became bittersweet memories for us.

We want to express our deepest appreciation to our advisor, Dr Ahmad Ridhuwan bin Abdullah, for his help and guidance throughout the creation of the research proposal. His advice on how to look for related research articles with our study's title was quite useful. We are grateful to have him as our supervisor since his passion allowed us to perform well while being less under pressure. Furthermore, he carefully explained certain parts that we were unable to understand.

We would not have been able to complete this study project without the help of our parents, family, and friends. They are the most supportive people we have ever had. Thank you to them for always understanding and giving us time to complete this project. Thank you for sharing the ideas and desires. Thank you for caring for us from the time we didn't know anything until the time we became determined to learn more. Thank you, siblings, for making our day less serious. We sincerely thank you.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

2FA	Two-factor authentication
ATM	Automated Teller Machines
DV	Dependent Variable
FHPK	Faculty of Hospitality, Tourism and Wellness
FSA	Financial Service Act
FSDK	Faculty of Data Science and Computing
IS	Information System
IT	Information Technology
IV	Independent Variable
MCO	Movement Control Order
MIT	Massachusetts Institute of Technology
MOF	Ministry of Finance
NSC	National Security Council
SAA	Bachelor of Accounting with Honours
SAB	Bachelor of Business Administration (Islamic Banking and Finance)
SAE	Bachelor of Entrepreneurship with Honours
SAH	Bachelor of Entrepreneurship (Welfare) with Honours
SAK	Bachelor of Entrepreneurship (Commerce) with Honours
SAL	Bachelor of Entrepreneurship (Logistics and Distributive Trade)
SAP	Bachelor of Entrepreneurship (Tourism) with Honours
SAR	Bachelor of Entrepreneurship (Retailing) with Honours
SAS	Bachelor of Information Technology with Honors
SD	Standard Deviation
SPSS	Statistical Package for Social Science

SST	Bachelor of Information Technology with Honors
TRA	Theory of Reasoned Action
UMK	University Malaysia Kelantan
UPU	University Portal Union

LIST OF SYMBOLS

-	Hyphen
%	Percentage
&	Ampersand
( )	Parentheses
,	Comma
:	Colon
;	Semicolon
?	Question Mark
“”	Quotation Mark
=	Equal
H1	Hypothesis one
H2	Hypothesis two
H3	Hypothesis three
H4	Hypothesis four
N	Population
a	Alpha Value
p	Probability Value
r	Responses

ABSTRACT

This study investigates cyber security awareness among students at the UMK city campus, focusing on Islamic digital banking. It uses the Theory of Reasoned Action (TRA) as a theoretical framework and collects 371 questionnaires. Statistical analyses, validity and reliability tests, regression analysis, and the Pearson correlation coefficient are used to test hypotheses and explore relationships between variables. For the research design, the researchers used a quantitative method to understand the factors influencing cyber security awareness. Findings from the study reveal a strong relationship between cyber security awareness and knowledge of technology, social media information, internet user experiences and internet user attitude. However, the research emphasizes the importance of cyber security awareness in the Islamic digital banking sector, highlighting its relevance in the context of the Theory of Reasoned Action (TRA). This study contributes to the existing literature on cyber security in digital financial services. The study emphasizes the significance of cyber security awareness in the Islamic digital banking sector for promoting financial inclusion, efficiency, and economic growth. It suggests that evolving cyber security awareness is crucial for the sector's continued growth and resilience.

Keywords*: Awareness, Cyber Security, Islamic, UMK, TRA*

CHAPTER 1 INTRODUCTION

1.1 Background of The Study

Since the beginning of the year 2000, we have been living in the era of globalisation 3.0, in which the Internet is used for almost every aspect of life. The internet makes it easier for people all over the world to communicate with one another and gain access to information by connecting them to a wide variety of networks, including both public and private networks, commercial networks, educational networks, and government networks. Based on Demand Sage in 2023, Internet users come from all ages. In 2021, nearly all persons aged 18 to 29 were connected to the web. Then, according to Statista, there were expected 5.3 billion internet users in the world in 2022, compared to 4.9 billion the year before. This proportion comprises roughly 66% of the entire population of humans.

People are able to learn anything they want to know through the Internet because of the existence of search engine such as Google and Yahoo and video-sharing websites likes YouTube. However, according to Rahman et al. (2020), the expanding realm of the Internet may also provide problems for individuals who make use of the internet, such as an increased risk of fraud, malicious codes, intrusion and many more types of cyber-attacks. Therefore, we need to address these issues as soon as possible so that they do not have a significant impact. Because of this situation, it is crucial that individuals who use the internet take measures to secure their personal information.

The process of ensure the safety of information and information systems,such as networks, computers, databases, data centres, and applications, by implementing appropriate policies and making use of the appropriate technology is known as cyber security (Tonge, 2013). In accordance to Shea et al. (2023), people and businesses use two-factor

authentication (2FA) to keep unauthorised people from getting into data centres and other electronic systems. A strong cyber security plan can give an organisation or user a good defense against attacks that try to access, change, delete, harm or extort private data from their systems. Another significant aspect of cyber security is to avoid cyber-attacks that seek to destroy or interrupt the operation of a system or device.

At the tail end of the first decade, the concept of cyber security made its appearance, which marked the beginning of the rise in favour of a new language. It had been utilised in previous years, but its popularity skyrocketed after President Barack Obama issued the following proclamation in 2009: "I call upon the people of the United States to recognise the importance of cybersecurity andto observe this month with appropriate activities, events, and trainings to strengthen national security and resilience" (Schatz et al., 2017). As in Malaysia, the director-general of the National Security Council (NSC), Datuk Rodzi Md Saad, was quoting in the New Straits Times as of September 2022 by saying, “Since the cyber security issue is currently the primary concern in the country, people and every organisation must be aware of the need to defend our nation from cyber-attacks and criminals and work together to create a safe online space”. Based on both proclamations, it is proven that the education about cyber security is essential since hacking can occur at any location, to anyone, and at any type of organisation or establishment.

Next, BERNAMA stated that Bank Negara Malaysia (BNM) made an announcement on 29th April 2022 regarding the approval of the Malaysian Ministry of Finance (MoF) to the consortiums that have applied for and been granted permission to operate as digital banks in the country. It has been separatedinto two groups: those licensed under the Financial Services Act 2013 (FSA), which has three licensees; and those licensed under the Islamic Financial ServicesAct 2013, which has two licensees. According to Vulcan in May 2022,

there are three of the five consortium that are primarily held by Malaysians which are; Boost Holdings and RHB Bank Berhad, Sea Limited and YTL Digital Capital, and KAF Investment Bank. This shown that Islamic banks have the effort to digitilise their banking system.

The use of Islamic bank is continuing its rapid expansion in a variety of new nations with populations that are generally younger. These clients previously desired very efficient and effective digital banking services, but now they anticipate that this will be the primary method through which they can obtain services (Bello et al., 2017). An online process that extends beyond traditional internet banking is referred to as a digital bank. Customers of banks are granted the ability to make use of online and electronic platforms in order to acquire banking goods and make use of banking services (Haralayya, 2021). Digital banking should be able to perform the same functions as a primary office, a branch office, an internet service, bank cards, and automated teller machines (ATMs). In addition, according to Bello et al. (2017), there are certain concerns regarding the level of service that may be expected from banks who offer digital banking. Concerns have been voiced regarding security, the user- friendliness of the platform, the reliability of the information it provides, and the cost of services.

1.2 Problem Statement

Due to the advancements in technology, Islamic digital banking is able to provide their customers with better service and a better overall value (Chauhan et al., 2022). This is in contrast to traditional banking institutions. As a result of this, Islamic digital banks are posing a threat to the business models of conventional banks by providing customers with more innovative and personalised service options (Agarwal & Chua, 2020). According to

the findings of Pio et al. (2023), digital banks offer a variety of advantages, some of which include increased transparency, decreased operational costs, and simplified access to information.

The digital banking or called as online transactions, have become increasingly popular in Malaysian organisations since they are more convenience and more secure than traditional transactions involving physical cash (Singh et al.,2020). However, there is a significant challenge faced by banking's sector, which is the increasing number of information technology applications utilised for digital banking. According to Hussain et al. (2017), this leads to danger to the customers' e-security, cyber-attacks on customers' profiles, account hijacking, data message fraud, stealing customers' privacy, and obtaining details about their financial activities without the customers' awareness.

Source: Statista Research Department

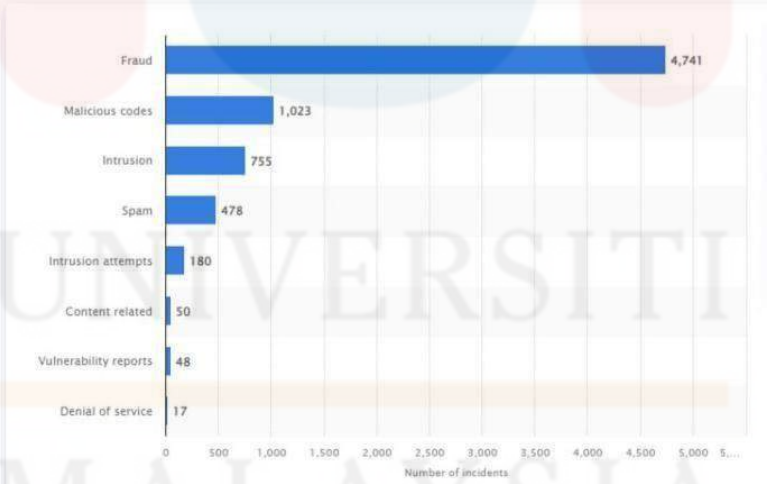

Figure 1.1: Number of cyber threat incidents in Malaysia 2022

Based on the figure 1.1, it shows that with more than 4,000 reports, Cyber security Malaysia said that online frauds were the biggest cyber danger in 2022. Malicious codes came in second, followed by intrusion, spam, intrusion attempts, content related,

vulnerability reports and a denial of service. Due to the huge number of cyber threats in Malaysia, Minister of Communications and Digital Deputy, Teo Nie Ching recently claimed in the statement in the New StraitTimes on 17th March 2023 that the Unity Government has recognised the critical importance of cyber security and cybercrime. In addition, Unity Government is also looking to implement many initiatives to protect its citizens and the nation's security. As of the end of February in 2023, there have been recorded 456 instances of fraudulent activity. Therefore, according to Teo Nie Ching, this commitment was shown in the allocation of RM10 million from the 2023 budget to the National Scam Response Centre (NSRC), which will be used to upgrade equipment as well as begin a campaign to raise awareness and promote the NSRC's 997 hotlines.

In order to mitigate the threats posed to information technology's security,internet users' education and awareness are required (Aloul, 2012). People shouldn't only accept the information, but should also put it to use in relevant and useful ways. This is because when people are not aware of cyber security, they may face the consequence like losing everything of value such as safety, peace, money, and land. Then, as for public and private institutions, in the event that they are unaware about cyber security, they will be having a major significant repercussion for the financial condition of the companies (Das & Nayak, 2013). Hence, in point of fact, the purpose of this research is to determine the level of awareness that individuals have regarding cyber security and the factors that influencing it when they utilise Islamic digital banking, particularly among UMK city campus students. Therefore, we can determine what can be done to make students more aware of the cyber security risks associated with digital banking.

1.3 Research Questions

In order to accomplish the goals of this study, it is necessary to find answers to these five different research questions. These are the research questions that will be investigated in this study:

1. Does knowledge of technology influence the level of cyber security awareness of the Islamic digital banking among UMK city campus students?
2. Does social media information influence the level of cyber security awareness of the Islamic digital banking among UMK city campus students?
3. Does internet users' experience influence the level of cyber security awareness of the Islamic digital banking among UMK city campus students?
4. Does internet users' attitude influence the level of cyber security awareness of the Islamic digital banking among UMK city campus students?
5. Do UMK city campus students aware about the cyber security of the Islamic digital banking?

1.4 Research Objectives

The objectives of this research are to determine the factors that have an influence on the level of awareness of the Islamic digital banking system among students at the UMK city campus and to present our findings. The objectives are as below:

1. To examine the relationship between the knowledge of technology and thelevel of cyber security awareness of the Islamic digital banking among UMK city campus students.
2. To analyse the relationship between the social media information and the level of cyber security awareness of the Islamic digital banking among UMK city campus students.

3. To examine the relationship between the internet users' experience and the level of cyber security awareness of the Islamic digital banking among UMK city campus students.
4. To discuss the relationship between the internet users' attitude and the level of cyber security awareness of the Islamic digital banking among UMK city campus students.
5. To determine the level of cyber security awareness of the Islamic digital banking among UMK city campus students.

1.5 Scope of The Study

The respondents, who will take part in this research are going to be students at University Malaysia Kelantan from Pengkalan Chepa (city campus). This is because UMK is one of the IPTA in Malaysia according to Info UPU (2020). There is no previous study done on the level of cyber security awareness of the Islamic digital banking among UMK students. Therefore, this study chooses the UMK city campus students. Students were chosen as respondents for this study because youngsters like students, frequently use digital payment methods (Abdul Rais et al., 2022). This is because they seek to benefit from the opportunities presented by new and improved payment technology. The primary objective of this research is to find out whether or not students at the UMK city campus are aware of the cyber security on Islamic digital banking based on their knowledge of technology, social media's information, experience as well as attitude.

1.6 Significance of Study

The study will assist the researchers in determining why students of UMK city campus have such a keen awareness of the cyber security risks in Islamic digital banking. This study can provide researchers with a clearer understanding of what they need to look into next in order to determine the factors that influence the level of cyber security awareness among students at UMK. The benefit that students at the UMK city campus are expected to gain from this study is the importance of cyber security in Islamic digital banking. Some individuals may not fully comprehend the importance of safety when using Islamic digital banking.

Next, this study will be very beneficial to the Islamic banks that offer digital banking, so that they can maintain the customer and employee trust. Customers and staff alike have assurance that any information they share will be safe from outsiders on the internet. Banks need to aware more about cyber security to secure the data of their customers and employees in order to maintain their trust against the bank.

In addition, internet users will receive the significant benefit from this study because if users are aware of cyber security, they will be less likely to trust those who try to defraud them. For instance, if they receive calls from someone who is pretending as a banker, they already know how to deal with them. This means that they are able to identify either the callers are fraudsters or bankers. Therefore, they are also able to safeguard their belongings, such as their money and other assets, from being taken by fraudsters.

Last but not least, this research will benefit the government by increasing awareness about cyber security among employees. Governments hold sensitive population information, which must be kept confidential. Therefore, regular system checks will ensure the safekeeping of sensitive information, indicating a higher level of caution in protecting citizens' personal information. This will help maintain a safer environment for sensitive data.

