A STUDY OF CYBERSECURITY AWARENESS OF THE TIKTOK APPLICATION AMONG GENERATION Z IN KELANTAN

MOHD SUKRI BIN JALAPAR, PREETI A/P SOCHITRO KUMAR, NOR SHAZWANI BINTI MD RODZI, NURUL MAISARAH BINTI LAN HAWARI

BACHELOR OF ENTREPRENEURSHIP (COMMERCE) WITH HONOURS

2024

A Study of Cybersecurity Awareness of the TikTok Application Among Generation Z In Kelantan

by

Mohd Sukri Bin Jalapar, Preeti A/P Sochitro Kumar, Nor Shazwani Binti Md Rodzi, Nurul Maisarah Binti Lan Hawari

A thesis submitted in fulfillment of the requirements for the Bachelor of Entrepreneurship (Commerce) 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.

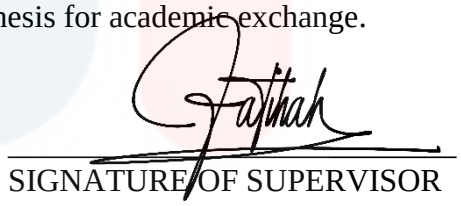
☒	**OPEN ACCESS**	I agree that my thesis is to be made immediately available as hardcopy or on-line open access (full text).
☒	**EMBARGOES**	I agree that my thesis is to be made available as hardcopy or on-line (full text) for a period approved by the Post Graduate Committee. Dated from 8 October 2023 until 18 January 2024.
☒	**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.

SIGNATURE

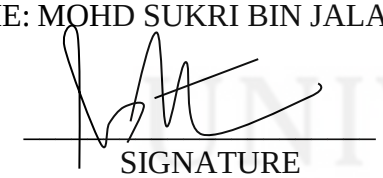
NAME: MOHD SUKRI BIN JALAPAR



SIGNATURE OF SUPERVISOR

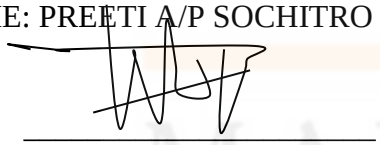
NAME: DR. FATIHAH BINTI MOHD

Date: 05 /02/ 2024



SIGNATURE

NAME: PREETI A/P SOCHITRO KUMAR



SIGNATURE

NAME: NOR SHAZWANI BINTI MD RODZI

SIGNATURE

NAME: NURUL MAISARAH BINTI LAN HAWARI

Date: 18 /01/ 2024

ACKNOWLEDGMENT

We would like to express our gratitude to everyone who aided us in completing our final year project. Firstly, we want to sincerely thank Dr. Fatihah Binti Mohd, our supervisor, for everything. We appreciate that she gave us the priceless opportunity to work under her direction and for providing us with vital support while we conducted our research. We would also like to thank our teammates for completing Research Project I (ACS4112) and Research Project II (ACS4113). Additionally, we cannot forget the respondents who cooperated in answering the survey questions we distributed.

Finally, we especially want to thank our families for their unwavering support and patience throughout our research. With their help and understanding, we were able to complete this study project on schedule. We are also appreciative of God's favor in providing us with a lot of encouragement as we conducted our investigation.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

ABBREVIATION	
Generation Z	GenZ
COVID-19	Corona Virus Disease of 2019
MCO	Movement Control Order
DOM	Department of Statistics Malaysia
TPB	Theory of Planned Behaviour
IV	Independent Variable
DV	Dependent Variable
SPSS	Statistical Package for the Social Science
MCT	Measure of Central Tendency
SPM	Sijil Pelajaran Malaysia
STPM	Sijil Tinggi Pelajaran Malaysia
SmartPLS	Smart Partial Least Squares
SEM	Structural Equation Modelling
TRA	Theory Reason Action

LIST OF SYMBOLS

SYMBOLS

%	Per cent
n	Sample size
p	Population
r	Coefficient
≥	Greater than
≤	Less than
β	Beta value
P	Significant Value

ABSTRAK

Generasi Z (GenZ) merupakan kumpulan demografi yang membesar dalam era digital dan sangat mahir dalam teknologi moden. Salah satu platform media sosial kegemaran mereka ialah TikTok, yang membolehkan mereka menyatakan diri melalui video pendek dan kerjasama kreatif. Walau bagaimanapun, penglibatan GenZ dalam aktiviti TikTok boleh menyebabkan ancaman siber potensial, seperti penipuan, penjenayah dalam talian, dan gangguan dalam talian, disebabkan oleh pengetahuan terhad mereka mengenai keselamatan siber. Oleh itu, peningkatan kesedaran keselamatan siber di kalangan pengguna GenZ di TikTok adalah penting untuk melindungi mereka daripada risiko-risiko ini. Kajian ini bertujuan untuk menyiasat faktor-faktor yang mempengaruhi kesedaran keselamatan siber di kalangan pengguna GenZ TikTok, dengan tumpuan kepada sikap, pengetahuan, dan persekitaran digital. Objektif penyelidikan adalah untuk mengkaji pengaruh faktor-faktor sikap, menyiasat hubungan antara faktor-faktor pengetahuan dan kesedaran keselamatan siber, serta mengenal pasti hubungan antara faktor persekitaran dan kesedaran keselamatan siber. Hasil kajian menunjukkan adanya korelasi yang signifikan secara statistik dan positif yang kuat antara faktor sikap, pengetahuan, dan persekitaran dengan kesedaran keselamatan siber pengguna aplikasi TikTok GenZ. Nilai P bagi setiap faktor menunjukkan 0.000 dan nilai P bagi korelasi kurang daripada 0.05. Temuan kajian ini akan memberikan pandangan berharga untuk mengatasi cabaran keselamatan siber yang dihadapi oleh pengguna GenZ di platform TikTok.

ABSTRACT

Generation Z (GenZ) is a demographic that grew up in the digital age and was highly familiar with modern technology. One of their favorite social media platforms was TikTok, which allowed them to express themselves through short videos and creative collaborations. However, the involvement of GenZ in TikTok activities could lead to potential cyber threats, such as fraud, hacking, and online harassment, due to their limited knowledge of cybersecurity. Therefore, improving cybersecurity awareness among GenZ users on TikTok was crucial to protect them from these risks. This study aimed to investigate the factors that influenced cybersecurity awareness among GenZ users of TikTok, focusing on attitudes, knowledge, and the digital environment. The research objectives were to examine the influence of attitude factors, investigate the correlation between knowledge factors and cybersecurity awareness, and identify the relationship between environment factors and cybersecurity awareness. The finding of the study showed that there was a statistically significant and strong positive correlation between the attitude, knowledge, and environment factors and the cybersecurity awareness of GenZ TikTok application users. The P-value for each factor was 0.000, and the P-value for correlations was less than 0.05. The findings of this study provided valuable insights to address the cybersecurity challenges faced by GenZ users on the TikTok platform.

CHAPTER 1

INTRODUCTION

1.1 Background of the Study

Generation Z (GenZ) was a group born around the mid-1990s to the early 2010s. The exact range of birth years may differ according to the source, but in general, they were the generation that grew up in the digital age and were familiar with the development of modern technology from an early age. They were called GenZ because they followed Generations X and Y and were given the letter Z to reflect their role as the successor generation that came after the previous generation. This name also reflected their speed and adeptness in adopting technology, especially related to the use of the internet (McKinsey, 2023). One of their favorite social media platforms was TikTok, which allowed them to express themselves through short videos and creative collaborations (Anonymous, 2023).

TikTok was a social media application that allowed users to create and share short videos, often accompanied by background music. This application was very popular among GenZ, offering a creative platform where they could express themselves through short videos. GenZ used TikTok for various activities, including dance challenges, lip-sync, comedy, and various other creative expressions. They often collaborated and interacted with each other, creating a trend that quickly spread within the TikTok community (D'Souza, 2023).

The involvement of GenZ in the activities of TikTok itself usually did not cause cybercrimes. However, risks arose when users were not aware of good digital security practices. For example, sharing personal information excessively or falling victim to phishing tactics. Involvement in these practices could increase the possibility of cybercrimes. Therefore, understanding cybersecurity and digital literacy was important to protect GenZ and other users on this platform (Lee et al., 2023).

Additionally, an article stated that there was an 82.5% increase in cybersecurity cases during the Coronavirus Disease of 2019 (COVID-19) (MeiKeng, 2020). The increase in cybersecurity incidents during this Movement Control Order (MCO) period marked a major shift, reflecting the outbreak's massive impact on cybersecurity vulnerabilities and risks. To ensure that users were aware of potential risks and followed safe online activities, cybersecurity awareness was a crucial component of the digital world. For GenZ, who was the most familiar with using platforms such as TikTok, this awareness became critical. The dangers of social media platforms, such as fraudulent messages, identity theft, and privacy violations, highlighted how important it was to comprehend TikTok's unique cybersecurity environment.

Recent studies have highlighted the cybersecurity weaknesses of GenZ users. Kamalulail et al. (2022) suggested that improving cybersecurity awareness among university students in Malaysia, and potentially in other similar contexts, should focus on increasing knowledge about cybersecurity. Similarly, the study conducted by Garba et al. (2020) stated that there was a baseline level of awareness, and there was room for improvement, especially in the absence of an active awareness program.

In summary, the research indicated that there was a need to enhance cybersecurity knowledge among university students in Malaysia to improve their overall cybersecurity awareness, as other demographic and attitudinal factors did not significantly impact awareness levels. Through an extensive investigation of the attitudes, knowledge, and environment of GenZ users on TikTok about cybersecurity, this study aimed to both uncover current risks and provide customized treatments. To enable GenZ users to use TikTok safely and securely, these interventions may take the shape of instructional campaigns, platform-specific security features, and approachable rules. In the end, the research aimed to provide insightful information that would improve the digital

safety of TikTok users and lay the groundwork for raising cybersecurity awareness on all the social media sites that GenZ used.

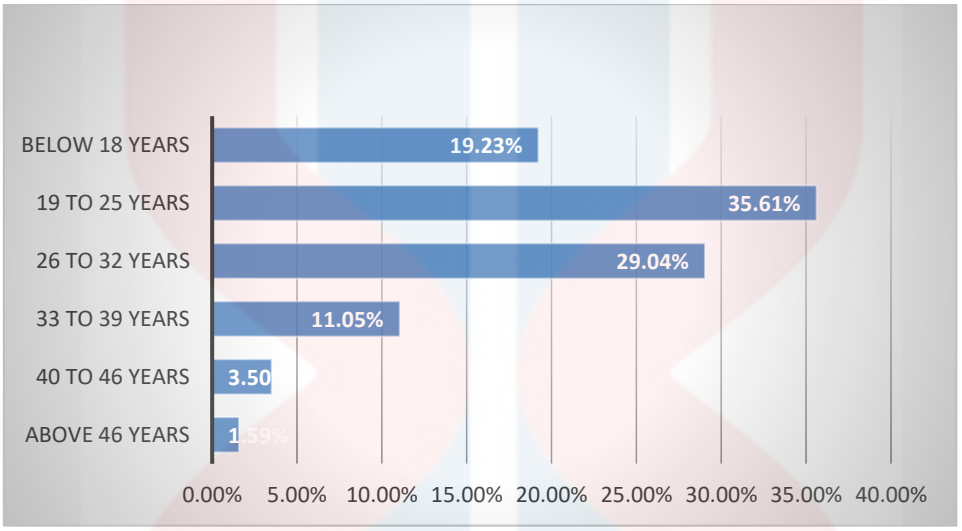
1.2 Problem Statement

In the era of increasing technological sophistication, many negative effects have been experienced by its users, especially those who often use social media such as the TikTok application. Most users of the TikTok application nowadays were GenZ or those born from 1994 to 2010. This is because this generation grew up in the world of modern technology which influenced them to use social media. Indirectly, they were frequent users of social media (Karol Król, 2020). Among the negative effects of using this application were cybersecurity issues. In 2020, based on the available data, a significant increase in cybersecurity incidents in Malaysia was recorded which amounted to 6,512 (Anonymous, 2023).

In addition, an increase in cybersecurity cases could be seen during the Movement Control Order (MCO) enforced due to the COVID-19 pandemic (MeiKeng, 2020). Cases increased dramatically to 82.5 per cent during this period, in contrast to the 12 per cent recorded in April 2019. The increase in cybersecurity incidents during this MCO period marked a major shift, reflecting the outbreak's massive impact on cybersecurity vulnerabilities and risks. The rapid increase in these incidents showed an increase in cyber threats and vulnerabilities, therefore, awareness of cybersecurity needed to be emphasized especially to GenZ.

Based on Figure 1.1, the data shows the percentage distribution of TikTok users in Malaysia as of June 2023 across different age groups. The largest portion of users were in the age range of 19 to 25 years, which is where they were from the GenZ group which made up 35.61% of the user base. The next important demographic was the 26 to 32-year-old age group, which comprised

29.04% of TikTok users. Those under 18 accounted for 19.23%, while users aged 33 to 39 made up 11.05%. The age group of 40 to 46 years and above 46 years contributed 3.50% and 1.59% respectively. This breakdown emphasized TikTok's popularity among GenZ.

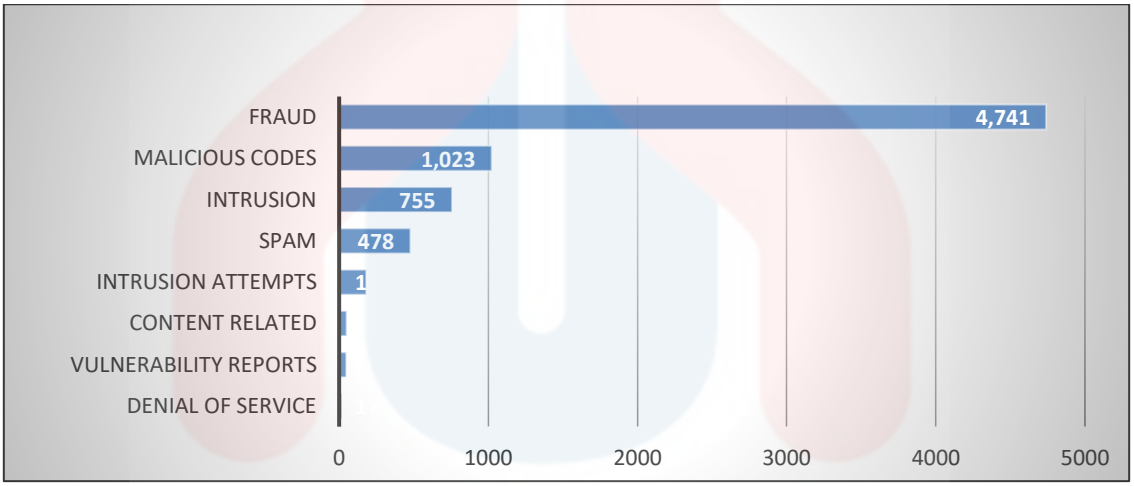


Source: Statista Research Department (13 July 2023)

Figure 1.1: The numbers of TikTok users in Malaysia as of June 2023 by age group

Consequently, there are several drawbacks to GenZ's use of the TikTok app, including a lack of knowledge of cybersecurity. Initially, those users were susceptible to outside influence. This was a result of their lack of knowledge regarding cybersecurity concerns, which could give rise to issues like fraud, hacking, and online harassment. Most of these occurrences, according to a MeiKeng (2020) article, happened during the MCO, a period when there was a rise in the use of applications and technology. Mail (2022) says that between January and July 2022, there were 11,367 reports of cybercrime, whereas there were 18,510 reports of commercial crime over the same period. He asserted that the trend in cybercrime rose from 39% to 61% between July 2022 and June 2026. Fraud is one of the cybercrimes that has increased the most. In conclusion, users were more susceptible to being duped by fraudsters, intrusions, or cyber criminals if they were not informed about cybersecurity.

Therefore, the purpose of this study is to comprehensively examine and analyze the various factors that make up the level of awareness of GenZ users when it comes to using the TikTok application in the context of cybersecurity. By investigating these factors, it can explain the importance of cybersecurity and the potential risks associated with their use of TikTok. Not only that, but this research also intends to reveal potential gaps in cybersecurity knowledge and awareness that could cause these users to be exposed to various online threats and be able to reduce the negative effects and issues that could arise because of a lack of cybersecurity awareness (Catal & et.al, 2022).



Source: Statista Research Department (27 February 2023)

Figure 1.2: Number of cyber threat incidents reported to Cybersecurity 2022, by type of crime

1.3 Research Questions

This study finds out three research questions (RQ):

RQ1. What is the relationship between the attitude factor and the cybersecurity of the TikTok Application among GenZ?

RQ2. What is the relationship between the knowledge factor and cybersecurity awareness of the TikTok Application among GenZ?

RQ3. What is the relationship between the environment factor and the cybersecurity awareness of the TikTok Application among GenZ?

1.4 Research Objectives

This study finds three research objectives (RO):

RO1. To examine the relationship of attitude factors on cybersecurity awareness cybersecurity of the TikTok application among GenZ.

RO2. To examine the relationship between knowledge factors and cybersecurity awareness cybersecurity of the TikTok application among GenZ.

RO3. To examine the relationship between environment factors and cybersecurity awareness cybersecurity of the TikTok application among GenZ.

1.5 Scope of the Study

The study focuses on cybersecurity awareness among GenZ in terms of the TikTok application. TikTok is a distinct social media platform that was the first to combine numerous other social media features into a single application, revitalizing the social media industry in the current decade (Rahman, 2021).

