

STUDY ON AWARENESS OF CYBERSECURITY  
ISSUES AND SOCIAL MEDIA USAGE AMONG  
YOUTHS

TEE KAI VERN

UNIVERSITI KEBANGSAAN MALAYSIA

STUDY ON AWARENESS OF CYBERSECURITY ISSUES AND SOCIAL  
MEDIA USAGE AMONG YOUTHS

TEE KAI VERN

PROJECT SUBMITTED IN PARTIAL FULFILMENT FOR THE MASTER OF  
CYBER SECURITY

FACULTY INFORMATION SCIENCE AND TECHNOLOGY  
UNIVERSITI KEBANGSAAN MALAYSIA  
BANGI

2025

STUDY ON AWARENESS OF CYBERSECURITY ISSUES AND SOCIAL  
MEDIA USAGE AMONG YOUTHS

TS. TEE KAI VERN

PROJEK YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN  
DARIPADA SYARAT UNTUK MEMPEROLEH IJAZAH SARJANA SIBER  
KESELAMATAN

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT  
UNIVERSITI KEBANGSAAN MALAYSIA  
BANGI

2025

## DECLARATION

I hereby declare that the work in this project is my own except for quotations and summaries, which have been duly acknowledged.

I acknowledge the use of OpenAI ChatGPT to generate the following:

Prompt: I entered the following prompt/s:

1. Provide me with a clear context on the usage of Pearson Correlation and Chi-Square test and its characteristics, and its formula

Use: I used the output to understand the characteristics and formulas involved in performing these tests for academics and determine which test is suitable for specific types of data.

15 March 2025

TEE KAI VERN  
P113852

## ACKNOWLEDGEMENT

I am deeply indebted to many individuals who have provided me with invaluable support and guidance throughout the journey of completing this project. First and foremost, I would like to extend my heartfelt gratitude to my supervisor, Dr. Umi Asma' binti Mokhtar. Her unwavering support, insightful feedback, and constant encouragement have shaped this research. Dr. Umi Asma's expertise and dedication have inspired me to strive for excellence, and her patience and understanding have been a source of great comfort throughout this challenging process.

I am also sincerely grateful to my faculty coordinator, Dr. Wandeep Kaur, for her indispensable guidance and assistance. Dr. Wandeep Kaur's commitment to fostering a supportive academic environment has been instrumental in completing this project. Her advice and administrative support have been greatly appreciated and have facilitated the smooth progress of my research work.

I want to acknowledge the Faculty of Information Science & Technology at Universiti Kebangsaan Malaysia (UKM) for providing the resources and academic environment necessary for the successful completion of this project. The faculty's commitment to educational excellence and research has been a constant source of motivation

Most importantly, my most profound appreciation goes to my parents, whose love, support, and encouragement have been my greatest strength. Their unwavering belief in my abilities has been the cornerstone of my achievements. Their sacrifices and support have been instrumental in my academic journey, and I am forever grateful for their constant presence in my life.

Finally, I would like to dedicate this project to all those who have supported me, directly or indirectly, throughout this journey. Thank you to my friends, colleagues, and everyone who has offered a kind word or a helping hand. Your encouragement and support have been invaluable, and I sincerely appreciate your contributions to this work.

## ABSTRAK

Kebergantungan golongan belia terhadap media sosial semakin meningkat, sekali gus menimbulkan perhatian terhadap tahap kesedaran keselamatan siber mereka dan kerentanan terhadap ancaman dalam talian. Walaupun penglibatan digital semakin ketara, kajian mengenai pengetahuan risiko keselamatan siber dan faktor-faktor yang mempengaruhi amalan keselamatan dalam talian mereka masih terhad. Kajian ini bertujuan menjawab soalan penyelidikan berikut: Apakah tahap kesedaran keselamatan siber dalam kalangan belia Malaysia? Bagaimanakah corak penggunaan media sosial mempengaruhi kerentanan mereka terhadap ancaman keselamatan siber? Apakah faktor demografi dan tingkah laku yang membentuk amalan keselamatan siber mereka? Tujuan utama kajian ini adalah untuk menilai tahap kesedaran keselamatan siber dalam kalangan belia Malaysia berusia 15 hingga 30 tahun dan mengenal pasti faktor utama yang mempengaruhi amalan keselamatan dalam talian mereka. Penyelidikan ini dijalankan di Malaysia menggunakan pendekatan kaedah campuran, termasuk tinjauan kuantitatif yang dianalisis menggunakan statistik deskriptif, ujian chi-kuasa dua, dan analisis korelasi Pearson. Hasil kajian menunjukkan jurang yang ketara dalam kesedaran keselamatan siber, dengan ramai peserta mempamerkan pengurusan kata laluan yang lemah, kesedaran rendah terhadap ancaman phishing, dan penggunaan tetapan privasi yang tidak mencukupi. Penggunaan media sosial yang tinggi dikaitkan dengan kerentanan yang lebih besar terhadap ancaman siber, dan faktor demografi seperti pendidikan, jantina, dan status sosioekonomi mempengaruhi tahap kesedaran keselamatan siber.