1.7 Definition of Terms

The terms are defined as they are shown in the table that follows:

Table 1.1: The definition of terms

TERM	DEFINITION
Cyber security	Cyber security is the process of keeping information and information systems like networks, computers, databases, data centres, and apps which are safe by using the right procedures, particularly when using Islamic digital banking (Tonge, 2013).
Awareness	Awareness refers to the state of being informed about, alert to, and otherwise in sync with external stimuli. It also refers to the condition in which a subject has access to information that can be used to guide a variety of behaviours such as avoiding cyber threats through cyber security (Wikimedia Foundation, 2023).
Islamic digital banking	A bank that exists solely online, without any physical offices. Their services can only be obtained digitally, and mostly through an app (IFG Staff Writers, 2022). Therefore, this is the reason why cyber security is really needed for Islamic digital banks.
University Malaysia Kelantan (UMK) city campus students	The students who are studying at University Malaysia Kelantan (UMK) city campus by pursuing a bachelor's degree, master's degree, or PhD.

1.8 Organization of The Proposal

The aim of this study is to find out how many students at the UMK city campus know about cyber security of the Islamic digital banking. This proposal's introduction to the study has already been discussed in chapter 1. It gives an overview of the study's background, the problem statement, research questions, and objectives of research, the study's scope, and the significance of research, the definition of terms and the organisation of the proposal. Then, it follows by Chapter 2 which pinned the literature review like introduction, underpinning theory, previous studies, hypothesis statements, conceptual framework, and a summary of the factors influencing the level of cyber security awareness among students. Lastly chapter 3 looks at the research methods in the introduction, research design, data collection methods, study population, sample size, sampling techniques, research instrument development, measuring variables, the procedure for analysing the data, and a summary.

CHAPTER 2 LITERATURE REVIEW

2.1 Introduction

The study will explain the dependent variable (DV) and independent variable (IV) in this chapter. A literature review's goal is to assist readers comprehend current studies on a topic or issue, and to share that knowledge in the form of a written report. A literature review can help researchers gain a greater understanding of the topic by providing a more or less systematic strategy to gathering and synthesizing previous research (Baumeister & Leary, 1997). This chapter will cover underpinning theory, previous study, conceptual framework, hypothesis, and conclusion.

For this topic, an Islamic digital bank is a financial institution that operates according to Sharia rules (Aisyah, 2018). An Islamic digital bank does not engage in any of the prohibited activities that other banks do. Digital banking uses technology to assure the best utility for both the customer and the bank in terms of accessibility, usefulness, and affordability (Epstein 2017). For example, dealing with interest or investing their money in illegal activities such as gambling. Besides, Islamic digital banking is evolving to meet Muslim expectations. However, Islamic banks are sometimes also referred to as conventional banks due to their full-service financial intermediaries (Raza et al., 2019). According to Ababa (2018), to gain a better understanding of the use of technology in service innovation, particularly in digital banking, it is crucial to consider the service users and their perception of the service. Overall, Muslims believe Islamic banks support economic growth and contribute significantly to Muslim society's well-being (Raza et al. 2019). With that, a review of studies on the usage of Islamic Digital Banking will be discussed.

2.2 Cyber Security

Cyber security is described as a computer-based discipline that protects operations against unauthorised access or threat. It includes technology, people, information, and procedures. The aim is to reduce the vulnerability to cyber-attacks and safeguard systems, networks, and technology from unauthorized use. Cyber security refers to all approaches that aim to protect data, systems, and networks from intentional and unintentional attacks, but, if necessary, from the lack of preparation for the recovery of this infrastructure (MIT, 2011). Nowadays, cyber security has become the latest issue (Dervojeda et al., 2014). Cyber security extends beyond data authentication in the IT industry to encompass various other websites and online platforms, including cyberspace and similar domains. Furthermore, improving cyber security and maintaining proper information systems are critical to any country's financial safety and growth. Meeting cybercrime requires widespread and safer practices (Gross, Canetti & Vashdi, 2016). Cyber security is about the insecurity caused by and through this new environment, as well as strategies or procedures that slowly protect it (Kumar & Somani, 2018). Therefore, improving cyber security and protecting sensitive data and infrastructure is important for every country's security priority (Panchanatham, 2015).

2.3 Maqasid Syariah

According to to Al-Shatibi (1884), Maqasid Syariah is defined as the achievement of goodness, well-being, advantages, benefits and distancing oneself from doing evil, causing harm or loss to creatures. Islamic law is designed to serve the best interests of Muslims, and the term"Maqasid" conveys the notion of purpose, objective, principle, intent, and goal (Kamali, 2008a). It encompasses the underlying wisdom and knowledge behind legal rulings and the intended outcomes of specific actions. The concept of Maqasid al-Shariah highlights the significance of wealth within Islamic law. This importance is also relevant to the

objectives of Islamic law in matters of finance and business transactions, as well as the broader goals of Shariah concerning wealth (Lahsasna, 2009). Islamic banking must develop products and services that are Shariah-compliant, competitive, profitable, and viable. The use of Islamic digital banking based on Maqasid Syariah has emerged to meet the needs of Muslims in digitizing the products and services of Islamic financial institutions.

However, digital banking is the process of digitizing traditional banking activities and transacting online, taking into account the universal and dynamic conception of Maqasid al-Shariah. Hyun-Soo Choi and Roger K. Loh (2020) argue that digital banking has caused many banks to limit their physical operations. Referring to the use of technology, digital banking enables banking transactions to be done smoothly (Sardana, 2018). According to Novi Rifai (2020), the use of digital banking has implemented the elements of Maqasid Shariah by offering the value of security to oneself and property (Hifzul nafs and mal) through safeguarding the security of personal information and the financial flow of users from misappropriation by irresponsible parties. Therefore, the use of Islamic digital banking based on Maqasid Syariah has emerged to meet the needs of Muslims in digitizing the products and services of Islamic financial institutions.

2.4 Underpinning Theory

Gregor (2002) defines underpinning theories as theories that are utilized in Information System (IS) studies to gain a better understanding of the social environment. The theories seek to explain "how" and "why" things occur in the manner that they do. The theory is defined differently by various people, and there is no consistent definition (Mouza, 2018). Underpinning theories employed in Information System (IS) studies and their utility to academics looking for a theoretical basis for their arguments. Information System (IS)

research has grown greatly and integrated socio-technical frameworks (Gregor, 2006). As we all know, the underpinning is any theoretical or background work done on the topic to support the research and thesis. The use of theories to support studies is most common in qualitative and quantitative interpretative research. A theory is a collection of ideas meant to explain anything about life or the world, particularly an unproven hypothesis (Kawulich, 2009).

2.4.1 Theory of Reasoned Action (TRA)

The theory of reasoned action (TRA or ToRA) seeks to explain how attitudes and behaviour interact in human actions. It suggests that a person's intention to perform or not to perform a behavior affects their behaviour, with a higher intention tending to increase the probability of the enactment of that behaviour (Ajzen & Fishbein, 1980). Hale et al. (2002) assert that the theory of reasoned action is the primary framework used to describe an individual's deliberate behavior. It posits that individual attitudes and normative influences, specifically subjective norms, play a crucial role in shaping behavior. In essence, the theory proposes that an individual's behavioral intentions are influenced by specific knowledge or key concepts, with individual attitudes and subjective norms serving as mediators (Madden et al., 1992). To put it simply, the theory of reasoned action was the first to argue for a connection between internal motivation and behaviour, providing a basis for further research into attitude-behavior relationships. In the theory of reasoned action, attitude involves the attitude of trust that completing a behaviour leads to a certain result, weighted by an assessment of the acceptance of that outcome in the theory of reasoned action (Teo & van Schaik, 2012). As a result, the theory of reasoned action identifies the causes of attitude and subjective norm, which represent behavioural perceives about the expected results of an action.

Source: Azjen & Fishbein (1975)

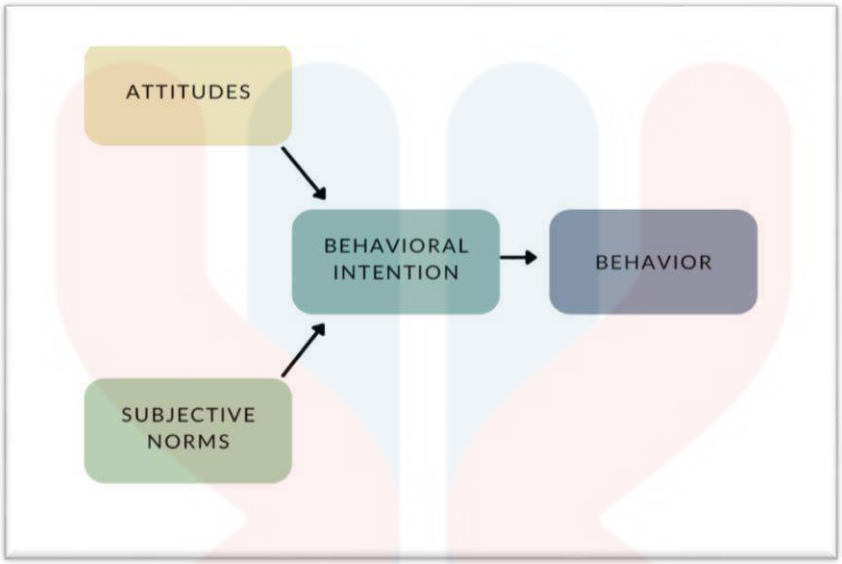

Figure 2.1: Theory of Reasoned Action (TRA)

The theory of reasoned action identifies the determinants of attitude and subjective norm, which reflect behavioral beliefs about the likely consequences of action.

In the era of globalization, various attitudes can be seen day to day as a result of individuals' exposure to utilizing the Internet. Martin Fishbein & Icek Ajzen (1975) proposed reasoned action as an improvement to information integration theory to address people's attitudes towards cyber security awareness. This scale examines attitudes related to cyber security and how individual employees perceive threats from cybercrime (Hadlington, 2017). In the context of internet user experience, TRA suggests that individuals' attitudes toward using the internet will shape their intentions to engage in specific online behaviors (Duggan et al., 2001). Chu (2011) discovered that Facebook group members have a more positive attitude towards social media and advertising. If an individual has positive attitudes towards the internet, such as perceiving it as a valuable tool for communication, information retrieval, or entertainment, they are more likely to have positive intentions to use it and have a

favorable user experience (Van et al., 2021). On the other hand, if individuals have negative attitudes towards the internet, such as concerns about privacy, security, or usability issues, their intentions to engage in online activities may be negatively impacted, leading to a less satisfying user experience.

Other than that, the subjective the norm is a fundamental concept in the theory of reasoned action (Fishbein & Ajzen 1975). It is motivated and a result of an individual's trust that certain referent people or groups approve of behaviour. It represents an individual's perception of his or her capacity to use Islamic financial services securely. The Theory of Reasoned Action (TRA) can be applied to understand the influence of subjective norms on individuals' knowledge of technology and social media information (Izuagbe et al., 2021). According to Ajzen (1991), subjective norms refer to the perceived social pressure or influence on an individual's behavior. In the context of technology and social media information, subjective norms can play a significant role in shaping individuals' knowledge and behaviors. These norms can influence individuals' knowledge acquisition and information-seeking behavior related to technology and social media (Askar & Mazman, 2013). For example, individuals are more likely to seek information, acquire knowledge, and stay updated if their social circle encourages them to use technology and engage in social media. On the other hand, individuals may be less motivated to seek relevant information or acquire knowledge if perceived social norms discourage or devalue technology use or social media engagement (Turner, 1991). In fields such as information technology acceptance and information security, the subjective norm is a significant influence on an individual behavior. Researchers used this theory to determine factors influencing the level of cyber security awareness.

2.5 Previous Studies

The previous study was based on the Theory of Reasoned Action (TRA) which consists of four independent variables: knowledge of technology, social media information, Internet users' experience, and Internet users' attitude. Meanwhile, the dependent variable is the factors influencing the level of cyber security awareness.

2.5.1 Knowledge of technology

In current society, technology has become an essential component that has a big impact on many aspects of our life. Previous researchers investigated and defined the idea of 'technology' from a variety of perspectives, influencing research frameworks, transfer agreements, and governmental policies (Reddy & Zhoa, 1990). Technology is related with particular goals, solving issues, and accomplishing tasks through the use of skills, knowledge, and resources (Lan & Young, 1996). It encompasses not only physical technology but also knowledge and information regarding its use, application, and development process (Lovell, 1998; Bozeman, 2000). Bozeman (2000) builds on Sahal's concept (1981) to argue that technology and knowledge are inseparable. In the modern world, technology serves a role beyond being a simple tool. Technological knowledge, including the ability to operate specific technologies, plays a critical role in integrating technology into the process of teaching and learning (Chai et al., 2010).

According to Bada (2015) and Saizan & Singh (2018), having knowledge and control over social media is important. A previous study by Bada et al. (2015) suggested that interventions based on theoretical knowledge are needed to change the behavior of social media users. Furthermore, a lack of understanding and ignorance about the consequences of disclosing personal information makes individuals more vulnerable to cyber-attacks (Das and Patel, 2017). Meanwhile, older age groups are particularly vulnerable to cyber-attacks, with

no variation in cyber knowledge across age groups, but men tend to have higher cyber knowledge than women (Cain, 2018). Knowledge is an important factor in promoting cyber security awareness, as individuals feel unsafe online and lack the necessary knowledge to protect themselves (Kovacevic et al., 2020). This is because individuals feel unsafe online and lack the necessary knowledge to protect themselves. To address this gap, there is a common misconception that students are no smarter when it comes to using technology.

2.5.2 Social media information

As we all know, social media is a computer technology that allows individuals to communicate with one another via online networks and communities. Social media use has increased significantly in recent years (Leong et al., 2019). It refers to all types of digital content communicated to and received from members of our social network via social networking websites (Nadda et al., 2015). People utilise social media for a variety of reasons, including entertainment, communication and information collecting. However, it also plays a role in fostering a sense of connectedness with relevant others, which may help reduce social isolation (Twenge & Campbell, 2019). Swar and Hameed (2017) define social media as "websites and online tools that facilitate interactions between users by providing opportunities to share information, opinions, and interests." It refers to any website or application that allows users to participate in social networking activities such as creating, sharing, or interacting with information (Piskorski et al., 2016).

Accessing social media platforms such as Facebook, Instagram, WhatsApp, and others has become a regular part of many people's routines. According to Madden (2012), privacy is a major concern for users of social networking sites. Benisch et al. (2011) found that social media users feel they lack control over their privacy. This is often due to users

freely sharing personal information, which can result in privacy violations. Additionally, the lack of security knowledge among social media users exposes them to various cybercrimes (Hadlington, 2017). Many users are unaware of the security and privacy measures that can be implemented on their individual accounts. Yerby et al. (2019) emphasize the importance of prioritizing personal information protection on social media sites. Carminati et al. (2011) suggest that implementing enhanced access control systems for social network sites is a crucial initial step in addressing the security and privacy threats associated with social media. In conclusion, social media can be beneficial when used appropriately but can also be harmful when misinterpreted. Future research should consider incorporating new elements, such as privacy concern, security concerns, trust and awareness on social media sites, into their investigations.