This study focused on Kelantan's GenZ. Furthermore, Gen Z is a trend-following generation. TikTok's cybersecurity awareness educates GenZ on scammers, hackers, and phishing. The table shows that GenZ was born between 1997 and 2012. GenZ's current ages range from 11 to 26. According to the (Department of Statistics Malaysia, DOSM), Kelantan's Gen Z population is 27.51%. Table 1.1 shows the range age of GenZ and Figure 1.3 shows the population of GenZ in Kelantan.

Table 1.1: Range age of GenZ

Generations	Born	Current Ages
Gen Z	1997-2012	11-26
Millennials	1981-1996	27-42
Gen X	1965-1980	43-58
Boomers II (a/k/a Generation Jones)*	1955-1964	59-68

Source: (Brunjes, K. 2023)

Source: Department of Statistics Malaysia

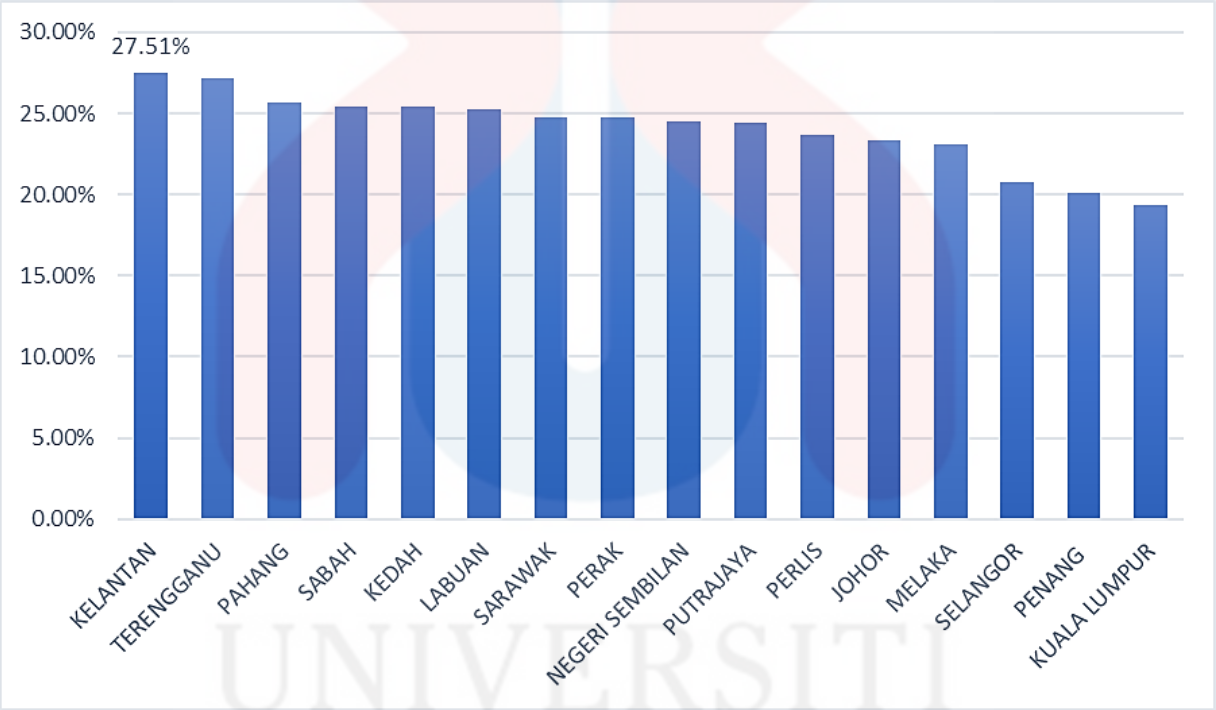


Figure 1.3: The population of GenZ in Kelantan

1.6 Significance of Study

This study aimed to benefit GenZ users who were involved in the TikTok application. GenZ which used the TikTok application could learn more about cybersecurity awareness. GenZ grew up in an era where cybersecurity threats became more sophisticated and prevalent. Understanding their level of awareness helped in devising strategies to mitigate risks and protect users from cyber

threats. It was also important to protect GenZ from cybercrimes. When GenZ was aware of cybersecurity, it reduced the threat of scammers.

Next, TikTok is one of the most popular social media platforms among GenZ. With a large user base, the security of TikTok users has become a critical concern. GenZ could provide more information and awareness about cybersecurity, especially when using the TikTok application. They will be more aware of the scamming, phishing, and fraud of cyber. This study is very important to GenZ as it gave awareness to them in dealing with TikTok applications about cybersecurity.

1.7 Definition of Term

1.7.1 Cybersecurity

Cybersecurity, also known as information technology security or electronic information security, is a broad topic that guards against hostile assaults on digital systems and data in a variety of contexts, including mobile computing and enterprises. This security domain can be categorized into different aspects (Kaspersky, 2019). Network security entails establishing a secure environment for devices, applications, and users to operate safely, safeguarding the underlying networking infrastructure from unauthorized access, misuse, or theft (Cisco, 2019).

Information security and cybersecurity have distinct scopes and objectives, although they are frequently used interchangeably. In a more precise delineation, cybersecurity falls under the umbrella of information security. Information security is a comprehensive domain encompassing various aspects, including physical security, endpoint security, data encryption, and network security. It is intricately linked with information assurance, which safeguards data from diverse threats like natural disasters and servers (Anonymous, 2023). Disaster recovery and business

continuity planning were integral, outlining how organizations responded to cybersecurity incidents and other events that disrupted operations or data. These plans facilitated the recovery of operations and continuity of business during resource disruptions (Kaspersky, 2019).

Lastly, end-user education is a critical element in cybersecurity. Educating individuals on best security practices, such as avoiding suspicious email attachments and unverified USB drives, was vital in reducing human errors that could compromise system security. In summary, cybersecurity covers a range of measures to protect digital systems, networks, and data in various contexts, emphasizing network and application security, data integrity, operational processes, disaster recovery, business continuity, and user education to ensure a holistic approach to security (Kaspersky, 2019).

1.7.2 Awareness

Awareness is a concept that can be understood in relative terms, with a focus on internal states like visceral feelings or external events perceived through the senses. It is akin to the act of sensing something, which differs from observing and perceiving, as it involves the initial process of acquainting ourselves with the things we perceive. This state of awareness, often linked to brain activation in response to stimuli, can be exemplified when the retina processes light waves, resulting in the perception of, say, the colour red. The challenge in defining awareness analytically lies in its complex and multifaceted nature.

Awareness was closely intertwined with consciousness, denoting a fundamental experience, like a feeling or intuition that accompanied our encounter with various phenomena, a phenomenon referred to as awareness of experience. Additionally, consciousness was believed to fluctuate continuously at different levels. In the awareness literature, three key concepts emerged. First was

cognitive awareness, which pertained to an individual's accurate and in-depth comprehension of their perceptions and thoughts. The second perspective posited that awareness was multilayered, encompassing both conscious and unconscious aspects, ultimately culminating in a final stage of awareness. The third viewpoint placed a strong emphasis on awareness about understanding other people's emotions and sentiments (Chiara, 2022).

1.7.3 Generation Z (GenZ)

The term GenZ refers to individuals born in the late 1990s and early 2000s in the United States. While some sources define this generation's timeframe as 1997–2012, there is ongoing debate and contention about the specific years, as delineating generations and their defining characteristics proves challenging. GenZ comes after the millennial generation, also known as Generation Y, which succeeded Generation X, the first generation designated with a letter. As GenZ concludes the standard Latin alphabet, it is followed by Generation Alpha, marking the first time a Greek letter is assigned to a generation (Eldridge, 2023).

An article titled “Four Reasons GenZ will be the Most Different Generation” asserts that GenZ possesses distinct expectations, preferences, and perspectives on work, making them a challenging demographic for organizations (Jenkins, 2017). The characteristics of GenZ individuals include greater diversity, a global outlook, and a significant impact on the culture and attitudes of the broader population. Notably, GenZ effortlessly incorporates technological changes into various aspects of their lives, with the use of technology being as innate to them as breathing.

1.7.4 Social Media Applications

Social media apps are applications designed for mobile devices or computers that facilitate the creation, sharing, and exchange of user-generated content within virtual communities. These platforms enable users to connect, share text, images, videos, and other multimedia content, and engage in real-time communication. Social media apps have become integral to modern communication and play a significant role in shaping online interactions and information dissemination (Tufts, 2023).

For the most up-to-date and specific references, please consult recent scholarly articles, books, or reputable online sources that cover developments in technology and social media trends. Popular platforms like Facebook, Instagram, Twitter, and LinkedIn are examples of widely used social media apps, each serving distinct purposes in the realm of online communication and networking.

1.7.5 TikTok Application

TikTok stood out as the premier hub for concise mobile video content, aiming to kindle creativity and spread joy. With global headquarters situated in Los Angeles and Singapore, and additional offices in major cities like New York, London, and Tokyo, TikTok served as a platform where over a billion users freely expressed themselves. Upholding a commitment to user safety, TikTok enforced comprehensive policies to ensure a secure environment for content creation and sharing (TikTok, 2023).

In response to concerning trends, TikTok intensified efforts to safeguard its global community. The platform consistently prohibited hateful ideologies such as antisemitism and remained dedicated to preventing the proliferation of hate speech. The TikTok team unwaveringly prioritized the safety, security, and privacy of its diverse user base, fostering an environment

where creativity and joy flourished. In October, TikTok proudly participated in Cybersecurity Awareness Month, reaching out to its 150 million-plus community members in the United States to raise awareness about cybersecurity. This year, TikTok spotlighted two significant groups: creators within the TikTok community providing cybersecurity education, and esteemed security researchers from Hacker One. The platform also shared valuable tips to help the user be cyber-smart in their online activities and offered guidance to those aspiring for a career in cybersecurity. TikTok, known for celebrating diversity and authenticity, served as a platform where users like Cececuttino, Lindavivah, and Merelyashley contributed to critical cybersecurity education, aiding the TikTok community in learning how to navigate the online space safely (TikTok, 2023).

1.7.6 Cybersecurity Awareness

Cybersecurity awareness in social media refers to the knowledge and consciousness of potential online threats, privacy issues, and safe online practices that users should have when engaging with social media platforms. It involves being informed about the risks associated with sharing personal information, interacting with unknown users, and clicking on suspicious links or attachments within social media environments. Additionally, cybersecurity awareness in social media includes understanding how to protect one's online identity and data, recognizing common social engineering tactics, and being vigilant against cyber threats. This is crucial in an era where social media platforms are increasingly targeted by cybercriminals (Anonymous, 2022)

According to a study titled "Cybersecurity Practices for Social Media Users" by Herath et al. (2022), the prevalence of cyberattacks on social media platforms poses a significant concern despite the existence of built-in security measures. Human error, potentially opening backdoors for cyberattacks, remains a critical issue. The influence of user demographics like age, gender, and education on cybersecurity awareness in social media is unclear. While studies support the

link between cyber awareness and behavior, evidence is lacking regarding the impact of secure user behavior on vulnerability. Further research is needed to identify factors affecting user awareness and behavior, as well as to establish recommended cybersecurity practices for social media users (Hong, 2022).

1.7.7 Attitude Factor

Attitude is a psychological construct that represents an individual's overall evaluation, feelings, and disposition toward a particular object, concept, or behavior. It encompasses the positive or negative assessment and emotional response someone holds regarding the subject at hand. In the context of the research titled Cybersecurity Awareness among GenZ Users of the TikTok Application, attitude relates to the GenZ users' perceptions and feelings regarding cybersecurity practices and risks associated with the use of TikTok (Anonymous, n.d.).

In the current era of globalization, social media attracts users from diverse backgrounds and age groups, displaying a variety of attitudes. Internet users must assume responsibility, exercising caution and discernment in assessing information due to its varying reliability. Zhang (2018) underscored that the escalating gravity of security and trustworthiness concerns, emphasizing the urgent need for resolution. A study established there is a positive correlation between a negative business cybersecurity attitude and the adoption of risky cybersecurity practices Hadlington (2017).

1.7.8 Knowledge Factor

The concept of knowledge factor in the context of cybersecurity refers to an individual's understanding of potential online threats, security best practices, and the ability to recognize and respond to security risks in the digital environment. It encompassed awareness of common cyber

threats, such as phishing, malware, and data breaches, as well as knowledge of how to safeguard personal information and digital assets (Anonymous, 2022).

A study underscored the critical gap between increasing internet dependence and lagging awareness of protection tools. Existing research suggested that cybersecurity training programs, such as theoretical lectures and simulators, could enhance knowledge and mitigate risks. When related to the research title Cybersecurity Awareness of the TikTok Application Among GenZ, these insights emphasized the importance of targeted awareness campaigns and training programs to address specific platforms like TikTok, ensuring effective cybersecurity practices among the younger generation (Zwilling et.al 2020).

1.7.9 Environmental Factor

Environmental factors, in the context of cybersecurity awareness research, pertained to the external conditions, influences, and contextual elements that surrounded individuals as they interacted with digital platforms or applications. It included the design and features of the platform, the availability of security settings, educational resources, peer influence, and the overall ecosystem in which users engaged in online activities. A recent investigation conducted by Ahmad & et.al (2018) also agreed that including environmental values in his study model as a cyber-literate environment was very important. Ibrahim (2014) stated that the existence of a cyber-literate environment could prevent the occurrence of cyberbullying and other cybercrimes.

1.8 Organization of the Proposal

The introduction of this paper was covered in the first chapter, which included an analysis of the historical context of research conducted up until that point. Next, the study's scope, importance, research questions, objectives, and problem statement were examined. Additionally, chapter one included the proposal's organization and term definitions.

The research introduction, supporting theory, earlier investigations, declaration of hypotheses, conceptual framework, and conclusion were all covered in the second chapter. The framework graphically depicted the relationship between the variables. The methodology of the study, which was covered in Chapter 3, included the research design, data collection strategies, study population, sample size, sampling procedures, development of research instruments, measurement of the variables, data analysis process, and conclusion.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

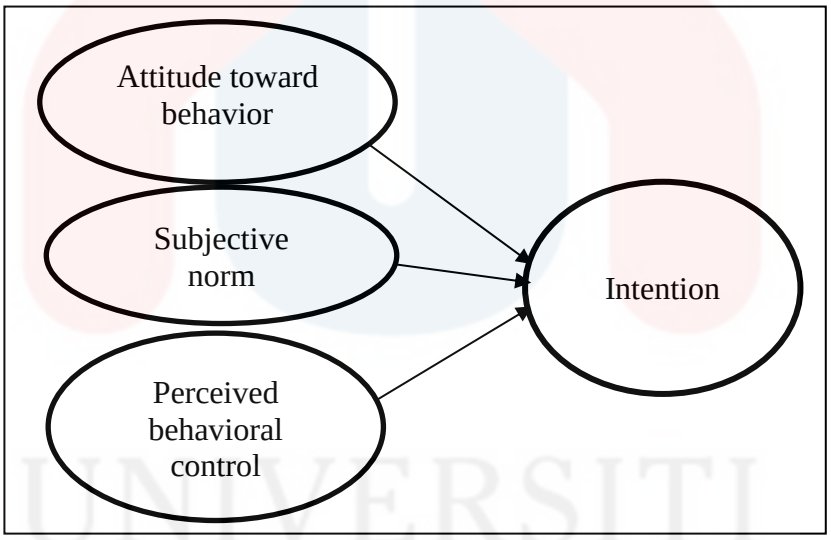
According to Munien (2010), a study was conducted to examine the correlation between users' awareness of the topic and their tendency to fall victim to phishing, a type of social engineering in which emails were used to maliciously request personal information from computer users, such as login credentials or bank account details. The study's findings revealed that despite being aware of its significance, GenZ fell for phishing due to incorrect attitude patterns regarding online security being blamed for this.

The problem of cybersecurity, brought on by the exposure of private data, demonstrated how little users of TikTok knew. Knowledge, attitude, and environmental factors were some of the variables that could impact GenZ's awareness of cybersecurity Pitchan & et.al, (2019). TikTok users had the freedom to select a wide variety of music, apply filters, and lip-sync content. Additionally, the platform's algorithm for your page enabled anyone to contribute to the creation of content that was visible to a large audience, regardless of the number of followers they may have. As a result of its infinite connectivity, it implied that TikTok would have an infinite amount of content (Eka Zahra Solikahan, 2019).

Next, the research investigated the underpinning theory that was applied in this study. This chapter also applied the literature review on the dependent variable, which was awareness of cybersecurity among GenZ users of the TikTok application, while the independent variables were attitude factor, knowledge factor, and environment factor. Moreover, the conceptual framework that was applied to this study was also explained in this chapter, together with the hypotheses statement.

2.2 Underpinning Theory

The Theory of Planned Behaviour is also used in this investigation (TPB). The TPB has been subject to empirical scrutiny in more than 4,200 papers referenced in the Web of Science bibliographic database, rendering it one of the most applied theories in the social and behavioural sciences (Bosnjak & et.al, 2020). A past study presents research on behaviour awareness using TPB (Ahmed et. al, 2021), (Emani et. al, 2016), (Pinto et. al, 2022). Many studies show that TPB involves attitude factor, knowledge factor and environment factors (White Baker et. al, 2007), (Bosnjak & et.al, 2020), (Bazargan-Hejazi et al., 2016). A diagram of the TPB model is presented in Figure 2.1 (Icek Ajzen, 1991).



Source: Icek Ajzen, 1991

Figure 2.1: Theory of Planned Behaviour

Three distinct factors, including attitudes, subjective norms, and perceived behavioural control, independently predict behaviour intention according to the Theory of Planned Behaviour (TPB) (Icek Ajzen, 1991). It is believed that intentions capture the driving forces behind behaviour. The amount of work someone intends to put forth to continue such activity in the future is referred to as their intentions (Bhat I. H., 2018).