2.5.3 Internet users' experience

The concept of user experience was introduced by Norman (2002) in the early 1990s. in the digital realm, user experience refers to ensuring that websites, mobil sites, or applications provide a positive and intuitive interactions for users, avoiding confusion. It encompasses the feelings and perceptions users have when using a product or service, typically a website or application. This includes all aspects of the end user's interaction with the company or service, such as apps, software, products, and websites (Babich, 2017). However, the definition of user experience remains open and controversial, even though it is widely regarded as a desirable aspect (Law et al., 2009). Users are concerned about privacy and data misuse, but there are opportunities to enhance user experience in terms of privacy, personalization, and community aspects. User experience significantly influences technological innovation by identifying users' wants and needs, as noted by Mullins (2015).

Maintaining a balance between security and user experience in mobile and Internet banking is a difficulty for banking service providers, as new fraud victims are exposed to financial losses. This is related to a previous study, according to Meikeng (2020) highlights that most cases during the MCO (Movement Control Order) involved fraud, intrusion, and cyber harassment. Without proper awareness of cyber security, internet users become vulnerable to hackers, scammers, and cyber-criminals. The necessity to provide an adequate level of security and privacy in Internet and mobile banking is a big obstacle to improving user experience. Security measures often have an influence on an application's ease of use, which is a critical factor for user satisfaction (Liao & Cheung, 2002). Users' experiences are influenced by factors like internet connection quality, device usability, and access to online resources (Chiu et al., 2005). In summary, the experiences of internet users can be diverse and influenced by individual preferences, online activities, and external factors.

2.5.4 Internet users' attitude

Various psychologists have characterized attitudes in various ways. According to Bruvold (1980), an attitude can be described as a positive or negative emotional response towards a specific object or proposition, whether concrete or abstract. Individuals develop varying positive and negative attitudes towards things and topics they are engaged with, including the Internet as a means of communication with its visual and auditory aspects. Additionally, an attitude can be understood as a state of belief, value, or emotion that influences actions or behaviors (Altmann, 2008). Internet usage has been linked to negative outcomes such as decreased social circles, increased psychological isolation, and higher rates of depression among users (Kraut et al., 1998). Furthermore, there is a negative correlation observed between individuals' attitudes towards using the Internet in teaching, utilizing it for research purposes, and their overall likability of Internet usage in teaching (Oral, 2008).

Internet users should have positive attitudes, adequate knowledge of the Internet, and a supportive learning environment. They should be aware of any information they come across, as not all information can be trusted. Attitude and service quality are important factors influencing consumers' choices for using Islamic digital banking goods and services (Dawami, 2020). A negative attitude towards cyber security in business is positively related to dangerous cyber security practices (Hadlington, 2017). For example, Smitherson (2012) stated that the readiness to share personal information with others should only be for someone who can be trusted and that any information supplied by others should be checked and validated. A recent study by Hadlington (2018) discovered an important negative link between attitudes towards cyber security and dangerous cyber security practices, with greater unfavourable views being associated with higher levels of risky behaviour. It is important to address that students should have positive attitudes toward using the Internet as a learning tool, adequate knowledge of the Internet, and a supportive learning environment.

2.6 Hypotheses Statement

Hypothesis are developed to study the relationship between the dependent variable which are the level of cyber security awareness and the other four independent variables which are knowledge of technology, social media information, internet users' experience, and internet users' attitude. This study focuses on the factors influencing the level of cyber security awareness in UMK students, and the following hypotheses are obtained:

H1: There is a significant relationship between knowledge of technology and the level of cyber security awareness among UMK students.

H2: There is a significant relationship between social media information and the level of cyber security awareness among UMK students.

H3: There is a significant relationship between internet users' experience and the level of cyber security awareness among UMK students.

H4: There is a significant relationship between internet users' attitudes and the level of cyber security awareness among UMK students

2.7 Conceptual Framework

This figure shows the conceptual framework comprising the dependent variable and the independent variable among University Malaysia Kelantan students.

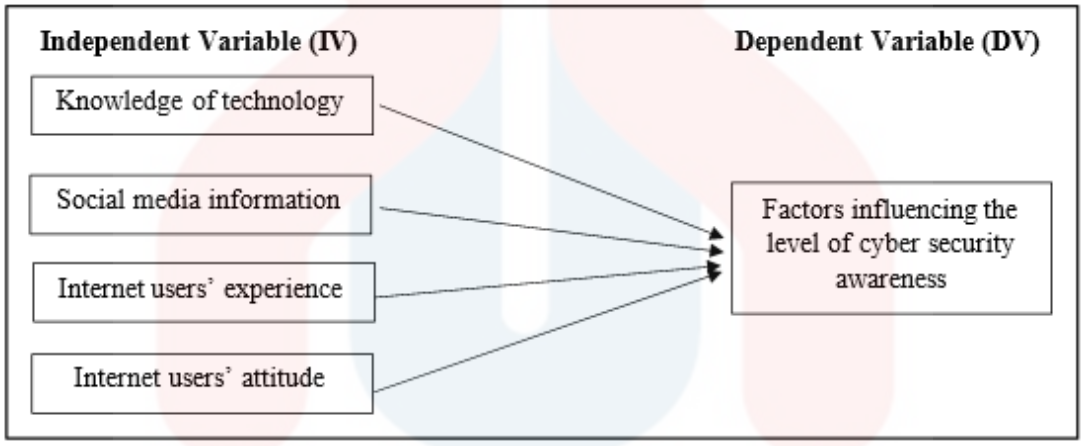

Figure 2.2: The conceptual framework for the factors influencing the level of cyber security awareness

2.8 Conclusion

The primary objective of this chapter is to examine the existing literature and focus on the knowledge of University Malaysia Kelantan students regarding the utilization of Islamic Digital Banking with regards to cyber security awareness. The findings reveal several important factors that should be taken into account, emphasizing the need for banks to ensure that clients have access to safety measures when using financial services and to enhance customer awareness. Additionally, banking customers must also take personal responsibility to prevent falling victim to cyber security issues. Through this chapter, students can identify

the independent variables, such as knowledge of technology, information obtained from social media, experience as internet users, and attitudes towards internet usage, while the dependent variables are the factors influencing the level of cyber security awareness. These variables form the foundation of the conceptual framework from this study. This study's conceptual framework is based on the dependent and independent variables.

CHAPTER 3 RESEARCH METHOD

3.1 Introduction

Following on Chapter 2, this chapter will discuss the research approach that will be employed in this study. In this chapter, the researcher can also determine if the study is qualitative or quantitative. This study discusses data collection methods, study populations, sample sizes, sampling techniques, research instrument creation, variable measurement, and data processing procedures.

3.2 Research Design

A research design is a set of procedures and tactics used by researchers to organize and logically combine various study components (The intactone, 2020). There are two types of research designs: quantitative and qualitative design. The rationally planned research components ensures that the researcher will deal with the problem properly in terms of developing an action plan, collecting and measuring and analysis data.

A quantitative research design will be used in this study to understand the relationship between independent variables (knowledge of technology, social media information, internet users' experience, and internet users' attitude) and dependent variables (cyber security awareness). This study will be conducted at random among UMK students in Pengkalan Chepa.

3.3 Data Collection Methods

In this segment, this study will discuss what type of method can use to collect data for the quantitative research. The data collection method is one of the methods used to gather all of the information, answer the questions posed, test the hypothesis, and assess the result (Bhat, 2023). Meanwhile, data collection is the systematic and specified act of gathering and measuring information regarding variables of interest. The researcher collects all relevant data in order to examine and confirm the problem that occurs within their research. For this research, the primary source can be used, which is the data collected through online surveys. For example, a questionnaire will be created using Google Forms. The questionnaire will be distributed randomly on social media sites such as Instagram, Facebook, WhatsApp, etc. to get respondents from UMK students.

3.4 Study Population

In this study, the population will be all the students at UMK campus in Pengkalan Chepa. This is because UMK is one of the IPTA in Malaysia according to Info UPU (2020). This research to study the factors that affect the level of cyber security awareness among UMK students because UMK is one of the universities based on entrepreneurship and business and is able to provide awareness to students related to cyber threats that are becoming more prevalent. In this campus have several faculty that suitable for this study such as Faculty of Entrepreneurship and Business, Faculty Hospitality, Tourism and Wellness and Faculty Science Data and Computer. Students can benefit from this research by being more cautious when utilising digital banking. So this study concentrate on students at the UMK Kota campus in Pengkalan Chepa and the overall number of students to be 6342. As a result, the population size for this study was 6342 students.

This table shows the number of student in UMK City Campus:

Table 3.1: The number of students UMK City Campus

No	Faculty	Number of student
1	Faculty of Entrepreneurship and Business	3534
2	Faculty Hospitality, Tourism and Wellness	2683
3	Faculty Science Data and Computer	125

3.5 Sample Size

A "sample size" is a research word that refers to the number of people involved in a study to represent the entire population (Bhat, 2023). The sample size refers to the overall number of respondents included in the study, which will be sorted into different subgroups based on demographics such as age and gender, so that the total sample can represent the complete population (Omniconvert, 2023). The term "sample size" refers to the total number of respondents who participated in the study. To ensure that the sample as a whole accurately represents the population, this number will be divided into several subgroups based on demographics, such as age and gender. The number of participants or observations included in a study, indicated by n, is sometimes referred to as sample size. The sample size for this study is 361 students, which was selected based on thepopulation size. The sample size was calculated using Krejcie and Morgan's table. This is formula to calculate the sample size:

$$\text{Sample Size} = \frac{(\text{Z-score})^2 \times \text{StdDev} \times (1-\text{StdDev})}{(\text{confidence interval})^2}$$

Figure 3.1: Formula for Sample Size

This is the table to determining sample size of the population:

Table 3.2: Table for determining Sample Size of a Known Population

Table for Determining Sample Size of a Known Population

N	S	N	S	N	S	N	S	N	S
10	10	100	80	280	162	800	260	2800	338
15	14	110	86	290	165	850	265	3000	341
20	19	120	92	300	169	900	269	3500	346
25	24	130	97	320	175	950	274	4000	351
30	28	140	103	340	181	1000	278	4500	354
35	32	150	108	360	186	1100	285	5000	357
40	36	160	113	380	191	1200	291	6000	361
45	40	170	118	400	196	1300	297	7000	364
50	44	180	123	420	201	1400	302	8000	367
55	48	190	127	440	205	1500	306	9000	368
60	52	200	132	460	210	1600	310	10000	370
65	56	210	136	480	214	1700	313	15000	375
70	59	220	140	500	217	1800	317	20000	377
75	63	230	144	550	226	1900	320	30000	379
80	66	240	148	600	234	2000	322	40000	380
85	70	250	152	650	242	2200	327	50000	381
90	73	260	155	700	248	2400	331	75000	382
95	76	270	159	750	254	2600	335	1000000	384

Note: N is Population Size; S is Sample Size *Source: Krejcie & Morgan, 1970*

3.6 Sampling Techniques

This study are using quantitative data collection method to collect the results. The study employed sampling techniques that is probability sampling to acquire data from UMK City Campus students as the participants in this study. Since this study are personally UMK City Campus students and choose not to include individuals from other universities, this is the most straight forward method of gathering data. Probability sampling implies a sampling technique in which every member of population has a known and non-zero chance of being selected for the sample. The probability techniques relies on random selection and that will be used in this study is simple random sampling.

3.6.1 Simple Random Sampling

Simple random sampling is an extensively used sampling methods in scientific research. Simple random sampling is selected for population which are highly homogenous where the members of the research are randomly selected to participate in the research (Bahrdwaj,

2019). Simple random sampling is the “simplest and most common method of selecting a sample, in which the sample is selected unit by unit, with equal probability of selection for each unit at each draw” (Singh, 2003).

3.7 Research Instrument Development

Before obtaining any other data, it becomes essential for the study to design a research instruments. Distribute questionnaires survey created by this study can be used to test the research instrument. Each respondent will receive the same questions, ensuring that the data gathering is more useful and organised for questionnaire analysis. The study's data collecting tool of choice is thought to be Google Forms as a method.

3.8 Measurement of The Variables

This study will collect and analyse data in order to create a statistically significant test for each of the variables on the scale. In these questions, the nominal and ordinal measuring scales are used. Sections A until F to form the six sections of the questionnaire. Section A is about the demography profile of the respondents, section B is related to the dependent variable and section C until F questions is regarded to the independent variables.

3.8.1 Nominal Scale

In this study, a nominal scale is used to collect the demographics of the respondents and is not suitable for mathematical calculations. This scale will be applied to section A in order to collect data. The respondent’s gender, age, faculty, and programme are all evaluated with the nominal scale.

3.8.2 Ordinal Scale

The items on this scale have been arranged from minimum to maximum in ascending order of acknowledged level. On section B, which highlights the factors influencing the level of cyber security awareness, the 5-Likert scale will be used, while section C until F are about independent variables, which includes elements of knowledge of technology, social media information, internet users' experiences, and attitudes, will use the same scale. The questionnaires are used to evaluate how strongly the respondent disagrees with or agrees with the assertions using the 5-Likert scale that are strongly disagree (1), disagree (2), neutral (3), agree (4), and strongly disagree (5).

3.9 Procedure For Data Analysis

The data in this study will be analysed and interpreted using the Statistical Package for Social Science (SPSS) version 20. The data from the questionnaires will be collected, modified, specified, and encrypted by SPSS. As a result, it will take less time to convert the raw data into the dataset. This technique is used to examine, personalise, and generate clear patterns between various data factors.

3.9.1 Descriptive analysis

The data's characteristics will be described by descriptive analysis using the mean, median, standard deviation, variance, range, and percentile. This method of summarising and describing data from a sample is used. Researchers can find elements that affect research findings with the help of descriptive analysis.

3.9.2 Validity Test

Based on the Table 3.3 below, this is the survey that the researchers took from previous study. Currently, the researchers build up the adopted items by taken the previous items to develop data.

Table 3.3: Original and adopted Items

Section	Variables	Source	Items	Adopted Items
A	Demographic		1. Gender 2. Age 3. Current year of Study 4. Faculty 5. Programme	1. Gender 2. Age 3. Current year of Study 4. Faculty 5. Programme
B	Factors influencing the level of cyber security awareness	1. Zwilling et al., 2022 2. Al Janabi et al., 2016 3. Oladapo et al., 2022	1. Are you familiar with the term cyber security? 2. When you receive an email from unfamiliar sender, do you open it? 3. Did you use backup software to back up your important data? 4. In your opinion, is it important that the academic institutions to have an information security officer? 5. I am familiar with the benefit of FinTech services. 6. I am aware of the Importance of the	1. I am aware with the term cyber security 2. I am aware of email from unfamiliar sender and decide to not open it. 3. I am aware of using backup software to back up my important data. 4. I am aware that the Islamic digital banking must have an information security officer. 5. I am familiar with the application of Islamic digital banking services. 6. I am aware of the significant of Islamic Digital banking activities.

			FinTech in conducting banking activities. 7. I am not concern about using FinTech services. 8. I have been exposed to the types of FinTech services. 9. I am not interested to use FinTech services at all. 10. I do not know much about FinTech services.	7. I am not concern about using Islamic digital banking. 8. I have been exposed to the types of Islamic digital banking services. 9. I am not interested to use Islamic digital banking services at all. 10. My awareness in Islamic digital banking is limited.
C	Knowledge	1. Ion et al., 2015 2. Oladapo et al., 2022	1. How would you rate your skill and knowledge in level of internet skills? 2. How would you rate your skill and knowledge in cyber threats online? 3. I have knowledge to use FinTech services. 4. I know it is better to use FinTech in conducting my banking activities. 5. I am usually interested to know more about FinTech services. 6. Using FinTech will provide opportunity to control my banking	1. My skill and knowledge in Islamic digital banking is limited. 2. My skill and knowledge in cyber security awareness is limited. 3. I have knowledge to use Islamic digital banking services. 4. I know it is better to use Islamic digital banking in conducting my banking activities. 5. I am interested to know more about Islamic digital banking services. 6. Using Islamic digital banking will provide opportunity to control my banking activities.

			activities. 7. I am willing to use the travel information on social media before and during the trip.	7. I am willing to share with others about my knowledge of Islamic digital banking.
D	Information	1. Farag et al., 2010 2. Chung et al., 2015	1. For me, travel information on social media is very timely. 2. For me, the accuracy of travel information on social media is strong 3. For me, the content of travel information on social media is very rich. 4. For me, travel information on social media is very applicable. 5. Social media helps me get more information about my trip. 6. The travel information on social media helps me to get solve the difficulties encountered on the trip. 7. Travel information on social media can improve my travel efficiency.	1. For me, information on social media about the Islamic digital banking is very timely. 2. For me, the accuracy of information on social media about the Islamic digital banking is strong. 3. For me, the content of information on social media about the Islamic digital banking is very rich. 4. For me, information on social media about the Islamic digital banking is very applicable. 5. Social media helps me get more information about the Islamic digital banking. 6. The information on social media guide me to solve the difficulties on Islamic digital banking. 7. Information on social media can improve my transaction on Islamic

				digital banking efficiency.
E	Experience	1. Adamu et al., 2021 2. Kankanh-alli et al., 2005 3. Laugwitz et al., (2008)	1. I will only make an online purchase after inspecting the seller's background. 2. I am worried when I received any suspicious online advertisement. 3. I will provide my personal information whenever I received calls from banking organizations. 4. The online platform can be trusted at all times. 5. Provides easy to understand information. 6. I believe that the platform will not misuse my donation. 7. The online platform has a high level of integrity. 8. User's impression that reaching goals using the product is quick and efficient.	1. I will only make an online transaction after inspecting the digital banking background. 2. I am worried when I received any suspicious link about digital banking. 3. I will never provide my personal information whenever I received calls from personal numbers that declare themselves from banking organizations. 4. For me, the Islamic digital banking platform can be trusted all the time. 5. The Islamic digital banking provide easy to access the platform. 6. I believe that the Islamic digital banking platform will not simply withdraw my money. 7. The Islamic digital banking platform has a high level of integrity. 8. I found out that reaching the Islamic digital banking is quick and efficient.
F	Attitude	1. Adamu et	1. I would spend more time on social media	1. I would spend more time on digital banking

		al., 2021 2. Oladapo et al., 2022	than having outdoor activities. 2. I will be extra excited when I use the Internet. 3. The time spent without surfing the Internet is the most boring moment. 4. Without the Internet, there is nothing I can do. 5. I believe using FinTech for my banking transaction is a good idea. 6. The FinTech platform makes banking operations faster. 7. FinTech will encourage me to transact online. 8. FinTech is user friendly. 9. FinTech makes banking transactions more efficient. 10. I will feel confident when I use FinTech for my transactions with the bank.	comparing to traditional banking. 2. I am very convenient when I use the digital banking. 3. It takes a longer time to accomplish our activity without the digital banking. 4. Without the digital banking, there is nothing I can do. 5. I believe using digital banking transaction is a good idea. 6. The Islamic digital banking platform makes the transactions faster. 7. Islamic digital banking will encourage me to transact online. 8. Islamic digital banking is user friendly. 9. Islamic digital banking makes banking transactions more efficient. 10. I will feel confident when I use the Islamic digital banking for my transactions with the bank.

3.9.3 Reliability Test

This study investigates reliability analysis, the characteristics that determine scales, and the components that comprise the scales. The reliability analysis method provides a variety of regularly used scale reliability statistics, as well as correlation data among the scale's components. Cronbach Alpha is a simple statistic to evaluate dependability in exploration writing.

The table 3.6 below is about the rules of thumb for the size of Cronbach's Alpha Coefficient, appropriate coefficient alpha should be equal to or greater than 0.7.

Table 3.4: The Rules of Thumb for the Size of Cronbach's Alpha Coefficient

Alpha Coefficient Range	Strength of Association
<0.6	Poor
0.6 to < 0.7	Moderate
0.7 to < 0.8	Good
0.8 to < 0.9	Very Good
0.9	Excellent

Sources: Hair et.al (2003); Essential of Business Research Method.

i. Pilot test

The purpose of the pilot test is to validate the validity of the questionnaire and establish whether the independent and dependent variables will contribute appropriately to the analysis. The researchers have to identify a connection between the overall purpose of the pilot study and the overall objective.

ii. Actual data

Actual data in research methodology refers to the information and facts collected through

research methods and instruments. In research, data serves as the basis for analysis and interpretation, leading to the development of research findings and conclusions. Data can be collected through various methods such as surveys, interviews, experiments or observation. Once collected, data needs to be organized, coded, and analyzed to reveal trends, patterns, and relationships. Actual data is the information and facts collected through research methods and instruments which are analyzed and interpreted to draw meaningful conclusions. The accuracy and quality of data collection and analysis are critical to ensure the validity and reliability of research findings.

3.9.4 Correlation Analysis

Correlation analysis is a statistical technique used to measure the strength and direction of the relationship between two variables. It involves calculating a correlation coefficient, which is a numerical value that indicates the degree to which two variables are related. Correlation analysis can be used to identify patterns and relationships between variables, and is commonly used to analyze data and make predictions. After have done the related test, the researchers can justify whether to use the Spearman Correlation Coefficient or Pearson Correlation Coefficient.

3.9.5 Multiple Linear Regression (MLR)

The multiple linear regression will be used to predict variables regarding the cyber security awareness of Islamic digital banking among UMK City Campus students. Since the independent variables of this study have four which are knowledge of technology, social media information, internet users' experience, and internet users' attitude, the researchers will analysed the factors that influence the level of cyber security awareness.

3.10 Conclusion

Overall, this chapter has come to a conclusion about how the research will be conducted. In order to determine the level of cyber security awareness of Islamic digital banking among UMK City Campus students, the topic discusses the research design, data collection methods, study population, sampling method, sample size, research instrument development, measurement of the variables, and methodology for data analysis.

CHAPTER 4 DATA ANALYSIS AND FINDINGS

4.1 Introduction

The researchers will analyze the procedures developed in previous chapters in this chapter. A total of 371 respondents to the provided questionnaire. The researchers analyzed the data using the Statistical Package for the Social Science (SPSS) version 20. The findings of the preliminary analysis, demographic profile of respondents, descriptive analysis, validity and reliability test, normality test, and hypothesis testing are the main topics of this chapter.

4.2 Preliminary Analysis

A research study was conducted at University Malaysia Kelantan (City Campus) with a focus on student respondents from three faculties. 371 respondents completed a questionnaire through Google Form, and all were considered legitimate in data analysis.

4.3 Demographic Profile of Respondents

Table 4.1: Demographic profile of respondents based on gender, age, and current year of study, faculty and programme.

Category	Type	Number of Respondents N = 371	Percentage
Gender	Male	123	33.2%
	Female	248	66.8%
Age	18 – 20 years old	67	18.1%
	21 – 23 years old	240	64.7%
	24 – 26 years old	64	17.3%
Current Year of Study	Year 1	61	16.4%

	Year 2	54	14.6%
	Year 3	184	49.6%
	Year 4	72	19.4%
Faculty	FKP	280	75.5%
	FHPK	78	21%
	FSDK	13	3.5%
Programme	SAB	184	49.6%
	SAK	21	5.7%
	SAE	19	5.1%
	SAL	21	5.7%
	SAR	21	5.7%
	SAA	16	4.3%
	SAP	25	6.7%
	SAH	32	8.6%
	SAS	20	5.4%
	SST	12	3.2%

Table 4.1 shows that a survey was conducted with 371 respondents that contain gender, age, current year of study, faculty and programmes. 66.8% (N = 248) of respondents were female and 33.2%(N = 123) were male. The largest age group was 21-23, with 64.7% (N = 240) of respondents. The next largest was 18-20 years old at 18.1% (N = 67) and 24-26 at 17.3% (N = 64). Year 3 students comprised majority at 49.6% (N = 184). Year 1 was 16.4% (N = 61), Year 2 was 14.6% (N = 54), and Year 4 was 19.4% (N = 72). Most respondents, 75.5% (N = 280), were from the Faculty of FKP. 21% (N = 78) were from FHPK, and 3.5% (N = 13) were from FSDK. The most significant programmes represented was SAB at 49.6% (N = 184). The other programmes described were SAKat 5.7% (N = 21), SAE at 5.1% (N = 19), SAL at 5.7% (N = 21), SAR at 5.7% (N = 21), SAA at 4.3% (N = 16), SAP at 6.7% (N = 25), SAH at 8.6% (N = 32), SAS at 5.4% (N = 20), and SST at 3.2% (N = 12).

4.4 Descriptive Analysis

Table 4.2: Mean, standard deviation and variance of all variables

Descriptive Statistics

	N	Mean	Std. Deviation	Variance
CYBER_SECURITY	371	4.1854	.53817	.290
KNOWLEDGE	371	4.1057	.50537	.255
INFORMATION	371	4.1919	.54091	.293
EXPERIENCE	371	4.2022	.52319	.274
ATTITUDE	371	4.1563	.55870	.312
Valid N (listwise)	371			

Table 4.2 reveals that the dependent variable, cyber security, has a mean score of 4.1854 with a standard deviation of 0.53817. In addition, the independent variables exhibit high mean scores, particularly experience, with a mean of 4.2022 and a standard deviation of 0.52319. Other independent variables also display strong mean scores that are knowledge (mean=4.1057, SD=0.50537), information (mean=4.1919, SD=0.54091), and attitude (mean=4.1563, SD=0.55870).

Table 4.3: Mean and standard deviation of cyber security

Descriptive Statistics

	N	Mean	Std. Deviation
1. I am aware with the term cyber security.	371	4.23	.666
2. I am aware of email/message from unfamiliar sender and decide to not open it.	371	4.21	.627
3. I am aware of using backup software to back up my important data.	371	4.18	.694
4. I am aware of Islamic digital banking services that expose to cyber security risk.	371	4.20	.638
5. Cyber security risk includes phising and malware.	371	4.10	.670
Valid N (listwise)	371		

The five questions in the descriptive analysis are based on Table 4.3. The respondents' mean response on the dependent variable factor is displayed using a five-point Likert scale ranging from 4.10 to 4.23. Table 4.2's average mean was 4.1854. To further explain, the mean for question 1 was the highest regarding awareness of the term cyber security. The mean for question 2, which asked whether you were aware of an email or message from an unfamiliar sender and decided not toopen it was 4.21 (SD=0.666). The mean for question 4, where the awareness of Islamic digital banking services that are exposed to cyber security risk, was 4.20 (SD=0.638). Next, the mean for question 3, which is about awareness of using backup software to back up their important data, is 4.18 (SD=0.694). Lastly, the mean for question 5, which is about cyber security risks, including phishing and malware, is 4.10 (SD=0.670).

Table 4.4 Mean and standard deviation of knowledge

Descriptive Statistics

	N	Mean	Std. Deviation
1. My skill and knowledge in Islamic digital banking services is limited.	371	4.04	.677
2. My skill and knowledge in cyber security awareness is limited.	371	4.04	.708
3. I have knowledge to use Islamic digital banking services.	371	4.11	.708
4. I know it is better to use Islamic digital banking in conducting my banking activities.	371	4.18	.641
5. I am interested to know more about Islamic digital banking services.	371	4.16	.629
Valid N (listwise)	371		

Based on Table 4.4, the descriptive analysis is about knowledge that consists of five questions answered using a five-point Likert scale. The mean response of the knowledge ranges from 4.04 to 4.18. The mean response for questions 1 and 2, which measure skill and knowledge in Islamic digital banking services and cyber security awareness is limited

and was the lowest. The mean for question 3, asking about knowledge of Islamic digital banking services, was 4.11. The mean for question 5 was 4.16. The average mean was 4.1043. The number 4 question, measuring whetherit is better to use Islamic digital banking in conducting their banking activities, had the highest mean at 4.18.

Table 4.5: Mean and standard deviation of information

Descriptive Statistics

	N	Mean	Std. Deviation
1. The information about cyber security awareness guide me to solve the difficulties on Islamic digital banking services.	371	4.18	.643
2. I am cautious about receiving phishing attempts or email scams aimed at stealing my personal information.	371	4.20	.629
3. Bank's cyber security notifications help enhance the security of my account.	371	4.21	.650
4. Islamic digital banking consistently reminds me to stay alert from potential cyber security.	371	4.23	.681
5. I regularly change my password on digital banking services to avoid unauthorized access and enhance security.	371	4.13	.710
Valid N (listwise)	371		

The five questions in the descriptive analysis are based on Table 4.5. The respondents' mean response on the independent variable of the information factor is displayed using a five-point Likert scale ranging from 4.13 to 4.23. Table 4.2's average mean was 4.1924. To further explain, the mean for question 4 was the highest regarding Islamic digital banking consistently reminding them to stay alert for potential cyber security. The mean for question 1, which asked whether cyber security awareness guides them to solve the difficulties of Islamic digital banking services was 4.18 (SD=0.643). The mean for question 2, where the cautious about receiving phishing attempts or email scams aimed at stealing their personal information, was 4.20 (SD=0.629). Next, the mean for question 3, about bank's cyber

security notifications helping enhance the security of the respondents' accounts, is 4.21 (SD=0.650). Lastly, the mean for question 5, which concerns respondent's regularly changing respondents' passwords on digital banking services to avoid unauthorized access and enhance security, is 4.13 (SD=0.710).