The attitude towards behaviour is the next aspect that influences the theory. Attitude is a person's perception of their desirability to act, influenced by their expectations and beliefs about its effects on themselves (Ajzen I. a., 1980). For example, personal control over a person's behaviour in controlling his attitude in a situation includes attitude factors (Rhodes & Courneya, 2003). Perceptions of one's desirability to act are referred to as one's attitude towards performing it. It is dependent upon one's expectations and beliefs on the effects that one's actions will have on oneself. A person's attitude towards behaviour is an assessment of the behaviour (Ajzen I. a., 1980). People behave in ways that are consistent with the attitudes they have about behaviour. He anticipates that the person will choose to conduct in his life with the attitude towards behaviour that he views as positive. As a result, attitude plays a crucial role in determining how someone behaves.

Subjective norms are also the second component impacting the hypothesis. Subjective norms are the belief that important people or groups will approve and support a particular behaviour, determined by perceived social pressure and motivation (Ham, 2015). For example, the social influence that influences someone to think that the behaviour they want to do or not do includes the knowledge factor (Rhodes & Courneya, 2003). Subjective norms are determined by the perceived social pressure from others for an individual to behave in a certain manner and their motivation to comply with those people's views. If the people in his life who he regards as significant can accept him for who he is, then that person will act in a particular way.

The belief in behavioural control is the third component affecting the idea. Perceived behavioural control is a significant factor influencing usage intention, as individuals can exercise self-control over their actions (Malabena, 2022). Both internal and external factors influence an individual's ability to control their actions, with internal characteristics and immediate surroundings being the

main sources of external variables. For example, a person influences social life by doing something whether negative or positive that includes environmental factors (Rhodes & Courneya, 2003). Individual characteristics such as abilities, motivation, knowledge, etc. are also considered internal influences. Aside from that, an individual's immediate surroundings are the source of external variables. A person's perception of behavioural control allows him to understand that the actions he takes are the outcome of his control.

2.3 Previous Studies

2.3.1 Cybersecurity of Awareness

Cybersecurity awareness refers to the extent of comprehension users have about the importance of information security, their related duties, and a set of practices aimed at maintaining an effective level of control over information security. It involves an individual's knowledge of the critical nature of safeguarding sensitive data and networks within an organization. As highlighted by Tasevski (2016), this heightened awareness serves as a proactive shield, enabling preventive measures to prevent security breaches, ensuring the protection of important assets, and strengthening defences against potential cyber threats in the digital domain. As discussed by Zwilling & et.al (2020), cybersecurity awareness encompasses not only recognizing the significance of securing information but also embracing specific actions and responsibilities that contribute to maintaining robust security measures, ensuring the protection of organizational data and networks against potential threats.

Based on a study done by Zakiah (2019), the study found that most social media users had moderate awareness of cybersecurity. The study highlights the importance of increasing awareness to fight cybercrime and the need to educate users about potential cybersecurity risks

and best practices to stay safe online. The measurement of social media consumer awareness is contingent upon multiple aspects, including attitude, knowledge, and environment. Because social media use is also a factor in social crime, this measurement is crucial.

Research on university students' cybersecurity awareness revealed a strong comprehension of aspects like cyberbullying, protecting personal data, and Internet banking. However, noticeable knowledge gaps, particularly in areas like cybersex and self-protection, were identified. This highlights the necessity for collaborative efforts across stakeholders to disseminate knowledge, especially to GenZ. Educational initiatives and awareness campaigns are crucial in bridging these gaps, ensuring a more comprehensive understanding of cybersecurity among younger individuals, and enabling them to navigate the digital landscape securely (Bhatnagar 2020).

2.3.2 Social Media Applications Users Among GenZ

GenZ was the first generation to have grown up using social media, cell phones, and the internet daily. These individuals, who were born between 1997 and 2012, quickly rose to prominence in the world economy. Because social media was such an integral part of their lives, they frequently had very different attitudes on consumption, which were formed by the realities of having grown up mostly online and growing up far away during a pandemic (Alves, 2023). Indirectly, most social media users nowadays are from GenZ.

According to a study by Tyson et.al (2021) comparing Gen Z with older adults, Gen Z was more likely to be influenced by social media. According to the study, Gen Z was more likely to utilize social media as a source of entertainment and information, which increased the likelihood that they would be influenced by it (Chang, 2023). The study also discovered that because Gen Z used social media more frequently for self-expression and interpersonal connections, it had a greater

potential to impact them. According to the study, social media significantly influenced the attitudes and behaviors of GenZ, and to effectively target them, marketers needed to have a thorough understanding of their social media habits (Coe et.al, 2023).

GenZ's social media usage was dominated by platforms such as YouTube, Instagram, and TikTok. YouTube led as the most preferred platform among Gen Z, with 88% of individuals from this cohort spending most of their time on the app. Following closely, Instagram had a large presence, with 76% of Gen Z users engaging on the platform. TikTok quickly gained popularity among this generation, capturing 68% of their attention (Roberts, 2023). This shift in consumption patterns reflected the preferences and habits of this demographic, showing a clear bias towards visually appealing and content-driven platforms such as YouTube, Instagram, and TikTok.

2.3.3 TikTok Application

According to a study conducted by Ettisa (2023), it was found that the use of TikTok had very little negative impact on teenagers and young adult students. However, the study also noted that TikTok's addictive nature could lead to excessive use, which could have negative consequences. In 2021, Montag and his colleagues conducted a study that provided a comprehensive overview of the psychological aspects of TikTok use. The study emphasized the need for more research on potential detrimental effects, especially among young users who are more vulnerable to these effects. Reports by Johnson F (2023) highlighted the risks associated with mobile apps, including TikTok, and the need for businesses to take heed. The report highlighted the ability of mobile applications to collect large amounts of data and metadata sent to storage locations around the world, which could pose significant security risks to businesses.

2.3.4 Attitude Factor

Studies have investigated how attitudes affect people's awareness of cybersecurity. Individual attitudes and behaviors about cybersecurity could be influenced by social influences from the workplace, family, and friends (Hong et.al, 2022). Regarding the attitude component, educators who exhibited a positive attitude toward cybersecurity served as role models for their students in this regard (Zulkifli et.al, 2020). Indirectly, pupils with positive attitudes were more conscious of cybersecurity.

Attitudes play an important role in shaping an individual's approach to cybersecurity awareness, including their behaviour in using social media platforms such as TikTok. For example, individuals' attitudes toward the perceived risk of sharing personal information, their belief in the effectiveness of security measures, and their propensity to adopt protective measures could impact their overall cybersecurity awareness. As a result, a wide range of people used social media, especially GenZ, which was primarily responsible for the adoption of platforms like TikTok. Daily interactions revealed a variety of attitudes. Furthermore, security and reliability issues became more serious and required immediate attention, according to (Zhiyong Zhang, 2018).

In aiming for substantial progress, prioritizing information security awareness was crucial. Challenges in this realm often involved gauging human attitudes, a task complicated by the influence of other facets like culture, motivation, values, and mentality. A prior study by Hadlington (2017) found a significantly unfavorable link between risky internet behavior and attitudes towards cybersecurity. This study discovered a correlation between higher levels of risky behavior and more unfavorable sentiments.

2.3.5 Knowledge Factor

In the realm of cybersecurity and social media usage, such as the TikTok application, education was crucial for individuals' capacity to observe and plan through the diverse online scenarios they may have experienced. As highlighted by Apps (2022), individuals with a strong understanding of cybersecurity were better prepared to recognize and respond to both positive and negative situations while engaging in social media platforms. Therefore, the knowledge factor was closely related to cybersecurity awareness.

Previous studies' findings suggested that cybercrimes and threats had become an international issue. Cybercriminals exploit security holes or vulnerabilities in people with the intent of directly stealing passwords, data, or money. Data breaches, phishing, ransomware, and hacking were the most common cyber threats. Cybercrime was a serious threat to public safety, national security, and the economy, with potential annual costs in the billions of dollars (Agency, 2023). Giving TikTok users, especially members of GenZ, the information and skills to take charge of their social media behavior was essential to averting cyberattacks and safeguarding their online identity.

While knowledge and awareness served as foundational elements, influencing behavior was a complex process that required more than just information dissemination. Past research, exemplified by Patel (2017), underscored the significance of knowledge in mitigating vulnerabilities to cyber-attacks. However, the mere possession of knowledge was insufficient in altering behavior, especially within the digital realm. Having the right knowledge was essential to acting appropriately in every circumstance. Within the domain of cybersecurity, this entailed identifying and being aware of threats, comprehending their possible consequences, and being aware of the countermeasures that could be implemented. Many users, due to a lack of

understanding, remained highly vulnerable to cyber-attacks and exhibited a lack of awareness when it came to the risks associated with sharing personal information on platforms like TikTok.

The study conducted by Kovacevic et.al (2020) highlighted a significant relationship between knowledge and cybersecurity awareness, particularly among GenZ individuals. Despite being among the most frequent users of digital platforms, this demographic often experienced a lack of confidence and perceived safety in the cyber world. The study found that deficiency in knowledge contributed to this sense of vulnerability. Consequently, there was a pressing need to address this gap in cybersecurity education, especially within educational institutions.

2.3.6 Environmental Factor

Environmental factors significantly influenced cybersecurity awareness, particularly among GenZ users of the TikTok application. Pitchan et.al (2019) underlined the pivotal role of the environment in shaping perceptions and practices related to cybersecurity. Within this environmental context, the influence of parents and peers stood out as a crucial determinant in shaping the cyber hygiene habits and awareness of young users.

Parents play a fundamental role in educating their children about cybersecurity practices. Research Pitchan (2017) highlighted the impact of parental guidance, indicating that most respondents were influenced by their parents' efforts in educating them about safe online practices. The proactive role of parents, including monitoring their children's social media activities, regardless of location, could profoundly impact the development of secure online behavior in their children. By discussing the risks and benefits of social media use, parents indirectly contributed to their children's awareness and understanding of using these platforms safely.

Moreover, the influence of peers and colleagues also played a significant role in promoting cybersecurity awareness. Another study noted the importance of peer-to-peer interactions in sharing accurate information about online threats and safe social media practices. Colleagues and peers could serve as mutual reminders and sources of accurate information, thus creating a culture of shared knowledge and support in using platforms like TikTok securely (Zakiah 2019).

By fostering a supportive environment where parents, peers, and colleagues actively engage in discussions about online safety, GenZ users could better understand the risks associated with social media and develop a heightened awareness of how to navigate these platforms securely. The collaborative efforts of parents and peer groups created a reinforcing environment that instilled the value of cybersecurity awareness, ultimately contributing to safer online practices among TikTok users within GenZ.

2.4 Hypotheses Statement

In this part, three hypotheses have been generated for this study to investigate the relationship between the independent variables (IV) and dependent variables (DV).

H1: There is a significant relationship between attitude and cybersecurity awareness among GenZ users of the TikTok application.

This hypothesis posited that the attitude of GenZ users towards cybersecurity practices on TikTok would have a measurable impact on their overall cybersecurity awareness. Attitude encompassed users' perceptions, feelings, and evaluations of the importance of cybersecurity measures on the TikTok platform. A positive attitude suggests a willingness to engage in secure online practices, such as setting strong passwords or being cautious with personal information (Sharabati & et.al, 2022).

H2: There is a significant relationship between the knowledge factor and the cybersecurity awareness of GenZ TikTok application users.

This hypothesis asserted that the knowledge factor, which represented users' understanding of cybersecurity risks and best practices, was a critical determinant of cybersecurity awareness among GenZ TikTok users. Knowledge encompassed awareness of common online threats, familiarity with security features on TikTok, and understanding of protective measures. Reid's study examined the impact of a cybersecurity awareness campaign on school-age children as well as their prior understanding of cybersecurity risks. He discovered that advertising helped people become more aware of and knowledgeable about cyber hazards (Niekerk, 2016).

H3: There is a significant relationship between the environmental factor and the cybersecurity awareness of GenZ TikTok application users.

This hypothesis suggests that the environmental factors, which included the features, settings, and overall online atmosphere within the TikTok application, played a significant role in shaping the cybersecurity awareness of GenZ users. The environment encompassed aspects such as the presence of security features, privacy controls, and the overall design of the platform. To measure the dimensions of environmental factors, parental education, workplace, and peers seemed to have played an important role in this factor. The study conducted by Pitchan et al. (2017) found that most of the respondents' parents played a role in educating their children about cybersecurity practices.

2.5 Conceptual Framework

From the literature review, this study proposes a conceptual framework as Figure 2.2. The framework includes one independent variable and three independent variables which are cybersecurity awareness among GenZ users of the TikTok application. Then, the first independent

variable is the attitude factor which has personal experience, social media influence, and cultural influence. The second variable is knowledge factors that have cyber laws and cyber threats and crimes. The third variable is environmental factors which are parental guidance and peer-to-peer interaction.

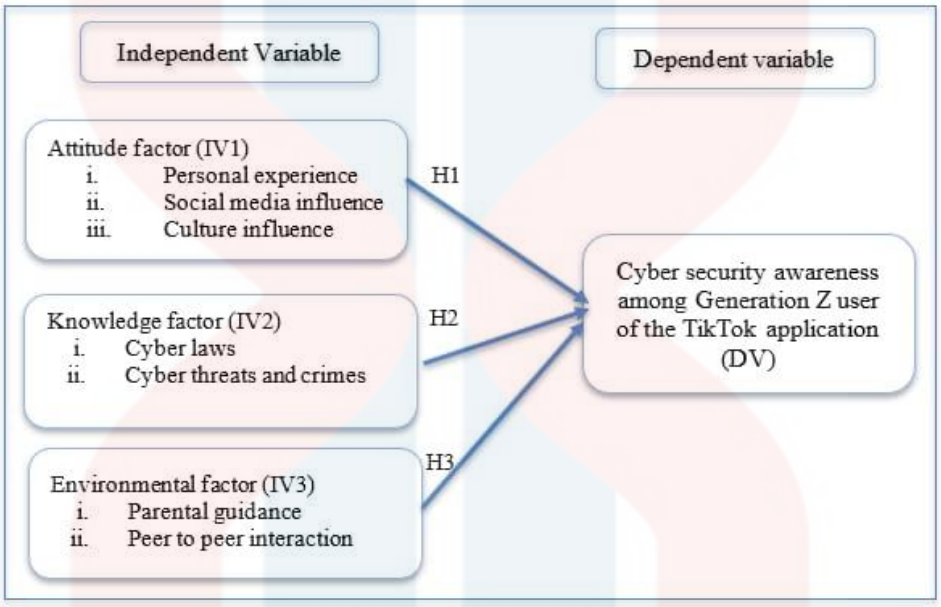


Figure 2.2: Conceptual framework

2.6 Summary

The relationship between the independent variable (IV) and the dependent variable (DV1), as well as the conceptual framework discussed in this part, were established by the study. Additionally, the Theory of Planned Behaviour (TPB) was utilized to establish an independent and dependent variable.

The research introduction of literature review, underpinning theory, previous studies, hypotheses statement, conceptual framework and summary for this chapter. The framework graphically depicted the relationship between the variables. The methodology of the study, which was covered in Chapter 3, included the research design, data collection strategies, study population,

sample size, sampling procedures, development of research instruments, measurement of the variables, data analysis process, and conclusion.

CHAPTER 3

RESEARCH METHODS

3.1 Introduction

The various methods of data collection used in this study were covered in the previous chapter. The protocol and procedures used to gather and analyze the data for this report comprised the analysis technique. This chapter covers the following topics: research design, data collection techniques, study population, sample size, sampling methodology, development of the research instrument, measurement of the variables, and data analysis procedures.

3.2 Research Design

Research design is the structured framework of methods and techniques selected by a researcher to systematically integrate different elements of research, ensuring an effective approach to addressing the research problem. It offers guidance on the how of conducting research within a specific methodology. With research design, researchers can methodically assess a set of research questions, providing a blueprint for the execution of the research. It serves as a roadmap for planning and organizing the research process (Sileyew, 2019).

To implement a deductive technique, researchers must formulate hypotheses based on existing theories and subsequently design a research strategy to test these ideas (Wilson & et.al, 2010). Descriptive analysis can then be conducted by utilizing information about the variables in each scenario (Sekaran & et.al, 2013). The survey instrument consists of multiple-choice questions, Likert scale items, and demographic inquiries. The Likert scale be used to measure the degree of agreement or disagreement with statements related to cybersecurity awareness.

3.3 Data Collection Method

Primary data from participants was collected using a standard survey Google form. A survey questionnaire method was used to collect primary data on a targeted sample using an online survey form (Google Form) administered to GenZ respondents who were aged from 11 to 26 years old. Surveys were mainly carried out on GenZ in Kelantan. From the beginning of the research, data was collected in Kelantan every day until the sample size was sufficient.

3.4 Study Population

The population is the group that the researcher intends to explore, known as the population being studied, and this population serves as the foundation for creating broad generalizations. According to Bandhari (2021), the target population was the complete group of researchers who wished to conclude, that this was the reason why the target population existed. The population consisted of both male and female genders, ranging from ages 11 to 26 years old. The population in this study consisted of GenZ in Kelantan. In this research, we wanted to know about the cybersecurity awareness of GenZ in the TikTok application. Table 3.1 shows the population of people in Kelantan is 1,758,701 million with males 902,330 million and female 856,371 million.