Table 4.6: Mean and standard deviation of experience

Descriptive Statistics

	N	Mean	Std. Deviation
1. I will never provide my personal information whenever I received calls from personal numbers that declare themselves from banking organizations.	371	4.27	.644
2. For me, the Islamic digital banking services platform can be trusted all the time.	371	4.19	.644
3. The Islamic digital banking services provides easy to access the platform.	371	4.22	.659
4.The Islamic digital banking services will not simply withdraw my money.	371	4.18	.653
5. The Islamic digital banking services has a high level of integrity.	371	4.15	.608
Valid N (listwise)	371		

The five questions in the descriptive analysis are based on Table 4.6. The respondents' mean response on the experience factor is displayed using a five-point Likert scale ranging from 4.15 to 4.27. Table 4.2's average mean was 4.2022. To further explain, the mean for question 1 was the highest regarding never providing their personal information whenever received calls from personal numbers that declare themselves from banking organizations. The mean for question 2, which asked whether they trusted the Islamic digital banking services all the time was 4.19 (SD=0.644). The mean for question 3, where the Islamic digital banking

services provide easy to access the platform, was 4.22 (SD=0.659). Next, the mean for question 4, which is about the experience of the Islamic digital banking services will not simply withdraw their money, is 4.18 (SD=0.653). Lastly, the mean for question 5, about the Islamic digital banking services has a high level of integrity, is 4.15 (SD=0.608).

Table 4.7: Mean and standard deviation of attitude

Descriptive Statistics

	N	Mean	Std. Deviation
1. I would prefer using digital banking rather than traditional banking.	371	4.20	.651
2. I will feel confident when I use the Islamic digital banking services for my transactions.	371	4.16	.666
3. I believe using digital banking transaction is a highly secured.	371	4.16	.681
4. The Islamic digital banking services platform makes the transactions faster and reliable.	371	4.17	.657
5. Islamic digital banking services is user friendly.	371	4.10	.655
Valid N (listwise)	371		

Based on Table 4.7, the descriptive analysis is about attitude that consists of five questions answered using a five-point Likert scale. The mean response of the knowledge ranges from 4.10 to 4.20. The mean response for questions 1, which measure prefer using digital banking rather than traditional banking was the highest mean that is 4.20 (SD=0.651). The mean for question 2 and 3, asking about to feel confident when using the Islamic digital banking services for the transactions and believe using digital banking transaction is a highly secured, was 4.16. The mean for question 4 was 4.17. The average mean was 4.1568. The number 5 question, measuring whether Islamic digital banking services is user friendly, had the lowest mean at 4.10.

4.5 Validity and Reliability Test

The reliability statistics below allow the researcher to determine whether these question sets are reliable in measuring variables. The table below presents the reliability tests for each variable. Cronbach's alpha was used to ascertain this test's reliability and internal consistency.

Table 4.8: Cyber Security

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.875	.876	5

Table 4.8 above indicates that Cronbach's Alpha of cyber security is 0.875, which is good on the Rule of Thumb of Cronbach's Alpha Coefficient Range and can be used in the research.

Table 4.9: Knowledge

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.806	.807	5

As per Table 4.9, Cronbach's Alpha for the five items of the knowledge of technology is 0.806. The obtained value is deemed suitable. The findings indicate that the research item used for concept measurement exhibits outstanding internal consistency. Therefore, the questionnaire can beused in the research.

Table 4.10: Information

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.874	.875	5

Table 4.10 above indicates that the Cronbach's Alpha of the social media information is 0.874, which is good on the Rule of Thumb of Cronbach's Alpha Coefficient Range and can beused in the research.

Table 4.11: Experience

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.874	.875	5

As per table 4.11, the Cronbach's Alpha for the five items of the internet users' experience is 0.874. The obtained value is good. The findings indicate that the research item used for concept measurement exhibits outstanding internal consistency. Therefore, the questionnaire can be used in the research.

Table 4.12: Attitude

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.899	.899	5

Table 4.12 above shows that Cronbach's Alpha of the internet users' attitude is 0.899, which is good on the Rule of Thumb of Cronbach's Alpha Coefficient Range and can be used in the research.

Table 4.13: Reliability statistics for cyber security, knowledge, information, experience, and attitude

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.946	.946	5

Based on Table 4.13 above about reliability, the performance expectancy coefficient alpha shows a commendable coefficient of 0.946, which is excellent. As good indicators, the coefficients for knowledge, information, experience, and attitude were 0.806, 0.874, 0.874, and 0.899, respectively.

Table 4.14: Summary of Reliability Statistics

Dependent variable (DV) and independent variable (IV)	**Croanbach's Alpha**	**Number of variable items**	**Interpretation**
Factors influencing the level of cyber security awareness	0.875	5	Very good
Knowledge of technology	0.806	5	Very good
Social media information	0.874	5	Very good
Internet user's experience	0.874	5	Very good
Internet users' attitude	0.899	5	Very good

4.6 Normality Test

Table 4.15: Test of Normality

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
CYBER_SECURITY	.166	371	.000	.914	371	.000
KNOWLEDGE	.167	371	.000	.917	371	.000
INFORMATION	.140	371	.000	.925	371	.000
EXPERIENCE	.172	371	.000	.920	371	.000
ATTITUDE	.172	371	.000	.915	371	.000

a. Lilliefors Significance Correction

Normality tests were conducted to determine whether the data in this study had a normal distribution. Since the Kolmogorov-Smirnov is more suitable, it was used rather than the Shapiro-Wilk. Despite the Kolmogorov-Smirnov test being the least effective for all types of distributions and sample sizes, the Shapiro-Wilk test's effectiveness remains limited for small sample sizes (Mohd Razali & Yap, 2011). All dependent and independent variables had a significant value of 0.000 in Table 4.15's normality test results.

4.7 Hypothesis Testing

Table 4.16: Pearson Correlation Results

Correlations

		CYBER_SECURITY	KNOWLEDGE	INFORMATION	EXPERIENCE	ATTITUDE
CYBER_SECURITY	Pearson Correlation	1	.736**	.808**	.781**	.761**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	371	371	371	371	371
KNOWLEDGE	Pearson Correlation	.736**	1	.778**	.750**	.740**
	Sig. (2-tailed)	.000		.000	.000	.000
	N	371	371	371	371	371
INFORMATION	Pearson Correlation	.808**	.778**	1	.825**	.779**
	Sig. (2-tailed)	.000	.000		.000	.000
	N	371	371	371	371	371
EXPERIENCE	Pearson Correlation	.781**	.750**	.825**	1	.805**
	Sig. (2-tailed)	.000	.000	.000		.000
	N	371	371	371	371	371
ATTITUDE	Pearson Correlation	.761**	.740**	.779**	.805**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	371	371	371	371	371

**. Correlation is significant at the 0.01 level (2-tailed).

4.7.1 Hypothesis 1: Relationship between Knowledge of Technology and Cyber SecurityAwareness on Islamic Digital Banking

H_0: There is no relationship between knowledge of technology and cyber security awareness on Islamic digital banking among UMK City Campus students.

H_1: There is a relationship between knowledge of technology and cyber security awareness on Islamic digital banking among UMK City Campus students.

Table 4.16 above shows a significant relationship between knowledge of technology and cyber security awareness on Islamic digital banking services among UMK City Campus students. The relationship is explained by a p-value of 0.000 (less than 0.05) and a Pearson Correlation Coefficient of 0.736. The H1 is acceptable.

4.7.2 Hypothesis 2: Relationship between Social Media Information and Cyber Security Awareness on Islamic Digital Banking

H_0: There is no relationship between social media information and cyber security awareness on Islamic digital banking among UMK City Campus students.

H_2: There is a relationship between social media information and cyber security awareness on Islamic digital banking among UMK City Campus students.

The Pearson correlation results above indicate that among UMK City Campus students, there is a significant correlation between social media information and cyber security awareness for Islamic digital banking services. The Pearson Correlation Coefficient value of 0.808, and the p-value is 0.000. The H_2 has been approved.

4.7.3 Hypothesis 3: Relationship between Internet Users' Experience and Cyber SecurityAwareness on Islamic Digital Banking

H_0: There is no relationship between internet users' experience and cyber security awareness on Islamic digital banking among UMK City Campus students.

H_3: There is a relationship between internet users' experience and cyber security awareness on Islamic digital banking among UMK City Campus students.

Table 4.16 above shows a significant relationship between internet users' experience and cyber security awareness of Islamic digital banking services among UMK City Campus students. This relationship is explained by the p-value of 0.000, less than 0.05, and the Pearson Correlation Coefficient value of 0.781. The H_3 is accepted.

4.7.4 Hypothesis 4: Relationship between Internet Users' Attitude and Cyber Security Awareness on Islamic Digital Banking

H_0: There is no relationship between internet users' attitude and cyber security awareness on Islamic digital banking among UMK City Campus students.

H_4: There is a relationship between internet users' attitude and cyber security awareness on Islamic digital banking among UMK City Campus students.

The Pearson correlation results above indicate that among UMK City Campus students, there is a significant correlation between social media information and cyber security awareness for Islamic digital banking services. The Pearson Correlation Coefficient value is 0.761, and the p- value is 0.000. The H_4 has been approved.

4.7.5 Summary of Pearson Correlation results

Table 4.17: Summary of Pearson Correlation results

	Hypothesis	Sig. (2-tailed)	Pearson Correlation	Value
H1	There is a relationship between knowledge of technology and cyber security awareness of Islamic digital banking services among UMK City Campus students.	0.000	.736	High correlation
H2	There is a relationship between social media information and cyber security awareness of Islamic digital banking services among UMK City Campus students.	0.000	.808	Very high correlation
H3	There is a relationship between internet users' experience and cyber security awareness of Islamic digital banking services among UMK City Campus students.	0.000	.781	High correlation
H4	There is a relationship between internet users' attitude and cyber security awareness of Islamic digital banking services among UMK City Campus students.	0.000	.761	High correlation

Table 4.17 shows the dependent variable and independent variable have a positive relationship. All the independent variables correlate highly with factors influencing the level of cyber security awareness among UMK students. Thus, all hypothesis testing is accepted.

4.8 Conclusion

The data analysis results for each test in Chapter 4 were obtained using the Statistical Package for Social Sciences (SPSS) software. The data was analyzed using descriptive analysis, reliability testing, normality testing, and hypothesis testing to determine the relationship between the independent and dependent variables and to identify the factors influencing UMK City Campus students' cyber security awareness of Islamic digital banking. Chapter 5 provides a more detailed explanation of the findings on the relationship between the independent and dependent variables, as well as the factors influencing cyber security awareness.

CHAPTER 5 DISCUSSION AND CONCLUSION

5.1 Introduction

This chapter explores the relationship between knowledge of technology, social media information,internet users' experiences, and internet users' attitudes towards cyber security awareness in Islamic digital banking among UMK city campus students. It also discusses the study's implications, limitations, and recommendations for future research. Besides, this chapter further analyzes the key findings, discussing demographic factors such as gender, age, and the current year of study. The researchers provide a detailed analysis of respondent demographics, including reliability tests and normality tests. They also discuss the research purpose and hypotheses, as well as the limitations faced during the study. This chapter concludes with an overview of what has been learned in the course of this research.

5.2 Key Findings

The primary purpose of this research is to identify the relationship between the dependent and independent variables. Pearson correlation was used to demonstrate the link between the dependent and independent variables. This survey included 371 respondents from the University Malaysia Kelantan (UMK). To obtain more complete and precise data, each questionnaire was analyzed using SPSS. According to the reliability test data presented in Chapter 4, which is related to the reliability test, researchers observed that the reliability test coefficient runs from 0 to 1, covering all measurement tests against the variable. The study questionnaire's Cronbach's alpha coefficient was consistently positive.

According to the research hypothesis, the researcher also discovered that all independent variables, including knowledge of technology, social media information, internet users' experiences, and internet users' attitudes, have a strong and significant

relationship with factors influencing the level of cyber security awareness. The results of the descriptive analysis study show that experience as an independent variable has the highest mean value, which is 4.2022, and the lowest mean value is knowledge, which is 4.1057.

The result of this study of the hypothesis can significantly benefit various stakeholders. Besides, technology developers can design user-friendly solutions, and public awareness campaigns can be tailored for maximum impact. The findings can also contribute to cross-cultural considerations and ongoing efforts to adapt strategies in response to evolving cyber threats. Overall, the study's results offer valuable information for enhancing cyber security at individual, organizational, and societal levels. Through this research, it can also provide an opportunity for individuals to enhance their cyber security skills and engagement, promoting a more secure digital environment.

Lastly, the overall result proves that the majority of respondents, which are UMK students, agree that all four independent variables—knowledge of technology, social media information, internet users' experiences, and internet users' attitudes have been accepted by them as factors influencing the level of cyber security awareness.

5.3 Discussion

5.3.1 Hypothesis 1

H1: There is a significant relationship between knowledge of technology and level of cybersecurity awareness on Islamic digital banking among UMK City Campus students.

The Pearson Correlation results show that there is significant positive correlation between knowledge of technology and cyber security awareness among UMK students. According to the data in Chapter 4, the significant correlation value is r=0.736, indicating a strong positive link between knowledge of technology and cyber security awareness among UMK students. The regression p-value is less than 0.05, indicating a significant relationship between technology abilities (p=0.000) and understanding of technology (p<0.01). As a result, the H1 is accepted. Knowledge of technology has a significant relationship with the level of cyber security awareness among UMK students. This indicates that cyber security awareness among students contributes to the advancement of technological understanding.

5.3.2 Hypothesis 2

H2: There is a significant relationship between social media information and level of cybersecurity awareness on Islamic digital banking among UMK City Campus students.

The Pearson Correlation finding shows that social media information and the level of cyber security awareness among UMK students are significantly positively correlated. The results presented in Chapter 4 indicate a significant beneficial relationship r=0.808 between the amount of cyber security awareness among UMK students and the information found on social media. Considering that the regression p-value for social media is 0.000, the value for

social media is p=0.000, which is very significant. Therefore, this hypothesis can be accepted because the p-value is 0.000. The social media information was moderately higher than other factors. This indicates that social media plays a pivotal role in fostering a noteworthy positive correlation with UMK students' cyber security awareness. Information from social media platforms and Islamic digital banking services are significantly correlated.

5.3.3 Hypothesis 3

> **H3:** There is a significant relationship between internet users' experience and level of cybersecurity awareness on Islamic digital banking among UMK City Campus students.

The Pearson correlate results demonstrate a significant positive relationship between UMK students' technology knowledge and cyber security awareness. According to the statistics presented in Chapter 4, the significant correlation value is r=0.736, demonstrating a strong positive relationship between knowledge of technology and cyber security awareness among UMK students. The regression p-value is less than 0.05, showing a significant link between technology abilities (p=0.000) and knowledge of technology (p<0.01). As a result, the initial hypothesis is accepted. The internet users' experience showed a lower level of positivity than the other factors. This means that internet users' experience has a discernible yet modest positive correlation with the level of cyber security awareness in the context of Islamic digital banking services.

5.3.4 Hypothesis 4

H4: There is a significant relationship between internet users' attitude and level of cyber security awareness on Islamic digital banking among UMK City Campus students.

The Pearson Correlation Coefficient for H4 shows the moderately positive relationship between internet users' attitude and level cyber security awareness of Islamic digital banking services with the value r=0.761. Therefore, the hypothesis can be accepted because the p-value is 0.0000. It also showed the significant relationship between internet users' attitude and cyber security awareness because the p-value less than 0.05 further underscores the significance of the relationship, emphasizing that internet users' attitudes play a crucial role in influencing their awareness of cyber security in the context of Islamic digital banking services. Internet users' attitudes had a less positive correlation than the other parts. According to the Pearson Correlation Coefficient, internet users' attitudes toward Islamic digital banking services are slightly associated with increased cyber security awareness.