Table 3.1: Population in Kelantan (Perangkaan Negeri Kelantan, 2023)

Population	**Million**
Kelantan	1,758,701
Male	902,330
Female	856,371

3.5 Sample Size

The number of participants in a research study intended to represent a population is known as the sample size. The sample size was the total number of respondents involved in the study. This

number was usually divided by demographics like age, gender, and location to ensure that the sample as a whole was representative of the entire population. Selecting an appropriate sample was one of the most important steps in statistical analysis. In this research, n was the sample size we used. Table n was created by Krejcie and Morgan (1970) to calculate the population size the same as the sample size. According to the Krejcie and Morgan sample size calculation table, the total population was 1,000,000, and the research sample consisted of 384 respondents. In terms of sample size, there were 1,758,701 people in Kelantan, and the data collected was 384 respondents.

Table 3.2: Table of Sample Size (Krejcie and Morgan,1970)

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

Note.—*N* is population size. *S* is sample size.
Source: Krejcie & Morgan, 1970

Source: Krejcie & Morgan (1970)

3.6 Sampling Technique

A probability sampling strategy was used in this investigation. A simple random sampling was used in this investigation. These methods are widely used by researchers to gather data from a readily accessible sample of respondents for market research. Probability sampling methods

generally produce results that are more representative of the population. GenZ in Kelantan is approached to be a part of the sample.

However, they may be more difficult to implement, particularly if do not have a complete population. It is the most widely used sampling technique because it is quick, simple, and time-saving. The utilization of this technique involves a simple data collection process, facilitated by the will use of Google Forms and survey questionnaires. The data collection tool chosen for this study was a questionnaire.

3.7 Research Instrument Development

The questionnaire approach was also used in this study as a research tool to obtain data from the participants. According to Bandhari (2021), a questionnaire is a series of questions or items that aim to obtain information from respondents about their beliefs, experiences, or opinions.

For our study, respondent data was collected through an online survey called a Google Form, as well as using bilingualism in this form. In addition to other social media networks, WhatsApp and Telegram were used to distribute the survey. For this study, the questionnaire was divided into four parts, starting with Parts A, B, C, and D. Part A contains demographic info, while Part B contains general questions. Part C is the dependent variable, which is a question about cybersecurity awareness, and Part D is the independent variable, which contains questions related to factors affecting cybersecurity.

Part A also contained five questions related to demographic info, namely age, gender, academic level, marital status, and occupation. Demographics is an analysis that collects study data that generalizes the characteristics of specific human behaviour (Potters, 2023). The first question in

the demographics of the respondents was the age question, which had age groups between 11 – 14, 15 – 18, 19 – 22, and 23 – 26. In addition, the second question was a question related to gender, which was divided into two, male and female. The third question was about the level of education and contained five groups, namely SPM, STPM, Diploma, Degree, and Master. The fourth question was a question related to marital status, married and single. The last question was related to occupations, which were government, private, student, and unemployed.

Further, part B also represented questions related to general questions containing four questions in this part. The first question was whether the respondent had a TikTok account, whether they answered yes or no. The second question was related to what kind of activities they did on the TikTok application, which had four groups of answers, namely sports, entertainment, marketing, and post video. Next, the third question was related to how frequently they used TikTok and had four daily answer options, several times a week, once a week, and rarely. The last question was related to how they knew about the TikTok application, which had four answer options, namely parents, online advertisement, colleagues, and teachers.

Besides that, part C also represented dependent variables that contained five questions in the questionnaire and used a 5-point Likert scale in the selection of answers. The first question was whether the respondent was familiar with common cybersecurity threats, such as phishing and malware. The second question was whether they regularly updated their passwords to enhance their TikTok account security, and the third question was whether they stayed informed about the latest cybersecurity trends and best practices. The fourth question was whether they were aware of the risks associated with sharing personal information on social media platforms. The last question was whether they could identify potential signs of a cybersecurity attack, such as suspicious emails or messages.

Therefore, part D was also represented by independent variables that contained fifteen questions in the questionnaire that were given a Likert scale answer option - 5 points. This section also contained three sections of questions related to factors that affect cybersecurity, namely the attitude factor, knowledge factor, and environment factor. These three factors also had five questions on each factor in the questionnaire. Table 3.3 shows the item variables of the questionnaires.

Table 3.3: Variables item of questionnaires

Section	**Variables**	**No. of item**	**Total of item**
A	**Demographics info** (Potters, 2023) A1. Age A2. Gender A3. Academic level A4. Marital status A5. Occupation	A1-A5	5
B	**General Question** B1. Do you have TikTok account? B2. What kind of activities do you do on the TikTok application? B3. How frequently do you use TikTok? B4. How do you know about the TikTok application.?	B1-B4	4
C	**Dependent Variables (DV)** Cybersecurity awareness (Zwilling & et.al, 2020) C1. I am familiar with common cybersecurity threats, such as phishing and malware. C2. I regularly update my passwords to enhance my TikTok account security. C3. I stay informed about the latest cybersecurity trends and best practices. C4. I am aware of the risks associated with sharing personal information on TikTok application. C5. I can identify potential signs of a cybersecurity attack, such as suspicious emails or messages.	C1-C5	5

D	**Independent Variables (IV)** Attitude factor (Zhiyong Zhang, 2018) D1. I ensure that the information updated on my TikTok account is accurate. D2. I am attentive to the accuracy of the information about acquaintances on the TikTok application. D3. I am aware of whom I share information about on the TikTok application. D4. I only share information about people whom I truly trust. D5. From my perspective, I can determine whether the information shared on TikTok is true or not. Knowledge factor (Patel, 2017) D6. I am aware of cyber laws in Malaysia. D7. I am aware of cybersecurity awareness programs on the TikTok application. D8. I am knowledgeable about cyber surveillance on the TikTok application. D9. I am knowledgeable about cyber fraud (scam) on the TikTok application. D10. I am aware of cyberbullying on the TikTok application. Environment factor (Zakiah Saizan, 2019) D11. I always share information about cybersecurity awareness on TikTok with my friends. D12. I always discuss cybersecurity threats on TikTok with my friends. D13. My parents always monitor every activity I do on TikTok. D14. I always remind each other about cybersecurity issues on TikTok with my parents. D15. My friends always keep an eye on every activity I do on TikTok.	D1- D5 D6 - D10 D11- D15	5 5 5

3.8 Measurement of the Variables

This study was conducted using both nominal and ordinal methods. Parts A and B were measured using the nominal method which contained questions related to demographic information and general questions. On the other hand, parts C and D were measured by the ordinal method, which was used for dependent variables and independent variables questions using a 5-point Likert scale. According to Ankur Joshi (2015), the Likert scale - 5 points is a set of statements (items) offered

for a real or hypothetical situation under study. Participants were asked to show their level of agreement from strongly disagree to strongly agree with the given statement (items) on a metric scale. In the Likert scale - 5 points, given answer choices between (strongly disagree (SD) =1), (disagree (D) = 2), (neutral (N) = 3), (agree (A) = 4), (strongly agree (SA) = 5) were provided in question part B and C. Table 3.4 below shows the 5-point Likert scale.

Table 3.4: The 5 – point Likert scales (Ankur Joshi, 2015)

Strongly Disagree (SD)	**Disagree (D)**	**Neutral (N)**	**Agree (A)**	**Strongly Agree (SA)**
1	2	3	4	5

3.8.1 Nominal Level of Measurement

This study was conducted using the nominal method on parts A and B questions which represented demographic info and general questions. Part A had five questions in demographics info while part B had four questions in general questions on the Google form. According to (Cramer, 2010), nominal measurements are defined as variables consisting of named categories that do not have mathematical properties. Part A (demographics info) also consisted of several questions in the form of age, gender, academic level, marital status, and occupation. Part B (general question) consisted of several questions, namely, do you have a TikTok account? What kind of activities do you do on the TikTok application? Frequency of using the TikTok application, and from whom do you know about the TikTok application?

Next, part A (demographics info) on the age question had four answer options, which were between 11 – 14, 15 – 18, 19 – 22, and 23 – 26. This was also because GenZ had a young age range which was between 11 - 26 years in Kelantan. In addition, the second question was gender between men and women. This was also because this level had only two genders in this group level. Next, the third question was academic level which was given five answer options which

were SPM, STPM, Diploma, Degree, and Master. This was also because GenZ is still young and has an academic level from SPM to Master. Further, the fourth question, which was marital status, was given two answer options, namely single or married. This was also because some of these groups had households and were still single. Finally, the fifth question was an occupation question that was given four answer options, namely government, private, student, and unemployed. This was also because, at this stage, some were already independent or still studying at any institute of study. Table 3.5 shows the questionnaire from part A.

Table 3.5: Questionnaires from part A

<table>
<tr><th>Section</th><th>Variables and Items</th></tr>
<tr><td>A</td><td>Demographics info / Info demografi
A1. Age / umur:
<table>
<tr><td>11-14</td><td>15-18</td><td>19-22</td><td>23- 26</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>
A2. Gender / Jantina:
<table>
<tr><td>Male/Lelaki</td><td>Female/ Perempuan</td></tr>
<tr><td></td><td></td></tr>
</table>
A3. Academic level / Tahap akademik :
<table>
<tr><td>SPM</td><td>STPM</td><td>Diploma</td><td>Degree /Ijazah</td><td>Master/ Sarjana</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>
A4. Maritial status / Status perkahwinan:
<table>
<tr><td>Single/ Bujang</td><td>Married/ Berkahwin</td></tr>
<tr><td></td><td></td></tr>
</table>
A5. Occupation / Pekerjaaan :
<table>
<tr><td>Government/ Kerajaan</td><td>Private/Swasta</td><td>Student / Pelajar</td><td>Unemployed / Menganggur</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

Besides that, part B (general question) had four questions in the questionnaire. The first question asked if the person had a TikTok account, with two answer options between yes and no. This is because Gen Z either has a TikTok account or does not have one due to their desire to socialize or not. The second question asked about the type of activities the person does on the TikTok application, with four answer options: sports, entertainment, marketing, and posting videos. This is also because many people at this young stage do online businesses or just entertain themselves. The third question was about how frequently the person used TikTok, with four answer options: daily, several times a week, once a week, and rarely. This is because it shows the frequency of Gen Z in using the TikTok application daily. The last question was about how the person learned about the TikTok application, with four answer options: parents, online advertisement, colleagues, and teachers. This is because these young people are likely to be attracted to any individual who uses this application, especially online advertisements. Table 3.6 shows the questionnaires of part B using the nominal method.

Table 3.6: Questionnaires of part B

<table>
<tr><th>Section</th><th>Variables and Items</th></tr>
<tr><td>B</td><td>General question / Soalan umum
B1. Do you have TikTok account / Adakah anda memiliki akaun TikTok?:
<table>
<tr><td>Yes/ Ya</td><td>No/ Tidak</td></tr>
<tr><td></td><td></td></tr>
</table>
B2. What kind of activities do you do on TikTok application / Apakah jenis aktiviti yang anda lakukan di aplikasi TikTok?:
<table>
<tr><td>Sports/ Sukan</td><td>Entertainment / Hiburan</td><td>Marketing/ Pemasaran</td><td>Post Video / Menyiarkan video</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>
B3. How frequently do you use TikTok? / Kekerapan menggunakan aplikasi TikTok.?:</td></tr>
</table>

Daily / *Setiap hari*	Several times a week / *Beberapa kali seminggu*	Once a week / *Sekali seminggu*	Rarely / *Jarang*

B4. How do you know about TikTok application / *Dari mana anda tahu tentang aplikasi TikTok.?:*

Parents / *Ibu bapa*	Online advertisement / *Iklan dalam talian*	Colleagues / *Rakan sekerja*	Teacher / *Guru*

3.8.2 Ordinal Level of Measurement

This study also used an ordinal scale in parts C and D, which were represented by dependent and independent variables. Parts C (dependent variables) and D (independent variables) were measured using the Likert scale method - 5 points. Part C had five questions, and Part D had 15 questions divided into three factors: attitude, knowledge, and environment. These three factors were divided equally, with each factor having five questions. The ordinal scale is defined as a variable measurement scale used to describe the order of variables and not the difference between each variable (Bhat, 2020).

Part C, represented by dependent variables, had five questions. The first question asked whether the participant was familiar with common cybersecurity threats, such as phishing and malware. The second question asked whether they regularly updated their passwords to enhance their TikTok account security, and the third question asked whether they stayed informed about the latest cybersecurity trends and best practices. The fourth question asked whether they were aware of the risks associated with sharing personal information on the TikTok application. The last

question from section C asked whether they could identify potential signs of a cybersecurity attack, such as suspicious emails or messages. Table 3.7 below shows section C from questionnaires that were measured using a 5-point Likert scale.

Table 3.7: Questionnaires of part C

Section	**Cybersecurity Awareness**	**SD**	**D**	**N**	**A**	**SA**
C	C1. I am familiar with common cybersecurity threats, such as phishing and malware. / *Saya kenal dengan ancaman keselamatan siber yang biasa, seperti pancingan data dan perisian hasad*.	1	2	3	4	5
	C2. I regularly update my passwords to enhance my TikTok account security. / *Saya sentiasa mengemaskini kata laluan saya untuk meningkatkan keselamatan akaun TikTok.*	1	2	3	4	5
	C3. I stay informed about the latest cybersecurity trends and best practices. / *Saya sentiasa dimaklumkan tentang trend keselamatan siber terkini dan amalan terbaik.*	1	2	3	4	5
	C4. I am aware of the risks associated with sharing personal information on *TikTok application. / Saya sedar akan risiko yang berkaitan dengan berkongsi maklumat peribadi di aplikasi TikTok.*	1	2	3	4	5
	C5. I can identify potential signs of a cybersecurity attack, such as suspicious emails or messages. / *Saya boleh mengenal pasti tanda-tanda potensi serangan keselamatan siber, seperti emel atau mesej yang mencurigakan.*	1	2	3	4	5

Part D is independent variables that have 15 questions in the questionnaire divided by three factors. The questions in the attitude factor section have five questions. That is, the first question is I ensure that the information updated on my TikTok account is accurate and the second question is I am attentive to the accuracy of the information about acquaintances on the TikTok application. The third question is whether I am aware of whom I share information about on the TikTok application and the fourth question is whether I only share information about people whom I truly

trust. The fifth question from the attitude factor is in my perspective, I can determine whether the information shared on TikTok is true or not. Table 3.8 below shows the attitude factor from section D which uses a 5-point Likert scale.

Table 3.8: Attitude factor from part D

Section	**Attitude Factor**	**SD**	**D**	**N**	**A**	**SA**
D	D1. I ensure that the information updated on my TikTok account is accurate. / *Saya memastikan maklumat yang dikemas kini pada akaun TikTok adalah tepat*	1	2	3	4	5
	D2. I am attentive to the accuracy of the information about acquaintances on the TikTok application. / *Saya seorang yang peka terhadap ketepatan maklumat rakan kenalan di aplikasi TikTok.*	1	2	3	4	5
	D3. I am aware of whom I share information about on the TikTok application. /*Saya sedar siapa yang saya kongsikan maklumat mengenai aplikasi TikTok.*	1	2	3	4	5
	D4. I only share information about people whom I truly trust. / *Saya hanya berkongsi maklumat tentang orang yang benar-benar boleh dipercayai sahaja.*	1	2	3	4	5
	D5. In my perspective, I can determine whether the information shared on TikTok is true or not. / *Dalam perspektif saya, saya dapat menentukan sama ada maklumat yang dikongsi di TikTok adalah benar atau tidak.*	1	2	3	4	5

Next, the knowledge factor in part D also has five questions that are measured using a 5-point Likert scale. The sixth question is whether I am aware of cyber laws in Malaysia and the seventh question is whether I am aware of cybersecurity awareness programs on the TikTok application. The eighth question is whether I am knowledgeable about cyber surveillance on the TikTok application, and the ninth question is whether I am knowledgeable about cyber fraud (scam) on the TikTok application. The tenth question from the knowledge factor is whether I am aware of cyberbullying on the TikTok application. Table 3.9 below shows the knowledge factor from section D.

Table 3.9: Knowledge factor from part D

Section	Knowledge Factor	SD	D	N	A	SA
D	D6. I am aware of cyber laws in Kelantan. / *Saya mengetahui mengenai undang-undang siber di Malaysia.*	1	2	3	4	5
	D7. I am aware of cybersecurity awareness programs on the TikTok application. / *Saya mengetahui berkenaan program kesedaran keselamatan siber di applikasi TikTok*	1	2	3	4	5
	D8. I am knowledgeable about cyber surveillance on TikTok application. / *Saya mengetahui mengenai intipan siber di aplikasi TikTok.*	1	2	3	4	5
	D9. I am knowledge about cyber fraud (scam) on the TikTok application. / *Saya mengetahui mengenai penipuan siber (scam) di aplikasi TikTok.*	1	2	3	4	5
	D10. I am aware of cyberbullying on the TikTok application. / *Saya mengetahui mengenai jenayah buli siber di applikasi TikTok.*	1	2	3	4	5

Furthermore, the environment factor in part D also has five questions. That is, the eleventh question is I always share information about cybersecurity awareness on TikTok with my friends. The twelfth question is whether I always discuss cybersecurity threats on TikTok with my friends the thirteenth question is whether my parents always monitor every activity I do on TikTok, and the fourteenth is whether I always remind each other about cybersecurity issues on TikTok with my parents. The last question from the environment factor in section D is whether my friends always keep an eye on every activity I do on TikTok. Table 3.10 below shows the environmental factors from section D.

Table 3.10: Environment factor from part D

Section	Environment Factor	SD	D	N	A	SA
D	D11. I always share information about cybersecurity awareness on TikTok with my friends. / *Saya sentiasa berkongsi maklumat tentang kesedaran keselamatan siber dalam TikTok dengan rakan-rakan saya.*	1	2	3	4	5
	D12. I always discuss cybersecurity threats on TikTok with my friends. / *Saya sentiasa berkongsi*	1	2	3	4	5

	maklumat tentang kesedaran keselamatan siber dalam TikTok dengan rakan-rakan saya.					
	D13. My parents always monitor every activity I do on TikTok. / *Ibu bapa saya sentiasa mengawasi setiap aktiviti saya di TikTok*	1	2	3	4	5
	D14. I always remind each other about cybersecurity issues on TikTok with my parents. / *Saya sentiasa saling memperingati mengenai isu ancaman siber TikTok dengan ibubapa.*	1	2	3	4	5
	D15. My friends always keep an eye on every activity I do on TikTok. / *Rakan saya sentiasa mengawasi setiap aktiviti saya di TikTok.*	1	2	3	4	5

3.9 Procedure for Data Analysis

Throughout the data analysis process, every element of the acquired data is looked at. In data analysis, measurements were made for variability, reliability, frequency analysis, and descriptive analysis.

3.9.1 Statistical Package for the Social Sciences (SPSS)

Analyzing data is essential to preventing mistakes in judgment. The statistical program known as the Statistical Package for the Social Sciences (SPSS) version 26 was used to analyse the data in this study. One tool used for statistical analysis is called SPSS Statistics, which is used to fit, analyse, and create original patterns among various data variables. The data analysis procedure is the process of going over each component of the data using analysis and reason. SPSS software was used to analyse every piece of data. A format that is simple to tabulate and comprehend is created by gathering, analysing, and condensing data.

3.9.2 Smart Partial Least Squares (PLS)

SmartPLS 4 was used to perform Partial Least Squares-Structural Equation Modelling (PLS-SEM). In terms of the structural model, the path coefficient, and the coefficient of determination (R^2). SmartPLS (Partial Least Squares) is a statistical tool used in structural equation modelling

(SEM) for analyzing relationships between variables. In the context of surveys, SmartPLS helps researchers assess and model complex relationships among survey variables. It allows for the examination of both the measurement model assessing the reliability and validity of survey instruments and the structural model examining relationships between latent constructs. SmartPLS is particularly useful when dealing with smaller sample sizes and non-normal data, making it a flexible option in various research scenarios.

3.9.3 Reliability Analysis

An essential statistical technique for evaluating the stability and consistency of measurements made with a particular tool, scale, or equipment is reliability analysis. It gauges how well a scale or measure performs consistently and dependably when applied repeatedly in various contexts or under comparable circumstances. The most used metric for assessing internal consistency is Cronbach's alpha, or "reliability." It is most used when a scale consisting of multiple Likert questions in a questionnaire or survey needs to have reliability verified. In addition, if inter-rater reliability concerns us, we have a guide on utilizing Cohen's kappa that may be useful.

A statistical indicator of test and measure internal consistency is Cronbach's alpha. A high value for alpha, which is given as a number between 0 and 1, means that the items' internal consistency is generally high Lee Cronbach (1951).

Table 3.11: Cronbach’s Alpha Value Lee Cronbach (2011)

Cronbach’s Alpha Value	**Indication**
$a \geq 0.9$	Excellent
$0.7 \leq a < 0.9$	Good
$0.6 \leq a < 0.7$	Acceptable
$0.5 \leq a < 0.6$	Poor
$a < 0.5$	Unacceptable

3.9.4 Descriptive Analysis

In the data analysis process, descriptive statistics will serve as a fundamental tool to explore the gathered information, employing techniques like percentage, frequency, and Measures of Central Tendency (MCT) such as mean, mode, and median. These statistical methods will help to distil and comprehend the characteristics of the collected data. Specifically, the inclusion of demographic factors like age, gender, ethnicity, major, and year of study provides a comprehensive understanding of the surveyed population. The respondents' positive reception to Section A of the questionnaire, which solicited this demographic data, not only streamlines the organization of information but also proves advantageous in revealing insights into group compositions. These insights will aid in the discernment of patterns and correlations between these demographic variables and the core subject matter, enriching the subsequent analysis and decision-making processes.

3.9.5 Normality Test

A normality test is an essential statistical tool used to assess whether a given sample of data adheres to a normal distribution pattern. Outline that these tests, which encompass measures such as the p-value, are employed to scrutinize the data and identify any substantial deviation from the normal distribution (Mishra & et.al, 2019). If the p-value resulting from these tests is significantly less than 0.05, it suggests a notable departure from the normal distribution. In the context of this study, Statistical software packages like SPSS are recommended by Mishra & et.al (2019) as valuable tools for performing these normality tests, enabling researchers to make informed interpretations about the distribution of their data.

3.9.6 Multiple Regression Analysis

Regression analysis is a useful statistical technique that may be applied to various organizational

situations to determine the extent to which independent factors impact a dependent variable. This instrument evaluates the type and intensity of the link that exists between two or more variables. In this case, the variables that are controlled or altered are thought to have a direct effect on the dependent variable. The dependent variable, in this study focusing on cybersecurity awareness among GenZ, is what's being measured and examined, and it's contingent on the independent variables. In this case, attitude factors, environmental factors, and knowledge factors serve as the independent variables that are presumed to impact cybersecurity awareness. By employing regression analysis, the study aims to elucidate how these independent variables interrelate with and potentially predict cybersecurity awareness among GenZ across diverse organizational settings.

3.9.7 Spearman Correlation

The Spearman correlation test determines whether there is a correlation between two variables. Spearman's test employs ranks rather than normal assumptions, it can be used to analyze data at both the ordinal and continuous levels. For questions on the 3, 5, and 7-point Likert scale or ordinal survey questions, this makes the Spearman correlation excellent. In situations where the fundamental presumptions of linearity and continuous variables required to conduct a Pearson's bivariate correlation study have not been satisfied, Spearman's test can be helpful (Anonymous, n.d.).

3.10 Summary

This chapter provides an overview of the researcher's research strategy. The study design, data collection methods, study population, sampling procedures, sample size, research instrument development, and variable measurement are all covered in this topic. The research methodology used was a quantitative research approach. Using quantitative methodology in research studies

provided an organized and systematic approach to understanding the phenomenon being investigated. The use of techniques such as data analysis using SPSS, reliability analysis, descriptive statistics, and various tests including normality tests and regression analysis enabled a detailed exploration of relationships, patterns, and the effects of independent variables on dependent variables. An online survey method was used for this study, and all information was collected and analyzed. The information was collected from a survey given to GenZ in Kelantan. The purpose of this study was to see how far the awareness of TikTok app users among GenZ was about cybersecurity.

The methodology of the study, which was covered in this chapter, included the research design, data collection strategies, study population, sample size, sampling procedures, development of research instruments, measurement of the variables, data analysis process, and conclusion. The following data analysis chapter 4 consists of an introduction, a preliminary analysis, a descriptive analysis, a validity and reliability test, a normality test, a spearman's rho correlation coefficient, squares-structural equation modeling (PLS-SEM), testing of hypotheses, and a conclusion.

CHAPTER 4

DATA ANALYSIS AND FINDINGS

4.1 Introduction

This chapter describes the findings of the study's analysis. A total of 400 data points were obtained for this investigation via a questionnaire survey. The findings to be included are the preliminary analysis, the demographic profile of respondents, descriptive analysis, the validity and reliability test, the normality test, and the Spearman Correlation analysis. All the analysis is done by using the Social Science Statistical System (SPSS) application version 26.

4.2 Preliminary Analysis

A pilot test is necessary for the study to determine whether the respondents comprehended the questionnaire. In addition, the pilot test is used to evaluate the survey's effectiveness and applicability before it is employed in real-world data collecting (Blog, n.d.). According to Bullen (2013), A good maximum sample size is usually around 10% of the population, if this does not exceed 1000. The total number of respondents gathered was 424. 40 respondents were used to run the pilot test. Table 4.1 shows that the overall reliability for the independent and dependent variables has reached 0.7 upper and reached Cronbach's Alpha.

Table 4.1: Reliability test coefficient alpha from overall reliability (Pilot Test)

Variables	No. of Items	Cronbach's Alpha
Cybersecurity of Awareness (DV)	5	0.716
Attitude Factor (IV1)	5	0.722
Knowledge Factor (IV2)	5	0.806
Environmental Factor (IV3)	5	0.824

Therefore, this study applied 40 respondents for pilot test. The reliability of the independent and dependent variables for the pilot test for the 20 items gathered is shown in Table 4.1. The dependent variable and independent variable are Cybersecurity of Awareness, Attitude factor, Knowledge factor and Environmental factor. The finding of pilot test shows that Cronbach's Alpha for the dependent variable and independent variable is upper than 0.7. The Cronbach's Alpha is 0.716 (SA), 0.722 (AF), 0.806 (KF), 0.824 (EF). It can be concluded that Cronbach's Alpha for the overall reliability is accepted for this study because the reliability is higher than 0.7 and above.

4.3 Descriptive Analysis

Descriptive analysis was performed on the interval scale factors that are dependent variables and independent variables to obtain frequency, per cent, mean, and standard deviation. This study consists of one dependent variable and three independent variables which are cybersecurity awareness, attitude factor, knowledge factor, and environmental factor. In Section C there are five items and Section D has 15 items. All the items were measured using a five-point Likert scale with values of strongly disagree (1), disagree (2), neutral (3), agree (4), and strongly agree (5).

4.3.1 Demographic Profile of Respondent

Among the 384 respondents in the study, the largest age group is 19-22 years old, making up 28.6% of the total. The age group of 23-26 years old accounts for 46.9% of the total. The younger age groups of 11-14 years and 15-18 years also contribute significantly, with 10.4% and 14.1%, respectively. In terms of gender, the representation is equal, with females making up 54.9%, which is 211 respondents, and males making up 45.1% with 173 responses. The academic level

of participants shows the largest frequency in the university level group, which accounts for 40.4% with 155 respondents. Primary-level respondents had the lowest frequency, with 47 responses and 12.2%. Secondary level and STPM/Diploma categories represent 17.2% and 30.2% of the total, with 66 and 116 respondents. The marital status of respondents shows a high percentage of single status, which is 86.5% with 332 respondents. The married group has the lowest frequency, with 13.5%, which is 52 respondents. Most participants, 58.3%, are students with 224 responses. Employed people account for 32.3% with 124 responses of the population, the second greatest frequency. The unemployed had the lowest frequency, which is 36 responses with 9.4%.

Table 4.2: Demographic Profile of Respondent

Category		**Frequency (n=384)**	**Percentage (%)**
Age	11-14 years	40	10.4
	15-18 years	54	14.1
	19-22 years	110	28.6
	23-26 years	180	46.9
Gender	Female	211	54.9
	Male	173	45.1
Academic Level	Primary Level	47	12.2
	Secondary Level	66	17.2
	STPM/ Diploma	116	30.2
	University Level	155	40.4
Marital Status	Married	52	13.5
	Single	332	86.5
Occupation	Employed	124	32.3
	Student	224	58.3
	Unemployed	36	9.4

4.3.2 Cybersecurity Awareness

Table 4.3 shows the number, mean, and standard deviation of respondents based on the dependent variable which is cybersecurity awareness. The highest mean for cybersecurity awareness is 3.99. It means that respondents tend to agree to identify potential signs of a cybersecurity awareness attack, such as suspicious emails or messages. Next, the second highest mean score is 3.94 and

the respondent understands the statement I am aware of the risks associated with sharing personal information on the TikTok application. The lowest mean score is 3.59 on the statement I know common cybersecurity threats, such as phishing and malware. It shows that the respondent did not have a lot of information about the cybersecurity threats. The overall standard deviation is less than 1 which means all the respondents understand and can answer the questionnaire. Most respondents have a moderate level of awareness of cybersecurity awareness. This can be seen based on the mean score for most items being at a moderate level.

Table 4.3: Descriptive Analysis of Cybersecurity Awareness

Section	Item	N	Mean	Std. Deviation	Level of Awareness
C1	I know common cybersecurity threats, such as phishing and malware.	384	3.59	.930	Moderate
C2	I regularly update my passwords to enhance my TikTok account security.	384	3.66	.978	Moderate
C3	I stay informed about the latest cybersecurity trends and best practices.	384	3.69	.905	Moderate
C4	I am aware of the risks associated with sharing personal information on the TikTok application.	384	3.94	.868	Moderate
C5	I can identify potential signs of a cybersecurity attack, such as suspicious emails or messages.	384	3.99	.832	Moderate
TOTAL			3.77		Moderate

4.3.3 Attitude Factor

Table 4.4 shows the number, mean, and standard deviation of respondents based on the first independent variable which is attitude factors. The highest mean for the attitude factor is 3.90. That means the respondent agrees and understands the statement that I am attentive to the accuracy of the information about acquaintances on the TikTok application and in my perspective, I can determine whether the information shared on TikTok is true or not. The second highest mean

is 3.89. It means that the respondent agrees and knows that I am aware of whom I share information about on the TikTok application and the second statement is I only share information about people whom I truly trust. Last, the lowest mean is 3.66 on the statement I ensure that the information updated on my TikTok account is accurate. The overall standard deviation is less than 1 which means all the respondents of GenZ can understand and answer the questionnaire. Most of the respondents have a moderate level of awareness based on the mean score.

Table 4.4: Descriptive Analysis of Attitude Factor

Section	Item	N	Mean	Std. Deviation	Level of Awareness
D1	I ensure that the information updated on my TikTok account is accurate.	384	3.66	.962	Moderate
D2	I am attentive to the accuracy of the information about acquaintances on the TikTok application.	384	3.90	.867	Moderate
D3	I am aware of whom I share information about on the TikTok application.	384	3.89	.890	Moderate
D4	I only share information about people whom I truly trust.	384	3.89	.947	Moderate
D5	In my perspective, I can determine whether the information shared on TikTok is true or not.	384	3.90	.887	Moderate
TOTAL			3.84		Moderate

4.3.4 Knowledge Factor

Table 4.5 shows that indicates the mean value for the second independent variable which is the knowledge factor. The highest mean for the knowledge factor is 3.93. This shows that the respondent agrees with the statement I am aware of cyberbullying on the TikTok application. The second highest mean is 3.86. The respondent also agrees that they know about cyber fraud (scam) on the TikTok application. Meanwhile, the lowest mean is 3.47 whereby the respondents think

that they have less information about cyber laws in Malaysia. As for the overall standard deviation, less than 1 means all the respondents can answer the questionnaire well. Most respondents have a moderate level of awareness of the knowledge factor. This can be seen based on the mean score for most questions being at a moderate level.

Table 4.5: Descriptive Analysis of Knowledge Factor

Section	Item	N	Mean	Std. Deviation	Level of Awareness
D6	I know about cyber laws in Malaysia.	384	3.47	.887	Moderate
D7	I am aware of cybersecurity awareness programs on the TikTok application.	384	3.76	.830	Moderate
D8	I know about cyber surveillance on the TikTok application.	384	3.76	.863	Moderate
D9	I know about cyber fraud (scam) on the TikTok application.	384	3.86	.903	Moderate
D10	I am aware of cyberbullying on the TikTok application.	384	3.93	.875	Moderate
TOTAL			3.75		Moderate

4.3.5 Environmental Factor

Table 4.6 shows the statement, mean, and standard deviation for the environment factor. The highest mean for the environment factor is 3.78. This means that the respondent agrees with the statement that my friends always keep an eye on every activity I do on TikTok. Next, the second highest mean is 3.76. This shows that the respondent also agrees that I always remind each other about cybersecurity issues on TikTok with my parents. On the other hand, the lowest mean is 3,45 and some respondent thinks that the statement I always share information about cybersecurity awareness on TikTok with my friends gives less contribution. The overall standard deviation is less than 1 which means the entire respondent understands the questionnaire. However, there is one statement that scores the highest standard deviation is 1.019.

Table 4.6: Descriptive Analysis of Environmental Factor

Section	Item	N	Mean	Std. Deviation	Level of Awareness
D11	I always share information about cybersecurity awareness on TikTok with my friends.	384	3.45	.993	Moderate
D12	I always discuss cybersecurity threats on TikTok with my friends.	384	3.70	.902	Moderate
D13	My parents always monitor every activity I do on TikTok.	384	3.61	.931	Moderate
D14	I always remind each other about cybersecurity issues on TikTok with my parents.	384	3.76	.922	Moderate
D15	My friends always keep an eye on every activity I do on TikTok.	384	3.78	1.019	Moderate
TOTAL			3.66		Moderate

4.4 Validity and Reliability

This section presents the research findings from the validity and reliability test. According to Roberts & Priest (2006), validity describes the extent to which a measure represents the concept that is alleged to be measured accurately. The verification aims to ensure that the measurement used contains certain characteristics and can be maintained so that the study results are accurate. The survey form also contains 29 questions submitted to respondents consisting of 4 parts namely A, B, C and D.

A reliability test is used to analyze Cronbach's Alpha values. According to Edwin (2019), reliability has been defined as a measure of stability over a variety of conditions in which results should be obtained. In this section, Cronbach's Alpha is used to test the reliability scale to determine whether each statement is positively correlated with another statement. This reliability also contains 384 sets of surveys, and the results are also shown in Table 4.7.

Based on Table 4.7, the result of the study shows Cronbach's Alpha for the dependent variable and the independent variable. Next, the Cronbach's Alpha value for the dependent variable of cybersecurity awareness is 0.775, then the value for the independent variable for the attitude factor is 0.833, the next value for the knowledge factor is 0.841, and the value for the environment factor is 0.854. Based on the reliability test, it was found that each questionnaire question showed a good indication. From Table 4.7, it is also found that the reliability test results are mostly high and above 0.5. This also means that this decision was accepted and answers the objective perfectly. Overall, the test results for reliability range from 0.775 to 0.854, which is considered a good range for the study. This study found that all four variables have a good level of reliability and consistency.