5.4 Implications of The Study

The term of implication of the study refers to the prospective effects, applications, or consequences that the findings of a research study may generate. Hassan (2023) stated that comprehending these consequences is essential for assessing the importance and usefulness of research. The consequences can cover multiple aspects, including social, political, technological, policy-related, or others, depending on the distinctive subject matter. The two most utilized forms are theoretical and practical. Theoretical implications means the way that findings establish connections with other concepts or theories within the field of study, whilst practical implications are concerned with the potential applications of the findings.

5.4.1 Theoretical Implications

The primary aim of this study is to investigate the effects of knowledge of technology, social media information, attitude, and experience on the level of cyber security awareness among UMK city campus students in Islamic digital banking. In relation to prior study conducted on this topic, the participants were primarily the general population and students from multiple places in Malaysia. In contrast, this study has restricted the sample to mainly UMK city campus students. This is because this study wants to obtain a more focused perspective on the comprehension of cyber security among students from diverse academic backgrounds, including tourism, logistics, hospitality, and many more. In addition, there are no final year students at UMK that have previously undertaken research on this topic of cyber security awareness. Therefore, this study aims to assess the students' current level of cyber security awareness. Finally, the results of this study can enhance the quantity of research in Malaysia and serve as a valuable resource for future academics investigating the cyber security awareness in Islamic digital banking.

5.4.2 Practical Implications

According to this study, 30.82% of the respondents strongly agree, while 55.99% agree with the level of cyber security awareness in Islamic digital banking. While over 50% of individuals are aware of the cyber security mechanisms in Islamic digital banking, this does not ensure that they are never be one of the cybercrime victims. Griffiths (2023) asserts that cybercrime is on the rise in Malaysia. A total of 20,000 cyber-crimes were reported in 2021, resulting in a loss of RM560 million for the victims. Between January and July 2022, a total of 11,367 incidents of cybercrime were reported, indicating a 61% rise in the crime rate compared to the period from 2016 to 2022. Based on this fact, it is obvious that a significant number of people remain unaware of the importance of cyber security. According to the

survey responses from UMK city campus students, a significant proportion of 0.62% of students remain unaware about cyber security in Islamic digital banking. Nevertheless, it is notable that it's just a small fraction, specifically fewer than 1% of respondents lack awareness. Despite this, the National Cyber Security Agency (NACSA) should have conducted more additional programs to enhance citizen awareness regarding cyber security. Hence, when the public, particularly UMK students, reach a level of progress on their awareness regarding cyber security in Islamic digital banking, this will swiftly contribute to a decrease in the frequency of cybercrimes in Malaysia.

5.5 Limitations of The Study

The limitations of the study refer to the specific design or method aspects that affected the applicability or comprehension of the study's findings. The restrictions on the generalizability and accessibility of findings arise from the study's design choices and the methods employed to demonstrate internal and external validity (Theofanidis & Fountouki, 2018). These limits may arise from a variety of sources, including methodological, data-related, theoretical, resource-related, and generalizability-related factors.

Every research, including this particular one, contains inherent limitations. Two limitations must be considered when conducting this research. Firstly, this study has discovered there is a methodological limitation in terms of sample size as it mainly focuses on students in the UMK city campus, excluding students from the Jeli campus and Bachok campus. For this study, the researcher strictly selected students as respondents. While the data on cyber security awareness is comprehensive for all citizens, this study is specifically limited to students at the UMK city campus. Therefore, the researcher is unable to thoroughly analyze the overall level of cyber security awareness in Islamic digital banking. This demonstrates the presence of a limitation in the sample size of this research.

On top of that, a further limitation identified in this study is the researcher's exclusive emphasis on undergraduates only within the UMK city campus. This means that the postgraduates are excluded from being considered as respondents. Consequently, this study is limited in terms of age. It is evident from the respondents' results that there are no respondents aged 27 and above. By including postgraduates into the survey, the likelihood of obtaining students aged 27 years and older is higher. What is the significance of age in conducting an online questionnaire? This is due to variations in life experiences among distinct age groups. Furthermore, Gigliotti and Dietsch (2014) noted that several studies indicate a greater likelihood for elderly adults to comply with survey inquiries. When the elderly population is more inclined to answer surveys, researchers can collect response data more quickly without having to wait for an extended period. This will shorten the process and reduce the time required for data collecting. Therefore, engaging postgraduates into the online questionnaire can prove really advantageous.

Lastly, meeting the stipulated time range for this study is challenging due to the scarcity of prior research that is comparable to this one. Due to the challenges encountered in gathering enough data, this study has limited applicability as a primary source for future research. Nevertheless, the researcher employed multiple references to enhance the resilience of research, making it a valuable additional resource for future researchers. Due to this limitation, this study is less functional as a main source.

5.6 Recommendations for Future Research

There are several recommendations to address the deficiencies in this research for future researchers who might explore topics related to this subject. The allocated time for this research project is really limited. In future research endeavors exploring similar topics,

researchers with plenty of time at their fingertips may choose to apply a combination of quantitative and qualitative research methodologies. By combining these two methodologies, researchers can obtain a broader perspective compared to a single quantitative or qualitative study, as it allows for an incorporation of the advantages offered by both techniques. This technique improves the reliability and precision of the findings while also enabling the collection of respondents' data in a more efficient and fast manner.

Additionally, this survey encompassed a mere 371 respondents, predominantly consisting of students from various programs and faculties at the UMK city campus. Researchers might suggest future researchers expand both the scope of their studies and the sample size by incorporating various locations or countries. Future researchers may also widen their study's scope to include people of all ages, from young to elderly. This is because future researchers will recognize the differing levels of cyber security awareness in Islamic digital banking among age groups. Reliability, validity, and relevance of the results will increase with a greater proportion of respondents due to the numerous factors that influence the level of cyber security awareness in Islamic digital banking. Consequently, researchers will have a chance to deliver more precise test outcomes.

Finally, this study primarily focused on four key factors which are knowledge of technology, social media information, experience and attitude. Therefore, researchers are expecting that future research will incorporate an additional variable to enhance their contribution to related organizations that focus on strengthening cyber security. According to a 2022 survey on internet users in Malaysia, Statista reported that over 66% of respondents indicated their utilization of online banking. Additionally, the adoption of digital banking is increasing in the Southeast Asian nation. In the same year, the total worth of internet banking transactions in Malaysia exceeded 1 trillion MYR. Hence, it is

anticipated that the ongoing rise in the number of individuals falling victim to cybercrime and experiencing cyber-attacks. Thus, forthcoming researchers can utilize this study to enhance the provision of strengthened safety in the context of cyber security. As a result, the improvements implemented by forthcoming researchers have the potential to minimize the number of individuals affected by cybercrime in the future.

5.7 Overall Conclusion of The Study

The objective of this research is to analyze and investigate the factors that influence the level of cyber security awareness in Islamic digital banking among UMK city campus students. The findings of this study indicate that four distinct factors, namely knowledge of technology, social media information, attitude, and experience, significantly influence the level of awareness regarding cyber security in Islamic digital banking. The outcomes of this research were acquired via questionnaires that were conducted through the Google Form platform. The respondents of the study consisted of all undergraduate students in UMK city campus, comprising all programs and faculties. The total number of respondents is 371, with 66.8% female and 33.2% male.

The research results and findings were obtained through the utilization of the Statistical Package for Social Science (SPSS) software to perform reliability analysis. The Pearson correlation coefficient is employed for data interpretation, and the final results indicate a positive correlation between the independent variables and the dependent variable. The last chapter has addressed the implications and limitations of this study to clarify the significance and short comings that were encountered during the project. This chapter also emphasized its recommendations for futureresearch to improve their findings in future studies.

In a nutshell, an analysis was to evaluate the influence of knowledge of technology, social media information, attitude, and experience on the level of cyber security awareness among UMK city campus students. As a result, all of the research objectives have been successfully achieved, and all of the hypotheses have been fulfilled to achieve.

REFERENCES

Ababa, A. (2018). Dashen Bank Launches "AMOLE," the New Ethiopian Digital Wallet. https://www.prweb.com/releases/dashen_bank_launches_amole_the_new_ethiopian digital_wallet/prweb15648028.htm

Abdul Rais, N. A., Mohd Yusop, N., Sabtu, S. N., & Shamsul Bahrin, N. E. E. (2022). Cashless society in campus: student's usage and level of awareness. *Voice of Academia (VOA)*, *18*(1), 58-66.

Adamu, A. G., Maheyzah, M. S., & Othman, S. H. (2022). An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. *International Journal of Electrical and Computer Engineering, 12*(1), 572-584. https://doi.org/10.11591/ijece.v12i1.pp572-584

Agarwal, S. and Chua, Y.H. (2020), "FinTech and household finance: a review of the empirical literature", China Finance Review International, 10 (4), 361-376.

Aisyah, M. (2018). Islamic Bank Service Quality and Its Impact on Indonesian Customers' Satisfaction and Loyalty. *10*, 367-388. https://doi.org/10.15408/aiq.v10i2.7135

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211. https://doi.org/https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior / Icek Ajzen, Martin Fishbein* (Paperback ed.). Prentice-Hall.

Al-Janabi, Samaher & AlShourbaji, Ibrahim. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information & KnowledgeManagement*. 15.

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of advances in information technology*, *3*(3), 176-183.

Altmann, T. (2008). Attitude: A Concept Analysis. *Nursing forum*, 43, 144-150. https://doi.org/10.1111/j.1744-6198.2008.00106.x

Askar, P., & Mazman, S. G. (2013). Adaptation of online information searching strategy inventory into Turkish. *Egitim ve Bilim*, *38*(168).

Bada, M., Sasse, A., & Nurse, J. (2015). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?*

Baumeister, R. F., & Leary, M. R. (1997). Writing Narrative Literature Reviews. *Review of General Psychology*, *1*(3), 311-320. https://doi.org/10.1037/1089-2680.1.3.311

Bello, N., Haque, M., Adeyemi, A. A., & Hasan, A. (2017). Maqāṣid Al-Sharī'ah and the Online Banking System: Implications for Service Delivery. *International Journal of Fiqh and Usul al-Fiqh Studies*, *469*(6082), 1-9

Benisch, M., Kelley, P., Sadeh, N., & Cranor, L. (2011). Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs. *Personal and Ubiquitous Computing*, *15*, 679-694. https://doi.org/10.1007/s00779-010-0346-0

Bernama. (2022, April 29). *Islamic Digital Bank to be operational within 2 years, says Aeon Credit*. BERNAMA. https://bernama.com/en/business/news.php?id=2077236

Bernama. (2022, September 20). NSC: Cyber Security Awareness master plan to be ready next year. https://api.nst.com.my/news/nation/2022/09/832884/nsc-cyber-security-awareness-master-plan-be-ready-next-year

Bernama. (2023, March 17). Malaysia faces increasing cybersecurity threats - teo - new straits times.https://www.nst.com.my/news/nation/2023/03/890120/malaysia-faces-increasing-cybersecurity-threats-teo

Bhardwaj P. (2019). Types of sampling in research. *Journal of the Practice of*

Cardiovascular Sciences, 5(3), 157. DOI: 10.4103/jpcs.jpcs_62_19
Bhat, A. (2023b). Data Collection: What It Is, Methods & Tools + Examples. *QuestionPro*. https://www.questionpro.com/blog/data-collection/
Bozeman, B. (2000). Technology transfer and public policy: a review of research and theory. *Research Policy*, *29*(4), 627-655. https://doi.org/https://doi.org/10.1016/S0048 7333(99)00093-1
Bruvold, W. H. (1980). Are beliefs and behaviour consistent with attitudes? A preliminary restatement and some evidence from a survey research project
Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications, 42*, 36-45. https://doi.org/https://doi.org/10.1016/j.jisa.2018.08.002
Carminati, B., Ferrari, E., Heatherly, R., Kantarcioglu, M., & Thuraisingham, B. (2011). Semantic web-based social network access control. *Computers & Security*, *30*, 108-115. https://doi.org/10.1016/j.cose.2010.08.003
Chai, C., Koh, J., & Tsai, C.-C. (2010). Facilitating Preservice Teachers' Development of Technological, Pedagogical, and Content Knowledge (TPACK). *Educational Technology & Society, 13*, 63-73.
Chauhan, S., Akhtar, A. and Gupta, A. (2022), "Customer experience in digital banking: a review and future research directions", International Journal of Quality and Service Sciences, 14 (2), 311-348.
Chiu, C.-M., Hsu, M.-H., Sun, S.-Y., Lin, T.-C., & Sun, P.-C. (2005). Usability, quality, value and e-learning continuance decisions. *Computers & Education*, *45*, 399-416. https://doi.org/10.1016/j.compedu.2004.06.001
Chu, S.-C. (2011).Viral advertising in social media: Participation in Facebook groups and responses among college-aged users. *Journal of Interactive Advertising*, *12*, 30-43.
Chung, N., Han, H., Koo, C., 2015. Adoption of travel information in user-generated content on social media: the moderating effect of social presence. Behav. Inform. Technol. 34 (9), 902–919. https://doi.org/10.1080/0144929x.2015.1039060.
Das, R., & Patel, M. (2017). Cyber Security for Social Networking Sites: Issues, Challenges and Solutions. *International Journal for Research in Applied Science and Engineering Technology*, *V*, 833-838. https://doi.org/10.22214/ijraset.2017.4153
Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International journal of engineering sciences & Emerging technologies*, *6*(2), 142-153.
Dawami, Q. (2020). Factors Influencing the Preference of Customers Towards Islamic Banking: Evidence from Malaysia. *Journal of Islamic Economic Laws*, *3*, 48-67. https://doi.org/10.23917/jisel.v3i1.10191
Duggan, A., Hess, B., Morgan, D., Kim, S., & Wilson, K. (2001). Measuring Students' Attitudes toward Educational Use of the Internet. *Journal of Educational Computing Research*, *25*, 267-281. https://doi.org/10.2190/GTFB-4D6U-YCAX-UV91
Epstein, J. (2017). Two Faces to a Cashless Future. American Bankers Association (ABA). *Banking Journal*.
Farag, S., Lyons, G. (2010). Explaining public transport information use when a car is available: Attitude theory empirically investigated. Transportation 37 (6), 897–913. https://doi.org/10.1007/s11116-010-9265-1.
Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behaviour: An introduction to theory and research* (Vol. 27).
Fleetwood, D. (2023). Sample Size Determination: Definition, Formula, and Example. QuestionPro. https://www.quetsionpro.com/blog/determining-sample-size/#:~:text=What%20is%20Sample%20Size%3F,can%20be%20vague%20or%20specific.

Gregor, S. (2002). A Theory of Theories in Information Systems. *Information Systems Foundations: Building the Theoretical Base*.

Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quarterly*, *30*, 611-642. https://doi.org/10.2307/25148742

Gross, M., Canetti, D., & Vashdi, D. (2016). *Cyber Terrorism: Its Effects on Psychological Well Being, Public Confidence and Political Attitudes*.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346. https://doi.org/https://doi.org/10.1016/j.heliyon.2017.e00346

Hadlington, L. (2018). Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology*, *12*, 269-281. https://doi.org/10.5281/zenodo.1467909

Hair, J. F. Jr., Babin, B., Money, A. H., & Samouel, P. (2003). Essential of business research methods. John Wiley & Sons: United States of America.

Hale, J. L., Householder, B. J., & Greene, K. L. (2002). The theory of reasoned action. *The persuasion handbook: Developments in theory and practice*, *14*(2002), 259-286.

Haralayya, B. (2021). How Digital Banking has brought innovative products and services to India. *Journal of Advanced Research in Quality Control and Management*, *6*(1), 16-18.

Hussain, Z., Das, D., Bhutto, Z.A., Hammad-u-Salam, M., Talpur, F., & Rai, G. (2017). E-Banking Challenges in Pakistan: An Empirical Study. *Journal of Computational Chemistry, 5*, 1-6.

Hyun-Soo, C., Roger Loh. (2020). Physical frictions and digital banking adoption. *ManagementScience,forthcoming*. https://doi.org/https://ssrn.com/abstract=3333636 or http://dx.doi.org/10.2139/ssrn.3333636

IFG Staff Writers (2022, May 31). *European Islamic Digital Banks - analysis*. Islamic Finance Guru. https://www.islamicfinanceguru.com/articles/european-islamic-digital-banks-analysis

Info UPU (2020, October 24). *Senarai Ua Universiti Awam Di Malaysia*. https://www.infoupu.com/senarai-ua-universiti-awam-di-malaysia/

Ion, I., Reeder, R., & Consolvo, S. (2015). "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices.

Izuagbe, R. (2021). Faculty research performance expectancy of online databases: system design characteristics as facilitating conditions. *The Journal of Academic Librarianship*, *47*, 102318. https://doi.org/10.1016/j.acalib.2021.102318

Kamali, M. H. (2008a). Maqasid Al-Shariah Made Simple. *The International Institute of Islamic Thought (IIIT)*.

Kankanhalli, A., Tan, B.C., Wei, K.K. (2005). Contributing knowledge to electronic knowledge repositories: An empirical investigation. MIS Quarterly 29 (1), 113–143.

Kawulich, B. (2009).The Role of Theoryin Research. In (pp.37). https://www.researchgate.net/publication/201834276_The_Role_of_Theory_in_Research

Kovacevic, A., Putnik, N., & Toskovic, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Access,8*, 125140-125148. https://doi.org/10.1109/ACCESS.2020.3007867

Kraut, R., Patterson, M., Lundmark, V., Kiesler, S., Mukopadhyay, T., & Scherlis, W. (1998). Internet Paradox: A Social Technology That Reduces Social Involvement and Psychological Well-Being? *The American psychologist, 53*, 1017-1031. https://doi.org/10.1037/0003-066X.53.9.1017

Kristina Dervojeda, D. V., Fabian Nagtegaal, Mark Lengton, Elco Rouwmaat, PwC, & Netherlands, a. L. P., Erica Monfardini & Laurent Frideres, PwC Luxembourg. (2014). Innovative Business Models: Supply chain finance. *Business Innovation Observatory European Union.*

Kumar, S., & Somani, D. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. *International Journal of Advance Research in Computer Science and Management*, *4*, 125-129.

Lahsasna, A. (2009). *Maqasid Al Shariah in Islamic Economics and Finance*.https://www.researchgate.net/publication/321746623_Maqasid_Al_Shariah in_Islamic_Economics_and_Finance

Lan, P., & Young, S. (1996). International technology transfer examined at technology component level: a case study in China. *Technovation*, *16*(6), 277-286. https://doi.org/https://doi.org/10.1016/0166-4972(96)00005-3

Laugwitz, B., Held, T., Schrepp, M. (2008). Construction and Evaluation of a User Experience Questionnaire. In: Holzinger, A. (eds) HCI and Usability for Education and Work. USAB 2008. *Lecture Notes in Computer Science*, vol 5298. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-89350-9_6

Law, E. L.-C., Roto, V., Hassenzahl, M., Vermeeren, A. P., & Kort, J. (2009). Understanding, scoping and defining user experience: a survey approach. Proceedings of the SIGCHI conference on human factors in computing systems,

Leong, L.-Y., Hew, T.-S., Ooi, K.-B., Lee, V.-H., & Hew, J.-J. (2019). A hybrid SEM-neural network analysis of social media addiction. *Expert Systems with Applications*, *133*, 296-316. https://doi.org/https://doi.org/10.1016/j.eswa.2019.05.024

Liao, Z., & Cheung, M. (2002). Internet-based e-banking and consumer attitudes: An empirical study. *Information & Management*, *39*, 283-295. https://doi.org/10.1016/S0378-7206(01)00097-0

Madden, M. (2012). Privacy management on social media sites. *Pew Research Centre* https://www.pewresearch.org/internet/2012/02/24/privacy-management-on-social-media-sites/

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and social psychology Bulletin*, *18*(1), 3-9.

Meikeng, Y. (2020). Cybersecurity cases rise by 82.5 percent. *thestar*. https://www.mef.org.my/MEFITN/Star20200412a.pdf

MIT. (2011). The Future of the Electric Grid: An Interdisciplinary MIT Study. *Massachusets Institute of Technology*. http://web.mit.edu/mitei/research/studies/documents/electric-grid 2011/Electric_Grid_Full_Report.pdf

Mouza, M. (2018). WHAT IS THEORY? https://doi.org/10.13140/RG.2.2.28009.34406

Mullins, C. (2015). *Responsive, mobile app, mobile first: untangling the UX design web in practical experience* Proceedings of the 33rd Annual International Conference on the Design of Communication, Limerick,Ireland. https://doi.org/10.1145/2775441.2775478

Nadda, V., Dadwal, S., & Firdous, A. (2015). Social Media Marketing. In (pp. 359-379). https://doi.org/10.4018/978-1-4666-8353-2.ch021

Norman, D. (2002). *The design of everyday things: Revised and expanded edition*. Basic books.

Novi, M. (2020). Konsep Fintech Lending Dalam Perspektif Maqāṣid Syarī'ah. *Islamic Economics Journal*, *6*, 101. https://doi.org/10.21111/iej.v6i1.4591

Oladapo, I, Hamoudah, M, Alam, MM, Olaopa, OR, & Muda, R. (2022). Customers' Perceptions of FinTech Adaptability in the Islamic Banking Sector: Comparative study on Malaysia and Saudi Arabia. *Journal of Modelling in Management*, 17(4), 1241-1261. (online) https://doi.org/10.1108/JM2-10-2020-0256

Omniconvert. (2023, May 11). *What is Sample Size? Definition - Omniconvert*. https://www.omniconvert.com/what-is/sample-size/

Panchanatham, D. N. (2015). A case study on Cyber Security in E-Governance. *International Research Journal of Engineering and Technology*.

Petrosyan, A. (2023, February 23). *Number of internet users worldwide 2022*. Statista. https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/#:~:text=As%20of%202022%2C%20the%20estimated,66%20percent%20of%20global%20population.

Pio, P., Fonseca Albuquerque Cavalcanti Sigahi, T., Rampasso, I., Satolo, E., Serafim, M., Quelhas, O., Filho, W., & Anholon, R. (2023). Complaint management: comparison between traditional and digital banks and the benefits of using management systems for improvement. *International Journal of Productivity and Performance Management*. https://doi.org/10.1108/IJPPM-08-2022-0430

Piskorski, M. J. (2016). *A social strategy: How we profit from social media*. Princeton University Press.

Rahman, N. A. A., Sairi, I., Zizi, N., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology, 10*(5), 378-382.

Raza, S. A., Shah, N., & Ali, M. (2019). Acceptance of mobile banking in Islamic banks: evidence from modified UTAUT model. *Journal of Islamic Marketing, 10*(1), 357-376. https://doi.org/10.1108/JIMA-04-2017-0038

Reddy, N. M., & Zhao, L. (1990). International technology transfer: A review. *Research Policy, 19*(4), 285-307. https://doi.org/https://doi.org/10.1016/0048-7333(90)90015-X

Research Design, Feature of a Good Research Design. (2020, February 12). Theintactone. https://theintactone.com/2019/03/03/brm-u2-topic-1-research-design-feature-of-a-good-research-design/comment-page-1/

Ruby, D. (2023, April 7). *Internet user statistics in 2023 - (Global Data & Demographics)*. Demand Sage. https://www.demandsage.com/internet-user-statistics/

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

Sardana, V. (2018). Digital Technology in the Realm of Banking: A Review of Literature.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law, 12*(2), 8.

Shea, S., Gillis, A. S., & Clark, C. (2023, January 11). *What is cybersecurity? everything you need to know: TechTarget*. Security. https://www.techtarget.com/searchsecurity/definition/cybersecurity

Singh, N., Sinha, N., & Liébana-Cabanillas, F. J. (2020). Determining factors in the adoption and recommendation of mobile wallet services in India: Analysis of the effect of innovativeness, stress to use and social influence. *International Journal of Information Management, 50*, 191-205.

Singh, S. (2003). Simple random sampling. In advanced sampling theory with applications (pp. 71-136). *Springer*, Dordrecht.

Smitherson, D. (2012). Impact of Cyber Crime and Security on Social Media. https://www.socialmediatoday.com/content/impact-cyber-crime-and-security-

social-media
Statista Research Department (2023, February 27). *Malaysia: Cybercrime incidents 2022*. Statista.https://www.statista.com/statistics/1043272/malaysia-cyber-crime-incidents/
Swar, B., & Hameed, T. (2017). Fear of Missing out, Social Media Engagement, Smartphone Addiction and Distraction: Moderating Role of Self-Help Mobile Apps-based Interventions in the Youth. *HEALTHINF*, *1*, 139-146.
Tan, J., Salim, Z., Tang, H., Sivakumar, Y., Hassan, H., Khaw, C., & Sabrina, S. (2022, May 23). *BNM has announced its 5 digital banks, here's what they'll bring to the table*. Vulcan Post. Retrieved May 6, 2023, from https://vulcanpost.com/786887/bank-negara-malaysia-digital-banking-licence-malaysia-companies/
Teo, T., & Schaik, P. v. (2012). Understanding the Intention to Use Technology by Preservice Teachers: An Empirical Test of Competing Theoretical Models. *International Journal of Human–Computer Interaction*, *28*, 178 - 188.
Tonge, A. M., Kasture, S. S., & Chaudhari, S. R. (2013). Cyber security: challenges for society-literature review. *IOSR Journal of computer Engineering*, *2*(12), 67-75.
Twenge, J. M., & Campbell, W. K. (2019). Media Use Is Linked to Lower Psychological Well-Being: Evidence from Three Datasets. *Psychiatric Quarterly*, *90*(2), 311-331. https://doi.org/10.1007/s11126-019-09630-7
Van Deursen, A. J., van der Zeeuw, A., de Boer, P., Jansen, G., & van Rompay, T. (2021). Digital inequalities in the Internet of Things: differences in attitudes, material access, skills, and usage. *Information, Communication & Society*, *24*(2), 258-276.
Wikimedia Foundation. (2023b, May 10). *Awareness*. Wikipedia. https://en.wikipedia.org/wiki/Awareness
Yerby, J., Koohang, A., & Paliszkiewicz, J. (2019). Social media privacy concerns and risk beliefs. *Online Journal of Applied Knowledge Management*, *7*, 1-13. https://doi.org/10.36965/OJAKM.2019.7(1)1-13
Zwilling, Moti & Klien, Galit & Lesjak, Dusan & Wiechetek, Łukasz & Çetin, Fatih & Basım, H. Nejat. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*. 62. 82-97

APPENDIX A

DRAFT OF QUESTIONNAIRE

SECTION A: DEMOGRAPHIC PROFILE

Gender

	Male
	Female

Age

	18 – 20 years old
	21 – 23 years old
	24 – 26 years old
	27 years old and above

Current year of study

	Year 1
	Year 2
	Year 3
	Year 4

Faculty

	Faculty of Entrepreneurship and Business (FKP)
	Faculty of Hospitality, Tourism and Wellness (FHPK)
	Faculty of Data Science and Computing (FSDK)

Programme

	Bachelor of Business Administration (Islamic Banking and Finance) with Honours - SAB
	Bachelor of Entrepreneurship (Commerce) with Honours - SAK
	Bachelor of Entrepreneurship with Honours - SAE
	Bachelor of Entrepreneurship (Logistics and Distributive Trade) with Honours - SAL
	Bachelor of Entrepreneurship (Retailing) with Honours - SAR
	Bachelor of Accounting with Honours - SAA
	Bachelor of Entrepreneurship (Tourism) with Honours - SAP
	Bachelor of Entrepreneurship (Hospitality) with Honours - SAH
	Bachelor of Entrepreneurship (Wellness) with Honours - SAS
	Bachelor of Information Technology with Honours - SST

SECTION B: CYBER SECURITY AWARENESS

The item below represent the level of cyber security awareness. Please tick your rating based on the scale below:

1. Strongly Disagree
2. Disagree
3. Neutral
4. Agree
5. Strongly Agree

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I am aware with the term cyber security					
I am aware of email/message from unfamiliar sender and decide to not open it					
I am aware of using backup software to back up my important data					
I am aware of Islamic digital banking service that expose to cyber security risk					
Cyber security risk includes phishing and malware					

SECTION C: KNOWLEDGE

The item below represent your knowledge of technology, information, experience and attitude of internet users. Please tick your rating based on the scale below:

1. Strongly Disagree
2. Disagree
3. Neutral
4. Agree
5. Strongly Agree

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
My skill and knowledge in Islamic digital banking service is limited					
My skill and knowledge in cyber security awareness is limited					
I have knowledge to use Islamic Digital Banking services					
I know it is better to use Islamic digital banking in conducting my banking activities					
I am interested to know more about Islamic digital banking services					

SECTION D: INFORMATION

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The information about cyber security awareness guide me to solve the difficulties on Islamic digital banking services					
I am cautious about receiving phishing attempts or email scams aimed at stealing my personal information					
Bank's cyber security notification help enhance the security of my account					
Islamic digital banking consistently reminds me to stay alert from potential cyber security					
I regularly change my password on digital banking services to avoid unauthorized access and enhance security					

SECTION E: EXPERIENCE

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I will never provide my personal information whenever I received calls from personal numbers that declare themselves from banking organization					
For me, the Islamic digital banking services platform can be trusted all the time					
The Islamic digital banking services provides easy to access the platform					
The Islamic digital banking services will not simply withdraw my money					
The Islamic digital banking services has a high level of integrity					

SECTION F: ATTITUDE

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I would prefer using digital banking rather than traditional banking					
I will feel confident when I use the Islamic Digital Banking services for my transaction					
I believe using digital banking transaction is a highly secured					
The Islamic digital banking services platform makes the transactions faster and reliable					
Islamic digital banking services is user friendly					