Table 4.7: Reliability Test Results of the Study

Variables	Dimensions	Cronbach's Alpha	Number of Items
Dependent Variable	DV	.775	5
Independent	IV1	.833	5
Variable	IV2	.841	5
	IV3	.854	5

4.5 Normality Test

Table 4.8 shows the results of the Kolmogorov-Smirnov test and the Shapiro-Wilk test that is being carried out in this normality test. The second of the two tests found that the values of all variables were abnormal data, that is, (p = 0.00) on the dependent variable and the independent variable. This will also be considered normal if the data sig Shapiro-Wilk test shows a value above 0.05. If the value is also less than 0.05, then the data is also abnormal for both variables. One of the reasons is that GenZ also does not care about cybersecurity awareness in Kelantan.

Table 4.8: Test of Normality

Variables	Kolmogorov - Smirnov			Shapiro – Wilk		
	Statistics	df	Sig.	Statistics	df	Sig.
DV	.104	384	.000	.973	384	.000
IV1	.152	384	.000	.957	384	.000
IV2	0.98	384	.000	.971	384	.000
IV3	.104	384	.000	.964	384	.000

4.6 Spearman ‘s Rho Correlation Coefficient

This study uses the Spearman rank correlation coefficient to show a statistical measure of the strength of the relationship between two variables, which is to identify a significant relationship between the independent variable (Cybersecurity awareness of GenZ TikTok application users) and the independent variable (Attitude Factor, Knowledge Factor, and Environmental factor). Spearman’s correlation coefficients range from -1 to +1. The sign of the coefficient indicates whether it is a positive or negative monotonic relationship. A positive correlation means that as one variable increases, the other variable also tends to increase. A negative correlation signifies that as one variable increases, the other tends to decrease. Values close to -1 or +1 represent stronger relationships than values closer to zero. Table 4.9 shows categorizing correlations by strength. A very weak correlation (0.00 to 0.19 or -0.00 to -0.19) implies minimal linear association, a weak correlation (0.20 to 0.39 or -0.20 to -0.39) suggests a modest relationship, a moderate correlation (0.40 to 0.69 or -0.40 to -0.69) signifies a more substantial connection, a strong correlation (0.70 to 0.89 or -0.70 to -0.89) indicates a clear and robust relationship, and a very strong correlation (0.90 to 1.00 or -0.90 to -1.00) reflects an almost perfect linear association between variables.

Table 4.9: Interpretation table of Spearman rank-order correlation coefficients

Value of coefficient	Positive	Negative
Very weak correlation	0.00 to 0.19	-0.00 to -0.19
Weak correlation	0.20 to 0.039	-0.20 to -0.039
Moderate correlation	0.40 to 0.69	-0.40 to -0.69
Strong correlation	0.70 to 0.89	-0.70 to -0.89
Very strong correlation	0.90 to 1.00	-0.90 to -1.00

Table 4.10: The result of Spearman ‘s Rho correlation coefficient

			DV	IV1	IV2	IV3
Spearman's rho						
	DV	Correlation Coefficient	1.000	.823**	.772**	.707**
		Sig. (2-tailed)	.000	.000	.000	.000
		N	384	384	384	384
	IV 1	Correlation Coefficient	.823**	1.000	.849**	.728**
		Sig. (2-tailed)	.000	.	.000	.000
		N	384	384	384	384
	IV 2	Correlation Coefficient	.772**	.849**	1.000	.795**
		Sig. (2-tailed)	.000	.000	.	.000
		N	384	384	384	384
	IV 3	Correlation Coefficient	.707**	.728**	.795**	1.000
		Sig. (2-tailed)	.000	.000	.000	.
		N	384	384	384	384

Table 4.11: Result of hypothesis based on the Spearman correlation between DV and IV

Hypothesis	Result	Spearman Correlation	Status	Conclusions
H1 There is a positive relationship between attitude factors and cybersecurity awareness among GenZ users of the TikTok application.	P < 0.01	0.823	Accepted	Strong positive correlation
H2 There is a positive relationship between knowledge factor and cybersecurity awareness among GenZ users of the TikTok application.	P < 0.01	0.772	Accepted	Strong positive correlation
H3 There is a positive relationship between environmental factors and cybersecurity awareness among GenZ users of the TikTok application.	P < 0.01	0.702	Accepted	Strong positive correlation

4.7 Squares-Structural Equation Modelling (PLS-SEM)

In this study, we also used SmartPLS, which is a software application for variance-based structural equation modelling (SEM) that is widely used in research because of its ability to handle complex models and small sample sizes. The utilization of SmartPLS as a variance-based structural equation modelling (SEM) tool played a pivotal role in enhancing the robustness and precision of the data analysis. SmartPLS greatly aids research to analyze mediation models, path analysis and process models, making it a valuable tool for conducting sophisticated data analysis (Abdel-Basst, 2020) Indirectly, we can collect and process a large amount of information to assist in the decision-making and development process, especially in the context of evaluating the innovation's value proposition regarding the familiarity of cybersecurity awareness of TikTok users among GenZ. Figures 4.1 and 4.2 show the outcomes of the analysis conducted using SmartPLS. These results showcased the findings from the PLS-SEM Algorithm result and PLS-SEM Bootstrapping result.

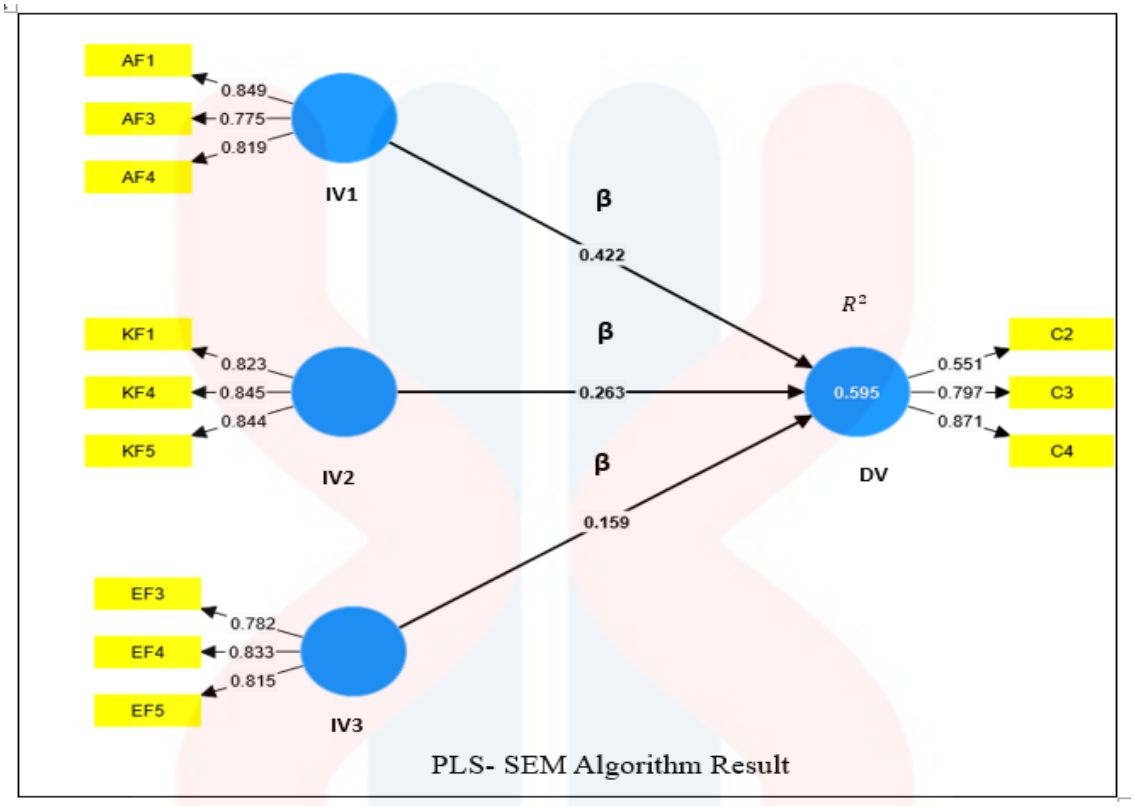


Figure 4.1: PLS-SEM Algorithm

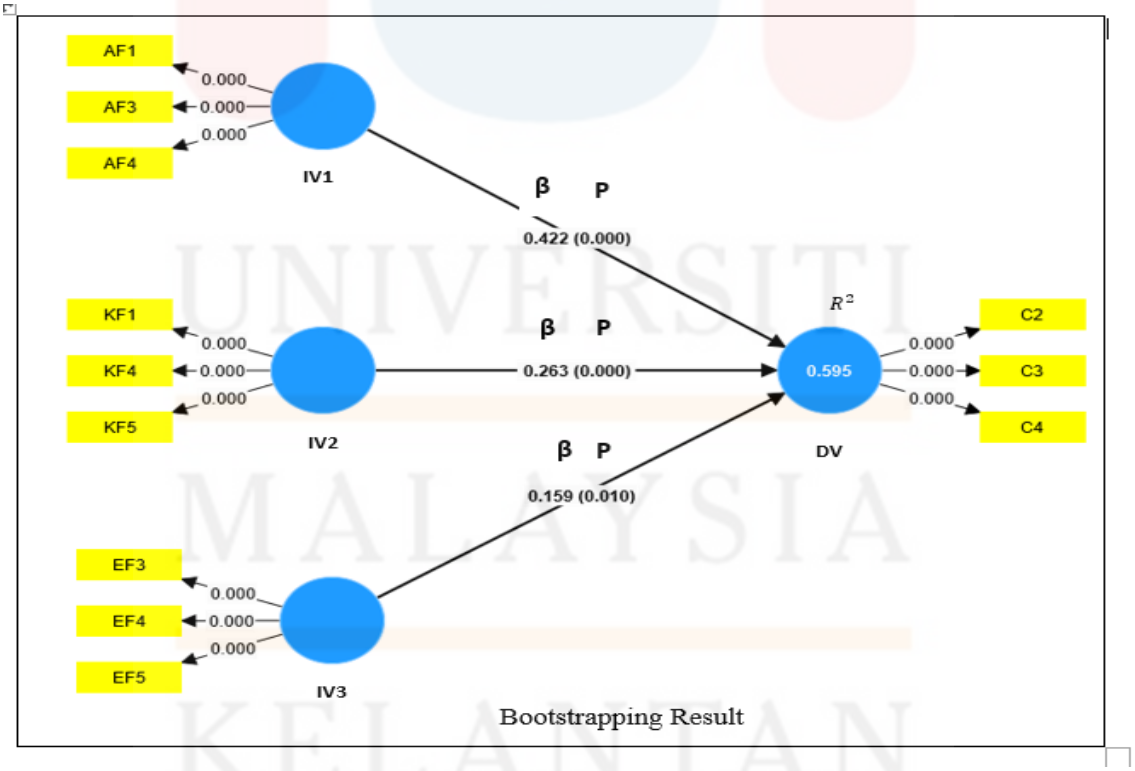


Figure 4.2: PLS-SEM Bootstrapping result

Table 4.12: Hypothesis test result from SmartPLS

Hypothesis	Variables	Path Coefficient	Significant Value, P	Remarks
H1	IV1-DV	0.422	0.000	Supported
H2	IV2-DV	0.263	0.000	Supported
H3	IV3-DV	0.159	0.010	Supported

Table 4.12 shows the analysis results to support Hypothesis 1, indicating a significant relationship between Independent Variable 1 (IV1) and the Dependent Variable (DV). The estimated path coefficient of 0.422 signifies the strength and direction of this relationship. Importantly, the associated p-value of 0.000, being less than the conventional significance threshold of 0.05, establishes the statistical significance of the observed relationship. This implies a high level of confidence in the result, suggesting that the impact of IV1 on DV is not due to random chance. Consequently, based on the robust statistical evidence, it can be concluded that there is a substantively meaningful and statistically significant association between IV1 and DV in the studied model.

Hypothesis 2 indicates a noteworthy relationship between Independent Variable 2 (IV2) and the Dependent Variable (DV). The path coefficient, which measures the strength and direction of this relationship, is estimated at 0.263. Additionally, the associated p-value of 0.000 is below the commonly accepted significance threshold of 0.05, establishing the statistical significance of the observed connection. This low p-value suggests that the likelihood of obtaining such results by random chance is highly improbable. Therefore, with a high level of confidence, it can be concluded that there exists a substantively meaningful and statistically significant relationship between IV2 and DV in the examined model, emphasizing the impact of IV2 on the variation in the Dependent Variable.

The findings substantiate Hypothesis 3, underscoring a significant relationship between Independent Variable 3 (IV3) and the Dependent Variable (DV). The estimated path coefficient

of 0.159 quantifies the strength and direction of this association. While the associated p-value of 0.010 is below the conventional 0.05 threshold, it still attests to the statistical significance of the observed relationship, albeit at a moderate confidence level. This implies that the likelihood of the observed result occurring by random chance is relatively low. In summary, the results of Hypothesis 3 contribute to the cumulative evidence supporting the existence of statistically significant relationships between each of the independent variables (IV1, IV2, IV3) and the dependent variable (DV) in the model, providing valuable insights into the interplay among these variables.

4.8 Hypotheses Testing

One of the most important analyses that examined the linear relationship between the two variables was the Spearman correlation analysis. The goal of this study is to find the relationship between the independent variables (Attitude factor, Knowledge factor, and Environmental factor) and the dependent variable (Cybersecurity awareness of GenZ TikTok application users). Researchers should decide if the amount of connection strength is satisfactory when the relationship is significant.

4.8.1 Hypothesis 1

There is a relationship between the Attitude Factor (AF) and Cybersecurity Awareness (SW) (AF → SW).

Table 4.13: Spearman's Correlation Coefficient Analysis (Attitude Factor)

	Cybersecurity Awareness	Attitude Factor
Spearman's rho	1	.823**
Sig. (2-tailed)		.000
N	384	384

H1: There is a significant relationship between attitude and cybersecurity awareness among GenZ users of the TikTok application. The table shows that there is a strong positive correlation (Spearman correlation coefficient = .823) between the dependent variable (Cybersecurity Awareness) and the independent variable (Attitude Factor). The very low p-value (.000) suggests that this correlation is statistically significant, providing evidence against the null hypothesis of no correlation.

4.8.2 Hypothesis 2

There is a relationship between Knowledge factor (KF) and cybersecurity awareness (SW) (KF → SW).

Table 4.14: Spearman's Correlation Coefficient Analysis (Knowledge Factor)

	Cybersecurity Awareness	Knowledge Factor
Spearman's rho	1	.772**
Sig. (2-tailed)		.000
N	384	384

H2: There is a significant relationship between the knowledge factor and the cybersecurity awareness of GenZ TikTok application users. The table shows that there is a strong positive

correlation (Spearman's correlation coefficient = .772) between the dependent variable (Cybersecurity Awareness) and the independent variable (Knowledge Factor). The very low p-value (.000) suggests that this correlation is statistically significant, providing evidence against the null hypothesis of no correlation.

4.8.3 Hypothesis 3

There is a relationship between Environmental factors (EF) and cybersecurity awareness (SW) (EF → SW).

Table 4.15: Spearman's Correlation Coefficient Analysis (Environmental Factor)

	Cybersecurity Awareness	**Environmental Factor**
Spearman's rho	1	.707**
Sig. (2-tailed)		.000
N	384	384

H3: There is a significant relationship between the environmental factor and the cybersecurity awareness of GenZ TikTok application users. The table shows that there is a strong positive correlation (Spearman's correlation coefficient = .707) between the dependent variable (Cybersecurity Awareness) and the independent variable (Environmental Factor). The very low p-value (.000) suggests that this correlation is statistically significant, providing evidence against the null hypothesis of no correlation.

4.9 Conclusion

Chapter 4 concludes with a discussion of the relationship between dependent variables (DV) that measure cybersecurity awareness. Additionally, there are three independent variables (IV) which are the attitude factor, knowledge factor, and environment factor. There was some information

obtained from the pilot test that was made to confirm the reliability of the questionnaire which proves the questionnaire is accepted or not for the actual survey. Next, normality data shows that all variables are normally distributed. Additionally, a descriptive analysis was completed to illustrate and clarify the segment profile and responses for the thing under investigation.

In this chapter 4 data analysis consists of an introduction, a preliminary analysis, a descriptive analysis, a validity and reliability test, a normality test, a spearman's rho correlation coefficient, squares-structural equation modeling (PLS-SEM), testing of hypotheses, and a conclusion. The following report is followed by Chapter 5 includes introduction, key findings, discussion, implications, limitations, recommendations for further research, and overall conclusion.

CHAPTER 5

DISCUSSION AND CONCLUSION

5.1 Introduction

The chapter explains the study's implications, including its limitations and recommendations.

5.2 Key Findings

Table 5.1 shows the findings of this study.

Table 5.1: The result of the hypotheses

Objective	Hypotheses	Result	Conclusion
To examine the influence of attitude factors on the cybersecurity awareness of the TikTok application among GenZ.	There is a significant relationship between attitude and cybersecurity awareness among GenZ users of the TikTok application.	R = 0.823 P = 0.000	There is a statistically significant and strong positive correlation between attitude factor and cybersecurity awareness among GenZ users of the TikTok application.
To investigate the correlation between knowledge factors and cybersecurity awareness of the TikTok application among GenZ.	There is a significant relationship between the knowledge factor and the cybersecurity awareness of GenZ TikTok application users.	R = 0.772 P = 0.000	There is a statistically significant and strong positive correlation between the knowledge factor and the cybersecurity awareness of GenZ TikTok application users.
To identify the relationship between environment factors and cybersecurity awareness of the TikTok application among GenZ.	There is a significant impact between the environment factor and the cybersecurity awareness of GenZ TikTok application users.	R = 0.707 P = 0.000	There is a statistically significant and strong positive correlation between environment factors and the cybersecurity awareness of GenZ TikTok application users.

5.3 Discussion

5.3.1 Hypothesis 1

According to Table 5.1, the hypothesis testing results indicate a significant relationship between attitude and cybersecurity awareness among GenZ users of the TikTok application, with a strong positive correlation (R = 0.823, P = 0.000). This suggests that the attitude of GenZ users influences their cybersecurity awareness when using the TikTok application. Therefore, the relationship between attitude and cybersecurity awareness among GenZ users of TikTok is considered statistically significant.

The attitude variables reflect the attitude and perception of GenZ towards cybersecurity. It involves a positive or negative assessment of security practices, perceptions of the importance and relevance of cybersecurity, as well as the level of motivation and readiness to adopt good security practices (Fattah et al., 2023). A positive assessment indicates that they believe in the importance of following security measures and consider them to be effective in protecting their personal information and privacy. If they perceive cybersecurity as important and relevant, they are more likely to prioritize and value security measures. A positive attitude towards cybersecurity would manifest as a willingness to learn about and implement security measures, such as using strong passwords, enabling two-factor authentication, and being cautious about sharing personal information online.

Based on these findings, it can be concluded that the attitude of GenZ users influences their cybersecurity awareness when using the TikTok application. This suggests that having a positive attitude towards cybersecurity is important for GenZ users to be more aware and cautious about potential cybersecurity risks while using TikTok. In conclusion, H1 is supported by a significant impact between the attitude factor and the cybersecurity awareness of GenZ TikTok application users.

5.3.2 Hypothesis 2

According to Table 5.1, the hypothesis testing results indicate a significant relationship between knowledge and cybersecurity awareness among GenZ users of the TikTok application, with a strong positive correlation (R = 0.772, P = 0.000). This suggests that the knowledge of GenZ users influences their cybersecurity awareness when using the TikTok application.

As can be seen in the analysis that has been carried out in this study which shows that Gen Z users who know cyber laws in their country are more likely to understand the importance of online privacy and security, which can influence their awareness of cybersecurity when using the TikTok application (Anonymous, 2023). This legal literacy appears to act as a catalyst, shaping their awareness of cybersecurity considerations when interacting with TikTok. Being well-versed in cyber laws empowers Gen Z individuals to navigate the digital landscape with greater discernment, recognizing potential risks and proactively addressing privacy concerns.

Not only that, GenZ users who are familiar with cybersecurity awareness programs on TikTok are more likely to engage with these programs and learn about online security measures, which can increase their cybersecurity awareness. This study also shows the same thing where awareness about cybersecurity programs plays an important role in increasing the awareness of TikTok application users about cybersecurity (Halim et.al, 2022). Therefore, H2 is supported by the significant relationship between knowledge and cybersecurity awareness among GenZ users of the TikTok application.

5.3.3 Hypothesis 3

According to Table 5.1, the hypothesis testing results indicate a significant relationship between environmental and cybersecurity awareness among GenZ users of the TikTok application, with a

strong positive correlation (R = 0.707, P = 0.000). This suggests that the environment of GenZ users influences their cybersecurity awareness when using TikTok.

Environmental factors, specifically parental and peer monitoring, play a significant role in influencing the awareness of GenZ individuals regarding cyber threats associated with TikTok. The research indicates that when parents and peers actively monitor and remind GenZ about cyber threats on TikTok, it has the potential to indirectly lead to more sustainable and secure online behaviour (Kokchang, 2023). This increased awareness and interest in cybersecurity can translate into more cautious and responsible behaviour when using applications like TikTok. GenZ individuals are likely to adopt safer online practices and be more mindful of potential risks, given the influence of their parents and peers.

The findings from data analysis in this study support the idea that environmental influences, such as parental involvement and peer influence, contribute significantly to raising awareness and interest in cybersecurity among GenZ. In other words, when parents take an active role in monitoring and reminding their children about potential cyber threats on TikTok, and when peers within the social circle also emphasize the importance of cybersecurity, it has a positive impact on GenZ individuals. In conclusion, H3 is supported by a significant impact between the environmental factor and the cybersecurity awareness of GenZ TikTok application users.

5.4 Implication of the Study

The findings of the study show the factors that influence cybersecurity awareness of the TikTok application among GenZ. As a result, after conducting a general discovery evaluation, some of the key implications should be discussed in this study. Based on the study findings, GenZ should be aware of cybersecurity threats such as scams and phishing. GenZ must know about the scam to avoid scamming in online applications, especially TikTok.

The next implication is enhancing user education programs. The findings can be used to develop targeted educational programmes aimed at increasing cybersecurity awareness among TikTok users, particularly those in GenZ. This may include tutorials, and campaigns to inform users about potential risks and best practices. Public awareness campaigns can be launched in Kelantan to educate students and the public about the importance of cybersecurity. To reach a larger audience, these campaigns could be carried out through schools, community centres, and online platforms.

In addition, user empowerment is also a finding of the study. In this study, especially in the GenZ demographic, can be more empowered to take control of their online security. This may involve adjusting privacy settings, using two-factor authentication, and being more discerning about sharing personal information on the platform. The finding also points out that people who have more knowledge of the various types of cybersecurity threats have a low probability of falling victim to cybersecurity crimes.

5.5 Limitation of Study

There are some limitations that have been found during this study. The first limitation in this study used a sample size from Kelantan to test the study model and hypotheses. Secondly, this study focused on Gen Z who was born between 1997 and 2012. Thirdly, only the elements of the Theory of Planned Behavior were used in this study.

Next, the scope of the study is limited. This study used one application which is the TikTok application. The awareness of cybersecurity is only explored among GenZ who used TikTok as their main application. Furthermore, the distribution of the questionnaire through platforms such as WhatsApp and Telegram introduces another limitation, as it may exclude individuals who do

not use these specific applications. Obtaining data and information may pose some challenges in completing this study.

5.6 Recommendations for Future Research

There were recommendations made that might be applied to this research in the future. The ideas presented in this proposal might prove beneficial for future research on this topic. For future research, we recommend increasing the sample size. This is because that information can be gathered from respondents in multiple states in addition to just one. Because it can expand the search for respondents in different states, this can help the researcher process the data more quickly, especially if the researcher is conducting a state-wide study project.

To increase the scope of respondents. This is also due to the possibility that respondents to the survey may belong to generations other than GenZ, or those born between 1997 and 2012. For example, adding Generations X and Y to the research project for the next. This can also add more ideas and knowledge for expanding this study. Expanding the scope of respondents may help this study progress in the future.

In addition to model theory. This is because this research project only uses the Theory of Planned Behavior elements. However, future studies can also use additional theories such as the Theory of Reason Action (TRA). TRA is also a theory in the field of social psychology that focuses on a person's intention to behave in a certain way in a certain situation. Therefore, the addition of two theories can also be used in future studies.

An additional platform. This is because this study only uses one application, TikTok, to investigate the threat of cybercrime. However, the next study can also use this application, including Shoppe, WhatsApp, Facebook, Instagram, and so on. The next study can also apply this

application in addition to TikTok as a reference for other research projects. Therefore, adding another platform to the study can also increase the researcher's ideas for continuing this research topic.

In conclusion, the recommendations displayed in the above section can also be used in the future in conducting this study. This also gives the researcher the advantage of continuing this study for several periods set by the guidance teacher.

5.7 Overall Conclusion of the Study

In conclusion, the purpose of this study is to identify dependent and independent variables that affect cybersecurity awareness in GenZ using the TikTok application. This research project has fulfilled its objective of determining the effect on the three variables, namely attitude factor, knowledge factor, and environment factor. Apart from that, 384 respondents answered this survey through a Google Form, and we have also conducted a pilot test on 40 GenZ people. SPSS version 26 software is used to collect and analyze data that provides descriptive statistics, reliability analysis, and correlation analysis. The results show that all three variables, including the dependent variable, have a positive and significant relationship with the use of the TikTok application among GenZ. As a result, all variables are interrelated and will influence the use of the TikTok application among GenZ.

REFERENCES

Abdel-Basst, M. &. (2020). *A novel framework to evaluate innovation value proposition for smart product–service systems. Environmental Technology & Innovation Volume 20, November 2020, 101036.*

Agency, N. C. (2023, September 7). *Cyber crime*. Retrieved from https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

Ahmad, N., & et.al. (2018). Cybersecurity Situational Awareness among Parents. *IEEE Xplore*.

Ahmed, N. L. (2021). *Purchase intention toward organic food among young consumers using theory of planned behavior: role of environmental concerns and environmental awareness. Journal of Environmental Planning and Management, 64(5), 796-822.*

Ajzen, I. (2015). *Belief, attitude, intention and behaviour: An introduction to theory and research.* Reading, MA: Addison-Wesley.

Ajzen, I. a. (1980). *Understanding Attitudes and Predicting Social Behavior*. Retrieved from https://www.scirp.org/(S(czeh2tfqw2orz553k1w0r45))/reference/referencespapers.aspx?referenceid=1826547

Alanazi, M. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computer in Human Behavior*.

Alili, S. (2023). *Gen Z's social media usage in 2023: Later. Later Social Media Marketing*. Retrieved from https://www.thestar.com.my/tech/tech-news/2023/09/15/three-quarters-of-gen-z-use- TikTok-as-a-search-engine

Alves, C. (2023). *How Gen Z Are Using Social Media*. Retrieved from https://www.searchenginejournal.com/social-media-gen-z/485152/#close

Anonymous. (2022). Retrieved from Cybersecurity Awareness: Definition, Importance & More. Spanning. : https://spanning.com/blog/cybersecurity-awareness/

Anonymous. (2023). *Information Security: The Ultimate Guide imperva a Thales company*. Retrieved from Information Security: The Ultimate Guide imperva a Thales company: https://www.imperva.com/learn/data-security/information-security-infosec/

Anonymous. (2023). *Nearly half of US TikTok users worry about their privacy.* Surfshark. Retrieved from surfshark: https://surfshark.com/research/chart/views-on-TikTok-privacy

Anonymous. (2023, December 12). *Protecting SME From Cyber Attacks kkd.gov.my*. Retrieved from https://www.kkd.gov.my/en/pengumuman-kkmm/233-kkd-news/19611-protecting-sme-from-cyber-attacks

Anonymous. (n.d). *What Is Generation Z?* Retrieved from PeopleHum: https://www.peoplehum.com/glossary/generation-z

Anonymous. (n.d.). *SurveyMonkey*. Retrieved from https://www.surveymonkey.com/market-research/resources/pearson-correlation-vs-spearman-correlation/#:~:text=What%20is%20the%20Spearman%20correlation

Apps, S. C. (2022, june 30). *Cybersecurity Awareness: Definition, Importance, Purpose and Challenges*. Retrieved from Spanning Kaseya Company: https://spanning.com/blog/cybersecurity-awareness/

Bandhari, P. (2021, December 8). Missing Data | Types, Explanation, & Imputation.

Bazargan-Hejazi, S. T. (2016). *The theory of planned behavior (TPB) and texting while driving behavior in college students. Traffic Injury Prevention, 18(1), 56–62.*

Bhat, A. (2018). *Research Design: What it is, Elements & Types*. Retrieved from https://www.questionpro.com/blog/research-design/

Bhat, A. (2020). *Levels of Measurement: "Nominal Ordinal Interval Ratio"*. Retrieved from https://www.scirp.org/(S(351jmbntvnsjt1aadkozje))/reference/referencespapers.aspx?referenceid=1138634

Bhat, I. H. (2018). Analyzing the Moderating Effect of Entrepreneurship Education on The Antecedents of Entrepreneurial Intention. *Journal Entrepreneurship Education*.

Bhatnagar, N. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study . *Information Systems Education Journal (ISEDJ), 18(1).*

Blog, F. (2023, December 19). *Pilot Survey*. Retrieved from Definition, Importance + [Question Examples]. Www.formpl.us.: https://www.formpl.us/blog/pilot-survey-questionnaire#:~:text=The%20main%20objective%20of%20a

Bosnjak, M., & et.al. (2020). The Theory of Planned Behavior: Selected Recent Advances and Applications. *Europe's Journal of Psychologyejop.psychopen.eu | 1841-0413*.

Bullen, P. (2013, October 18). *How to choose a sample size (for the statistically challenged)*. Retrieved from https://tools4dev.org/resources/how-to-choose-a-sample-size/#:~:text=A%20good%20maximum%20sample%20size

Catal, C., & et.al. (2022). Analysis of cybersecurity knowledge gaps based on cybersecurity body of knowledge. *Education and Information Technologies, 28(2), 2405-2405.*

Chang, C.-W. C.-H. (2023). The Impact of Digital Disruption: Influences of Digital Media and Social Networks on Forming Digital Natives' Attitude. *SAGE Open, 13(3).*

Chiara, M. (2022). *Awaraness.Academia Letters.* Retrieved from https://www.academia.edu/71115586/Awareness

Cisco. (2019). *What Is Network Security?* Retrieved from Cisco: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

Coe, E., & et.al. (2023). Gen Z mental health: The impact of tech and social media. *McKinsey & Company*.

Cramer, H. a. (2010). *Introduction to Research Methods in Psychology. 3rd Edition*.

Edwin, K. (2019, September). *Reliability and Validity of Research Instruments Correspondence* Retrieved from https://www.researchgate.net/publication/335827941_Reliability_and_Validity_of_Research_Instruments_Correspondence_to_kubaieinyahoocom

Eka Zahra Solikahan, A. M. (2019). entrepreneurial orientation, market orientation and financial orientation in supporting the performance of karawo smes in gorontalo city. *Semantic Scholar*.

Eldridge, A. (2023). *Gen Z | Years, Age Range, Meaning, & Characteristics.* Retrieved from Encyclopedia Britannica.: https://www.britannica.com/topic/Generation-Z

Emani, S. H. (2016). *Awareness and Use of the After-Visit Summary Through a Patient Portal: Evaluation of Patient Characteristics and an Application of the Theory of Planned Behavior. Journal of Medical Internet Research, 18(4), e77*. Retrieved from https://www.jmir.org/2016/4/e77

Ettisa, D. L. (2023). The Impact of TikTok on Students: A Literature Review. *Qeios*.

Fattah, A. W. (2023). *Enhancing Cybersecurity Awareness among University Students: A Study on the Relationship between Knowledge, Attitude, Behavior, and Training. JSI: Jurnal Sistem Informasi (E-Journal), 15(1).* .

Garba, A. A., & et.al. (2020). A Study on Cybersecurity Awareness Among Students in Yobe: A Quantitative Approach. *International Journal on Emerging Technologies, 11(5),*.

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.*

Halim, F., & et.al. (2022). Determinants of Intention to Use the TikTok Application among Generation Z. *Ideas Jurnal Pendidikan Sosial dan Budaya 8(3):721*.

Ham, M. (2015). The role of subjective norms in forming the intention to purchase green food.

Economic Research-Ekonomska Istraživanja, 28(1), 738-748.
Herath, T. B., & et.al. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *Journal Of Cybersecurity and Privacy, 2(1), 1-18*.
Hong, W. C., & et.al. (2022). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Education and Information Technologies*.
Ibrahim, C. H. (2014). Kajian Penerokaan Buli Siber Dalam Kalangan Pelajar UMT. *Procedia - Social and Behavioral Sciences, 134, 323-329*.
Jenkins. (2017). *4 Reasons Generation Z will be the most different generation*. Retrieved from Ryan Jenkins: https://blog.ryan-jenkins.com/2017/01/26/4-reasons-generation-z-will-be-the-most-different-generation
Jenkins, R. (n.d.). *4 Reasons Generation Z Will Be The Most Different Generation*. Retrieved from https://blog.ryan-jenkins.com/2017/01/26/4-reasons-generation-z-will-be-the-most-different-generation
Johnson, F. (2023). *Why Apps Like TikTok Can Be a Security Issue for Your Business.* Info Security Magazine.
Johnson, R. B. (2015). Educational Research Quantitative, Qualitative, and Mixed Approaches Fifth Edition. *SAGE Publication, Inc*.
Kamalulail., A., & et.al. (2022). Awareness of Cybersecurity: A Case Study in UiTM Negeri Sembilan Branch, Seremban Campus. *E-Academia Journal, 11(1)*.
Karol Król, D. Z. (2020). Social media use and its impact on intrinsic motivation in Generation Z: a case study from Poland. *Global Knowledge, Memory and Communication, 70(4/5), 442-458*.
Kaspersky. (2019). *What is Cybersecurity?* Retrieved from Kaspersky.com.: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
Kokchang, D. I. (2023). Factors Influencing Generation Z's Pro-Environmental Behavior towards Indonesia's Energy Transition. *Sustainability 2023, 15, 13485.* .
Kovacevic, A., & et.al. (2020). Factors Related to Cybersecurity Behavior. *Factors Related to Cybersecurity Behaviour. IEEE Acces, 8, 125140-125148.*
Kumar, A. a. (2021). Cybersecurity Awareness and Behaviors on Social Media Platforms. *Journal Oof Cybersecurity, 6(1), cyab013*.
Mail, M. (2022). *cybercrime cases reported from January to July this year.* Retrieved from https://www.malaymail.com/news/malaysia/2022/08/05/police-11367-cybercrime-cases-reported-from-january-to-july-this-year/21316
Malebana, S. T. (2022). Effects of Gender on Students' Entrepreneurial Intentions: A Theory of Planned Behaviour Perspective. *Open Journal of Business and Management > Vol.10 No.1, January 2022*.
MeiKeng, Y. (2020). *Cybersecurity cases rise by 82.5% | The Star.* Retrieved from https://www.thestar.com.my/news/focus/2020/04/12/cybersecurity-cases-rise-by-825
Mishra, P., & et.al. (2019). *Descriptive statistics and normality tests for statistical data*. Retrieved from https://pubmed.ncbi.nlm.nih.gov/30648682/
Montag, C., & et.al. (2021). On the Psychology of TikTok Use: A First Glimpse From Empirical Findings. *Frontiers in Public Health, 9(1).*
Munien, R. (2010). Internet phishing hook, line and hopefully not sunk . *MBA thesis*.
Niekerk, R. R. (2016). Decoding audience interpretations of awareness campaign messages. *Information and Computer Security, 24(2), 177-193.*
Patel, R. D. (2017). Cybersecurity for Social Networking Sites: Issues, Challenges and Solution. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*.