The number of student in Faculty of Entrepreneurship and Business

UNIVERSITI MALAYSIA KELANTAN
ENROLMEN PELAJAR AKTIF IJAZAH SARJANA MUDA SESI 2022/2023
(Mengikut Program dan Semester Pengajian)

			Semester 2			Semester 3		Semester 4			Semester 5			Semester 6			Semester 7			Semester 8			Semester 9			Semester 10			Semester 11			Semester 12			Jumlah		
			L	P	Jum	L	Jum	L	P	Jum	L	P	Jum	L	P	Jum	L	P	Jum	L	P	Jum	L	P	Jum	L	P	Jum	L	P	Jum	L	Jum	L	P	Jum
FAKULTI KEUSAHAWANAN DAN PERNIAGAAN	SAA -	B. Accounting (Hons)	22	67	89			2	16	18	5	13	18	1		1																		24	96	124
	SAB -	BBA. (Hons) (Islamic Bank & Fin)	46	166	212			37	161	198		3	3	34	164	198				40	158	198	2	2	4	4	4	8						163	658	821
	SAE -	B.Ent. (Hons)	11	36	47			18	32	50				14	32	46				12	44	56		1	1		2	2						55	147	202
	SAK -	B. Ent. (Hons.) (Commerce)	45	133	178	2	2	40	137	188				56	159	215		2	2	64	159	223		1	1	4	3	7	1	1	2			221	595	816
	SAL -	B. ENT. (HONS) (LOGISTIC)	50	138	188			56	141	200		1	1	56	151	207				73	142	215	1		1	1		1						340	573	913
	SALB -		2	9	11			1		1				3	2	5																		6	11	17
	SAR -	B. Ent. (Hons) (Retailing)	42	136	178			50	138	188		2	2	36	148	184	2	12	14	48	116	164	1	3	4	2	4	6				1	1	182	559	741
		Jumlah Fakulti	218	685	903	2	2	216	625	841	5	19	22	200	696	896	2	14	16	237	619	856	4	7	11	11	13	24	1	1	2	1	1	895	2639	3534
		Jumlah Keseluruhan	218	685	903	2	2	216	625	841	5	19	22	200	696	896	2	14	16	237	619	856	4	7	11	11	13	24	1	1	2	1	1	895	2639	3534

The data of Faculty Hospitality, Tourism and Wellness

UNIVERSITI MALAYSIA KELANTAN
ENROLMEN PELAJAR AKTIF IJAZAH SARJANA MUDA SESI 2022/2023
(Mengikut Program dan Semester Pengajian)

			Semester 1			Semester 2			Semester 3		Semester 4			Semester 5		Semester 6			Semester 7			Semester 8			Semester 9		Semester 10			Jumlah		
			L	P	Jum	L	P	Jum	P	Jum	L	P	Jum	L	Jum	L	P	Jum	L	P	Jum	L	P	Jum	P	Jum	L	P	Jum	L	P	Jum
FAKULTI HOSPITALITI, PELANCONGAN DAN KESEJAHTERAAN	SAH -	B.Ent. (Hons)(Hospitality)				40	146	186			38	131	169			30	123	153	4	2	6	30	135	165						142	537	679
	SAP -	B. Ent. (Hons.)(Tourism)	7	17	24	52	279	361	1	1	65	244	329	1	1	70	229	299		3	3	79	218	297	1	1	2	1	3	326	993	1319
	SAS -	B.ENT. (HONS) (WELLNESS)				51	162	213	1	1	28	137	165	1	1	18	132	150		4	4	24	127	151						122	563	685
		Jumlah Fakulti	7	17	24	173	587	760	2	2	151	512	663	2	2	118	484	602	4	9	13	133	480	613	1	1	2	1	3	590	2093	2683
		Jumlah Keseluruhan	7	17	24	173	587	760	2	2	151	512	663	2	2	118	484	602	4	9	13	133	480	613	1	1	2	1	3	590	2093	2683

APPENDIX B

GANTT CHART (PPTA 1)

Week / Activities	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Distribution of PPTA activities, guidelines and rubrics															
Students meeting with supervisor Briefing of PPTA I															
Database searching and reference manager class at the library															
Discussion and selection research topic Discussion Chapter 1 : Introduction															
Starting up to writing for chapter 1 & 2															
Continue writing in chapter 2 & 3 Review correction for chapter 1 until 3															
Final review of the research project proposal draft															
Submission of proposal draft to supervisor															

Correction of the draft proposal															
Submission report to supervisor and examiner															
Online presentation															
Final editing of the proposal															

GANTT CHART (PPTA II)

Activities \ Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Division of groups, supervisors and examiners for certain groups															
Briefing of PPTA II															
Preparation for data collection															
Distribute questionnaire and collect data															
Start writing for chapter 4															
Proceed writing for chapter 5															
Writing final reports and posters															
Submission of proposals and posters to the supervisor for review purposes															
Send a soft copy of the poster to the supervisor for review and correction															

Send the complete poster in Google drive to supervisors, evaluators and PPTA coordinators															
Continuation of writing final reports and papers in the final stage															
Preparation of the poster presentation to the physical colloquium															
Physical Colloquium Poster Presentation															
Submission of the draft Final Report of the Research Project and Article to the supervisor.															
Final editing of the proposal															
Collection of final report to PPTA2 coordinator															

UNIVERSITI MALAYSIA KELANTAN

FAKULTI KEUSAHAWANAN DAN PERNIAGAAN
UNIVERSITI MALAYSIA KELANTAN

BORANG KELULUSAN PENYERAHAN
LAPORAN AKHIR PROJEK PENYELIDIKAN TANPA JILID

Kepada,

Dekan,
Fakulti Keusahawanan dan Perniagaan
Universiti Malaysia Kelantan

Kelulusan Penyerahan Draf Akhir Laporan Akhir Projek Penyelidikan Tahun Akhir Tanpa Jilid

Saya, **Dr Ahmad Ridhuwan bin Abdullah** penyelia kepada pelajar berikut, bersetuju membenarkan penyerahan dua (2) naskah draf akhir Laporan Akhir Projek Penyelidikan Tahun Akhir tanpa jilid untuk pentaksiran.

Nama Pelajar: AMIRAH FADHLINA BINTI AZAHAR	**No Matrik: A21B2390**
Nama Pelajar: NUR HIDAYAH BINTI MOHD ZAKI	**No Matrik: A21B3378**
Nama Pelajar: NURUL AFIQAH BINTI MAZENEE	**No Matrik: A21B3407**
Nama Pelajar: NURULAIN AQILAH BINTI HALIZAN	**No Matrik: A21B3496**

Tajuk Penyelidikan:

THE CYBER SECURITY AWARENESS OF ISLAMIC DIGITAL BANKING AMONG UMK CITY CAMPUS STUDENTS

Sekian, terima kasih

A Ridhuwan

Tandatangan Penyelia

Tarikh:

Universiti Malaysia KELANTAN	**REKOD PENGESAHAN PENYARINGAN *TURNITIN*** ***VERIFICATION RECORD OF TURNITIN SCREENING***

Kod/Nama Kursus*:* AFS4112
Code/ Course Name: PROJEK PENYELIDIKAN (PERBANKAN DAN KEWANGAN ISLAM II)
Sesi/*Session:* September 2023/2024
Semester*:* 5
Nama Program/*Name of Programme:* SAB
Fakulti/Pusat/*Faculty/Centre:* Fakulti Keusahawanan Dan Perniagaan/ *Faculty of Entrepreneurship and Business*

Pengesahan Penyaringan Plagiat/ *Verification of Plagiarism Screening*

Saya, **AMIRAH FADHLINA BINTI AZAHAR** (Nama), No.Matrik **A21B2390** dengan ini mengesahkan Kertas Projek Penyelidikan ini telah melalui saringan aplikasi turnitin. Bersama ini dilampirkan sesalinan laporan saringan Turnitin dengan skor persamaan sebanyak 26%.

*I, **AMIRAH FADHLINA BINTI AZAHAR** (Name), Matrix number **A21B2390** hereby declare that I have screen my thesis using Turnitin Software. Enclosed here with a copy of verification of Turnitin screening with similarity score of 26%.*

Tajuk Kertas Kerja Penyelidikan/ *The Tittle of Research Project Paper*:-

THE CYBER SECURITY AWARENESS OF ISLAMIC DIGITAL BANKING AMONG UMK CITY CAMPUS STUDENTS

Tandatangan/*Signature*

af

……

Nama Pelajar/*Student Name*: AMIRAH FADHLINA BINTI AZAHAR

No.Matrik/*Matrix No*: A21B2390

Tarikh/*Date*: 10/1/2024

Pengesahan Penyelia/*Supervisor*: Tandatangan/*Signature:* Tarikh/*Date:*

ORIGINALITY REPORT

26%	20%	11%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

ASSESSMENT FORM FOR FINAL YEAR RESEARCH PROJECT: RESEARCH REPORT (Weight 50%)
(COMPLETED BY SUPERVISOR AND EXAMINER)

Student's Name: AMIRAH FADHLINA BINTI AZAHAR **Matric No: A21B2390**
NUR HIDAYAH BINTI MOHD ZAKI **A21B3378**
NURUL AFIQAH BINTI MAZENEE **A21B3407**
NURULAIN AQILAH BINTI HALIZAN **A21B3496**
Name of supervisor: DR AHMAD RIDHUWAN BIN ABDULLAH **Name of programme: SAB**
Research Topic: THE CYBER SECURITY AWARENESS OF ISLAMIC DIGITAL BANKING AMONG UMK CITY CAMPUS STUDENTS

NO.	CRITERIA	PERFORMANCE LEVEL				WEIGHT	TOTAL
		POOR (1 MARK)	FAIR (2 MARKS)	GOOD (3 MARKS)	EXCELLENT (4 MARKS)		
1.	**Content (10 MARKS)** (Research objective and Research Methodology in accordance to comprehensive literature review) Content of report is systematic and scientific (Systematic includes Background of study, Problem Statement, Research Objective, Research Question) (Scientific refers to researchable topic)	Poorly clarified and not focused on Research objective and Research Methodology in accordance to comprehensive literature review.	Fairly defined and fairly focused on Research objective and Research Methodology in accordance to comprehensive literature review.	Good and clear of Research objective and Research Methodology in accordance to comprehensive literature review with good facts.	Strong and very clear of Research objective and Research Methodology in accordance to comprehensive literature review with very good facts.	____ x 1.25 (Max: 5)	
		Content of report is written unsystematic that not include Background of study, Problem Statement, Research Objective, Research Question and unscientific with unsearchable topic.	Content of report is written less systematic with include fairly Background of study, Problem Statement, Research Objective, Research Question and less scientific with fairly researchable topic.	Content of report is written systematic with include good Background of study, Problem Statement, Research Objective, Research Question and scientific with good researchable topic.	Content of report is written very systematic with excellent Background of study, Problem Statement, Research Objective, Research Question and scientific with very good researchable topic.	____ x 1.25 (Max: 5)	

ASSESSMENT FORM FOR FINAL YEAR RESEARCH PROJECT: RESEARCH REPORT (Weight 50%)
(COMPLETED BY SUPERVISOR AND EXAMINER)

2.	**Overall report format (5 MARKS)**	***Submit according to acquired format***	The report is not produced according to the specified time and/ or according to the format	The report is produced according to the specified time but fails to adhere to the format.	The report is produced on time, adheres to the format but with few weaknesses.	The report is produced on time, adheres to the format without any weaknesses.	____ x 0.25 (Max: 1)	
		Writing styles (clarity, expression of ideas and coherence)	The report is poorly written and difficult to read. Many points are not explained well. Flow of ideas is incoherent.	The report is adequately written; Some points lack clarity. Flow of ideas is less coherent.	The report is well written and easy to read; Majority of the points is well explained, and flow of ideas is coherent.	The report is written in an excellent manner and easy to read. All of the points made are crystal clear with coherent argument.	____ x 0.25 (Max: 1)	
		Technicality (Grammar, theory, logic and reasoning)	The report is grammatically, theoretically, technically and logically incorrect.	There are many errors in the report, grammatically, theoretically, technically and logically.	The report is grammatically, theoretically, technically and logically correct in most of the chapters with few weaknesses.	The report is grammatically, theoretically, technically, and logically perfect in all chapters without any weaknesses.	____ x 0.25 (Max: 1)	
		Reference list (APA Format)	No or incomplete reference list.	Incomplete reference list and/ or is not according to the format.	Complete reference list with few mistakes in format adherence.	Complete reference list according to format.	____ x 0.25 (Max: 1)	
		Format organizing (cover page, spacing, alignment, format structure, etc.)	Writing is disorganized and underdeveloped with no transitions or closure.	Writing is confused and loosely organized. Transitions are weak and closure is ineffective.	Uses correct writing format. Incorporates a coherent closure.	Writing include a strong beginning, middle, and end with clear transitions and a focused closure.	____ x 0.25 (Max: 1)	

ASSESSMENT FORM FOR FINAL YEAR RESEARCH PROJECT: RESEARCH REPORT (Weight 50%)
(COMPLETED BY SUPERVISOR AND EXAMINER)

3.	**Research Findings and Discussion (20 MARKS)**	Data is not adequate and irrelevant.	Data is fairly adequate and irrelevant.	Data is adequate and relevant.	Data is adequate and very relevant.	____ x 1 (Max: 4)	
		Measurement is wrong and irrelevant	Measurement is suitable and relevant but need major adjustment.	Measurement is suitable and relevant but need minor adjustment.	Measurement is excellent and very relevant.	____ x 1 (Max: 4)	
		Data analysis is inaccurate	Data analysis is fairly done but needs major modification.	Data analysis is satisfactory but needs minor modification.	Data analysis is correct and accurate.	____ x 1 (Max: 4)	
		Data analysis is not supported with relevant output/figures/tables and etc.	Data analysis is fairly supported with relevant output/figures/tables and etc.	Data analysis is adequately supported with relevant output/figures/table and etc.	Data analysis is strongly supported with relevant output/figures/table and etc.	____ x 1 (Max: 4)	
		Interpretation on analyzed data is wrong.	Interpretation on analyzed data is weak.	Interpretation on analyzed data is satisfactory.	Interpretation on analyzed data is excellent	____ x 1 (Max: 4)	
4.	**Conclusion and Recommendations (15 MARKS)**	Implication of study is not stated.	Implication of study is weak.	Implication of study is good.	Implication of study is excellent	____ x 1.25 (Max: 5)	
		Conclusion is not stated	Conclusion is weakly explained.	Conclusion is satisfactorily explained.	Conclusion is well explained.	____ x 1.25 (Max:5)	
		Recommendation is not adequate and irrelevant.	Recommendation is fairly adequate and irrelevant.	Recommendation is adequate and relevant.	Recommendation is adequate and very relevant.	____ x 1.25 (Max:5)	
						TOTAL (50 MARKS)	