Pinto, S. K. (2022). *Impact of a Public Health Awareness Campaign on Patients' Perceptions of Expanded Pharmacy Services in South Dakota Using the Theory of Planned Behavior. Pharmacy, 10(6), 178.* . Retrieved from https://www.mdpi.com/2226-4787/10/6/178

Pitchan, M. A. (2017). *Kesedaran dan amalan keselamatan siber dalam kalangan pengguna internet di Malaysia Doctoral thesis, Universiti Putra Malaysia.*

Pitchan, M. A., & et.al. (2017). *Analisis Keselamatan Siber Dari Perpekstifpersekitaran Sosial: Kajian Terhadap Pengguna Internet Di Lembah Klang Journal of Social Sciences and Humanities Vol. 12, No. 2 (2017) 016-029, ISSN: 1823-884x*.

Pitchan, M. A., & et.al. (2019). *Amalan Keselamatan Siber Pengguna Internet terhadap Buli Siber, Pornografi, E-Mel Phishing & Pembelian dalam Talian journal komunikasi: Malaysian Journal Of Communication*.

Potters, C. (2023). *Demographics: How to Collect, Analyze, and Use Demographic Data*. Investopedia.

Rahman, M. S. (2021). Analysis Regresion and Path Model: The Influence Both Instagram and TikTok in Improving Students Vocabulary. *Sketch Journal, 1(1), 48-61*.

Rhodes, R. E. (2003). *Investigating multiple components of attitude, subjective norm, and perceived control: An examination of the theory of planned behaviour in the exercise domain. British Journal of Social Psychology, 42(1), 129–146.* .

Roberts, J. (2023, january 27). Where Does Gen Z Spend the Majority of Their Time Online? *Gen Z's Social Media Usage: Where Do They Spend Their Time Online?*

Roberts, P. &. (2006). *Reliability and validity in research. Nursing Standard, 20(44), 41–45.* . Retrieved from https://doi.org/10.7748/ns2006.07.20.44.41.c6560

Salamah, F. B. (2023). An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work. *Applied Sciences, 13(17),9595*.

Sekaran, N., & et.al. (2013). Fall-Associated Difficulty with Activities of Daily Living in Functionally Independent Individuals Aged 65 to 69 in the United States: A Cohort Study. *Journal of the American Geriatrics Society, 61(1), 96-100.*

Sharabati, A.-A. A., & et.al. (2022). The Impact of TikTok User Satisfaction on Continuous Intention to Use the Application. *Journal of Open Innovation: Technology, Market, and Complexity, 8(3), 125.*

Sigh, S. (2023). What is research design? Understand types of research design, with examples. *Reseacher.Life*.

Sileyew, K. J. (2019). *Research Design and Methodology.* intenchopen.

Smith, J. A., & et.al. (2022). Interpretative Phenomenological Analysis Theory, Method and Research. *SAGE Publications Ltd*.

Tasevski, P. (2016). IT and Cybersecurity Awareness – Raising Campaigns. *Information & Security: An International Journal, 34,7-22*.

TikTok. (2023, October 19). *#BeCyberSmart for Cybersecurity Awareness Month 2023 TikTok*. Retrieved from #BeCyberSmart for Cybersecurity Awareness Month 2023 TikTok TikTok: https://newsroom.TikTok.com/en-us/becybersmart-for-cybersecurity-awareness-month-2023

TikTok. (2023). *About | TikTok - Real Short Videos.* Retrieved from TikTok.com.: https://www.TikTok.com/about?lang=en

Tufts, U. (2023). *Social Media Overview*. Retrieved from University Communication and Marketinng: https://communications.tufts.edu/marketing-and-branding/social-media-overview/

Tyson, A., & et.al. (2021). *Gen Z, Millennials Stand Out for Climate Change Activism, Social Media Engagement with Issue.* Pew Research Center.

White Baker, E. A.-G. (2007). *The effects of gender and age on new technology implementation*

in a developing country. Information Technology & People, 20(4), 352–375.
Wilson, K., & et.al. (2010). Psychological predictors of young adults' use of social networking sites. *Cyberpsychology, behavior, and social networking, 13(2), 173-177.*
Yamin, E. A. (2023). *Beware of new scam tactic on Facebook and TikTok using Tabung Haji logo* |. Retrieved from New Straits Times. NST Online.: https://www.nst.com.my/news/nation/2023/10/969725/beware-new-scam-tactics-facebook-and-TikTok-using-tabung-haji-logo
Zakiah Saizan, D. S. (2019). cybersecurity awareness among social media users: case study in german-malaysian institute (GMI). *Asia-Pacific Journal of Information Technology & Multimedia, 07(02(02)), 111-127.*
Zhiyong Zhang, B. B. (2018). Social media security and trustworthiness: Overview and new direction. *Future Generation Computer Systems, 86(1), 914-925.*
Zulkifli, Z., & et.al. (2020). Cybersecurity Awareness Among Secondary School Students in Malaysia. *Journal of Information System and Digital Technologies*.
Zwilling, M., & et.al. (2020). Cybersecurity Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems, 62(1), 82-97.*

APPENDIX A

QUESTIONNAIRE

A STUDY OF CYBERSECURITY AWARENESS OF TIKTOK APPLICATION AMONG GENZ IN KELANTAN.

Dear respondent,

This survey is conducted to study the Cybersecurity Awareness of TikTok Application Among GenZ in Kelantan. Congratulations on being selected to answer the questionnaire. Your opinion is very important in the complication of the research. All information you provide is confidential and used for research purposes only. Thank you for taking the time to answer this questionnaire.

Note

Please note that participation in this survey is voluntary, you can withdraw by cancelling any time and there will not be any repercussion. No names or sensitive information will be required from the participant. The information obtained will be stored anonymously and treated confidentially and it will be used solely for academic purpose. There is no risk associated with this survey, as we will not meet you in person and no names, contact information or IP address will be collected. If you would like to know more about the researchers involved in the study, you can contact us on the following email addresses.

Researcher:

1. Mohd Sukri Bin Jalapar. a20a2160@siswa.umk.edu.my
2. Preeti A/P Sochitro Kumar a20a1909@siswa.umk.edu.my
3. Nor Shazwani Binti Md Rodzi. a20a1633@siswa.umk.edu.my
4. Nurul Maisarah Binti Lan Hawari. a20a1876@siswa.umk.edu.my

Faculty of Entrepreneurship and Business, Universiti Malaysia Kelantan

By clicking “I agree” below you are indicating that you have read and understood this consent form and agree to participate in this research study.

I agree

I disagree

PART A: DEMOGRAPHIC INFO

You are required to place a tick (/) at the appropriate answer.

A1. Age /*Umur*:

11-14	15-18	19-22	23- 26

A2. Gender / *Jantina*:

Male/*Lelaki*	Female/*Perempuan*

A3. Academic Level / *Tahap akademik*:

SPM	STPM	Diploma	Degree / *Ijazah*	Master / *Sarjana*

A4. Maritial Status / *Status perkahwinan*:

Single / *Bujang*	Married / *Berkahwin*

A5. Occupation / *Pekerjaan*:

Government/ *Kerajaan*	Private/*Swasta*	Student / *Pelajar*	Unemployed / *Menganggur*

PART B: GENERAL QUESTION

Please respond to each item by ticking (√) on the appropriate answer that reflects your cybersecurity awareness in TikTok application.

B1. Do you have TikTok account / *Adakah anda mempunyai akaun TikTok*:

Yes/*Ya*	No/*Tidak*

B2. What kind of activities do you do on TikTok Application / *Apakah jenis aktiviti yang anda lakukan di aplikasi TikTok.*:

Sports /*Sukan*	Entertainment /*Hiburan*	Marketing /*Pemasaran*	Post Video/ *Menyiarkan Video*

B3. How frequently do you use TikTok ?. / *Kekerapan menggunakan aplikasi TikTok* :

Daily / *Setiap hari*	Several times a week / *Beberapa kali seminggu*	Once a week / *Sekali seminggu*	Rarely / *Jarang*

B4. How do you know about TikTok application / *Dari mana anda tahu tentang aplikasi TikTok*:

Parents / *Ibu bapa*	Online advertisement / *Iklan dalam talian*	Colleagues / *Rakan sekerja*	Teacher / *Guru*

PART C: DEPENDENT VARIABLES

This section will measure your cybersecurity awareness among Gen Z users of TikTok Application in Kelantan. Please mark your answer based on the scale from 1 to 5.

Strongly Disagree (SD)	**Disagree (D)**	**Neutral (N)**	**Agree (A)**	**Strongly Agree (SA)**
1	2	3	4	5

Cybersecurity Awareness		**SD**	**D**	**N**	**A**	**SA**
C1.	I am familiar with common cybersecurity threats, such as phishing and malware. / *Saya kenal dengan ancaman keselamatan siber yang biasa, seperti pancingan data dan perisian hasad.*	1	2	3	4	5
C2.	I regularly update my passwords to enhance my TikTok account security. / *Saya sentiasa mengemaskini kata laluan saya untuk meningkatkan keselamatan akaun TikTok.*	1	2	3	4	5
C3.	I stay informed about the latest cybersecurity trends and best practices. / *Saya sentiasa dimaklumkan tentang trend keselamatan siber terkini dan amalan terbaik.*	1	2	3	4	5
C4.	I am aware of the risks associated with sharing personal information on TikTok application. / *Saya sedar akan risiko yang berkaitan dengan berkongsi maklumat peribadi di aplikasi TikTok.*	1	2	3	4	5
C5.	I can identify potential signs of a cybersecurity attack, such as suspicious emails or messages. / *Saya boleh mengenal pasti tanda-tanda potensi serangan keselamatan siber, seperti emel atau mesej yang mencurigakan.*	1	2	3	4	5

PART D: INDEPENDENT VARIABLE

This section will measure your attitude factor, knowledge factor and environmental factors in cybersecurity awareness. Please mark your answer based on the scale from 1 to 5.

Strongly Disagree (SD)	**Disagree (D)**	**Neutral (N)**	**Agree (A)**	**Strongly Agree (SA)**
1	2	3	4	5

Attitude Factor		**SD**	**D**	**N**	**A**	**SA**
D1.	I ensure that the information updated on my TikTok account is accurate. / *Saya memastikan maklumat yang dikemas kini pada akaun TikTok adalah tepat.*	1	2	3	4	5
D2.	I am attentive to the accuracy of the information about acquaintances on the TikTok application./ *Saya seorang yang peka terhadap ketepatan maklumat rakan kenalan di aplikasi TikTok.*	1	2	3	4	5
D3.	I am aware of whom I share information about on the TikTok application./ *Saya sedar siapa yang saya kongsikan maklumat mengenai aplikasi TikTok.*	1	2	3	4	5
D4.	I only share information about people whom I truly trust./ *Saya hanya berkongsi maklumat tentang orang yang benar-benar boleh dipercayai sahaja.*	1	2	3	4	5
D5.	In my perspective, I can determine whether the information shared on TikTok is true or not./ *Dalam perspektif saya, saya dapat menentukan sama ada maklumat yang dikongsi di TikTok adalah benar atau tidak.*	1	2	3	4	5
Knowledge Factor		**SD**	**D**	**N**	**A**	**SA**
D6.	I am aware of cyber laws in Malaysia. / *Saya mengetahui mengenai undang-undang siber di Malaysia.*	1	2	3	4	5
D7.	I am aware of cybersecurity awareness programs on the TikTok application. / *Saya mengetahui berkenaan program kesedaran keselamatan siber di TikTok application.*	1	2	3	4	5
D8.	I am knowledgeable about cyber surveillance on TikTok application. / *Saya mengetahui mengenai intipan siber di aplikasi TikTok.*	1	2	3	4	5
D9.	I am knowledge about cyber fraud (scam) on the TikTok application. / *Saya mengetahui mengenai penipuan siber (scam) di aplikasi TikTok.*	1	2	3	4	5
D10.	I am aware of cyberbullying on the TikTok application. / *Saya mengetahui mengenai jenayah buli siber di TikTok application.*	1	2	3	4	5

Environment Factor		**SD**	**D**	**N**	**A**	**SA**
D11.	I always share information about cybersecurity awareness on TikTok with my friends. / *Saya sentiasa berkongsi maklumat tentang kesedaran keselamatan siber dalam TikTok dengan rakan-rakan saya.*	1	2	3	4	5
D12.	I always discuss cybersecurity threats on TikTok with my friends. / *Saya sentiasa berkongsi maklumat tentang kesedaran keselamatan siber dalam TikTok dengan rakan-rakan saya.*	1	2	3	4	5
D13.	My parents always monitor every activity I do on TikTok. / *Ibu bapa saya sentiasa mengawasi setiap aktiviti saya di TikTok.*	1	2	3	4	5
D14.	I always remind each other about cybersecurity issues on TikTok with my parents. / *Saya sentiasa saling memperingati mengenai isu ancaman siber TikTok dengan ibubapa.*	1	2	3	4	5
D15.	My friends always keep an eye on every activity I do on TikTok. / *Rakan saya sentiasa mengawasi setiap aktiviti saya di TikTok.*	1	2	3	4	5

APPENDIX B

DATE	GANTT CHART														
	Project Plans	WEEKS													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
8 OCT 2023	1. Briefing on PPTA I and PPTA II.														
15 OCT 2023 17 OCT 2023	2. Group discussion and finding related topic journals. 3. Meet our supervisor for brainstorming.														
22 OCT 2023	4. Discussion of the title with our lecturer.														
26 OCT 2023	5. Discussion about the problem statement, research questions and research objectives (draft of PPTA I)														
1 Nov 2023 - 8 Nov 2023	6. Review on literature's independent variable and dependent variable														
15 Nov 2023	7. Creating PowerPoint for presentation														
16 Nov 2023	8. Submission &presentation (PPTA I)														
25 Nov 2023 - 2 Dec 2023	9. Distribution questionnaire among UMK students & data collection														
16 Dec 2023	10. Data analysis														
20 Dec 2023	11. Writing final year research project														
14 Jan 2024	12. Submission & Presentation (PPTA II)														

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

Student's Name: **MOHD SUKRI BIN JALAPAR(A20A2160), PREETI A/P SOCHITRO KUMAR(A20A1909), NOR SHAZWANI BINTI MD RODZI(A20A1633), NURUL MAISARAH BINTI LAN HAWARI(A20A1876)**
Name of Supervisor: **DR. FATIHAH BINTI MOHD** **Name of Programme:** **SAK**
Research Topic: **A STUDY OF CYBERSECURITY AWARENESS OF THE TIKTOK APPLICATION AMONG GENERATION Z IN KELANTAN**

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)	

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)	
3.	**Research Findings and**		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	

	Discussion (20 MARKS)					(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)	

ASSESSMENT FORM FOR FINAL YEAR RESEARCH PROJECT (PPTAII): REFLECTIVE NOTE (Weight 20%)

(COMPLETED BY SUPERVISOR)

Student's Name: MOHD SUKRI BIN JALAPAR(A20A2160), PREETI A/P SOCHITRO KUMAR(A20A1909), NOR SHAZWANI BINTI MD RODZI(A20A1633), NURUL MAISARAH BINTI LAN HAWARI(A20A1876)

Name of Supervisor: DR. FATIHAH BINTI MOHD **Name of Programme: SAK**

Research Topic: A STUDY OF CYBERSECURITY AWARENESS OF THE TIKTOK APPLICATION AMONG GENERATION Z IN KELANTAN

NO.	CRITERIA	PERFORMANCE LEVEL				WEIGHT	TOTAL
		POOR (1 MARK)	FAIR (2 MARKS)	GOOD (3 MARKS)	EXCELLENT (4 MARKS)		
1.	Determination	Is not determined and does not put in any effort in completing the research report	Is determined but puts in little effort in completing the research report	Is determined and puts in reasonable effort in completing the research report	Is very determined and puts in maximum effort in completing the research report	____ x 1 (Max: 4)	
2.	Commitment	Is not committed and does not aim to complete on time and/ or according to the requirements	Is committed but makes little effort to complete according to the requirements	Is committed and makes reasonable effort in fulfilling some of the requirements	Is very committed and makes very good effort in fulfilling all the requirements, without fail.	____ x 1 (Max: 4)	
3.	Frequency in meeting supervisor	Has not met the supervisor at all.	Has met the supervisor but less than five times.	Has met the supervisor for at least five times.	Has met the supervisor for more than five times.	____ x 1 (Max: 4)	
4.	Take corrective measures according to supervisor's advice	Has not taken any corrective action according to supervisor's advice.	Has taken some corrective actions but not according to supervisor's advice, or with many mistakes.	Has taken some corrective actions and most are according to supervisor's advice, with some mistakes.	Has taken corrective actions all according to supervisor's advice with few mistakes.	____ x 1 (Max: 4)	
5.	Initiative	Does not make any initiative to do the research.	Make the initiative to work but requires consistent monitoring.	Make the initiative to do the research with minimal monitoring required.	Makes very good initiative to do the research with very little monitoring required.	____ x 1 (Max: 4)	
	TOTAL (20 MARKS)						/20