## ABSTRACT

The increasing reliance of Malaysian youths on social media has brought attention to their cybersecurity awareness and susceptibility to online threats. Despite significant digital engagement, limited research has been conducted to evaluate their knowledge of cybersecurity risks and the factors influencing their online safety practices. This study addresses the following research questions: What is the level of cybersecurity awareness among Malaysian youths? How do social media usage patterns affect their susceptibility to cybersecurity threats? What demographic and behavioural factors shape their cybersecurity practices? The study's primary aim was to assess the level of cybersecurity awareness among Malaysian youths aged 15 to 30 and to identify key factors influencing their online safety practices. The research employed a mixed-methods approach in Malaysia, including quantitative surveys analysed through descriptive statistics, chi-square tests, and Pearson correlation analyses. The findings revealed significant gaps in cybersecurity awareness, with many participants displaying poor password management, limited phishing awareness, and inadequate use of privacy settings. High social media usage correlated with greater vulnerability to cyber threats, and demographic factors such as education, gender, and socioeconomic status influenced cybersecurity awareness levels. A critical disconnect between awareness of risks and proactive behaviour was identified, pointing to the need for practical interventions.

## TABLE OF CONTENTS

		<b>Page</b>
<b>DECLARATION</b>		<b>iii</b>
<b>ACKNOWLEDGEMENT</b>		<b>iv</b>
<b>ABSTRAK</b>		<b>v</b>
<b>ABSTRACT</b>		<b>vi</b>
<b>TABLE OF CONTENTS</b>		<b>vii</b>
<b>LIST OF TABLES</b>		<b>x</b>
<b>LIST OF ILLUSTRATIONS</b>		<b>xi</b>
<b>LIST OF ABBREVIATIONS</b>		<b>xiii</b>
<b>CHAPTER I</b>	<b>INTRODUCTION</b>	
1.1	Research Background	1
1.2	Problem Statemet	3
1.3	Research Objective	6
1.4	Research Question	6
1.5	Significance Of Study	7
1.6	Nature Of Challenge	9
1.7	Outline	10
<b>CHAPTER II</b>	<b>LITERATURE REVIEW</b>	
2.1	Introduction	12
2.2	Definition Of Youth	13
2.3	Definition Of Cybersecurity Awareness	14
2.4	Primary Objective Of Cybersecurity Awareness	15
2.5	Factors Affecting The Effectiveness Of Cybersecurity Awareness	16
2.6	Social Media Usage And Trends In Malaysia	17
2.7	Challenges And Risks Associated With Social Media	18
2.8	Current Cybersecurity Awareness Among Youth	19
2.9	Importance Of Targeted Interventions In Enhancing Digital Safety	21
2.10	Existing model of cybersecurity awareness levels	22

2.11	Conclusion	24
<b>CHAPTER III METHODOLOGY</b>		
3.1	Introduction	25
3.2	Research Design	26
3.3	Descriptive Statistics	27
3.4	Chi-square Test	28
3.5	Pearson Correlation	29
3.6	Survey Development And Data Collection	30
3.7	Research Hypothesis Based On Research Objective	32
3.8	Summary	33
<b>CHAPTER IV IMPLEMENTATION OF STUDY AND RESULTS</b>		
4.1	Introduction	34
4.2	Research Characteristics	34
4.4	Participants	36
4.5	Experimental Design	37
4.6	Survey	37
4.7	Data Processing	37
4.8	Perform Statistical Model Using IBM SPSS	38
4.9	Summary	39
<b>CHAPTER V RESULTS</b>		
5.1	Introduction	40
5.2	Results	41
	5.2.1 Age	41
	5.2.2 Gender	42
	5.2.3 Ethnicity	43
	5.2.4 Region	44
	5.2.5 Education	45
	5.2.6 Employment Status	46
	5.2.7 Social media platform trend and frequency	47
	5.2.8 Time spent on social media	48
	5.2.9 Social media posting	49
	5.2.10 Social media posting activity	50
	5.2.11 Awareness of online scams and hackers	51
	5.2.12 Password reuse	52
	5.2.13 Utilisation of two-factor authentication (2FA)	53
	5.2.14 Frequency of password change	54

5.2.15	Cybersecurity and online safety	55
5.2.16	Installation of Anti-Virus	56
5.2.17	Social media compromised	57
5.3	Pearson Correlation Analysis	58
5.4	Chi-square Test	59
5.4.1	Assess the understanding of cybersecurity risks	59
5.4.2	Cybersecurity Education	62

## **CHAPTER VI CONCLUSION AND FUTURE WORK**

6.1	Introduction	66
6.2	Achievement And Limitation Of Objective	67
6.3	Future Work	69

## **REFERENCES 70**

## **APPENDICES**

Appendix A	Questionnaire And Survey	73
Appendix B	Collected Data	87

**LIST OF TABLES**

<b>Table No.</b>		<b>Page</b>
Table 3.1	Research hypothesis based on research objective	32

LIBRARY FTSM

## LIST OF ILLUSTRATIONS

<b>Figure No.</b>		<b>Page</b>
Figure 1.1	Key pillar of the significance of the study	7
Figure 4.1	Demographics information	36
Figure 5.1	Frequency of age	49
Figure 5.2	Bar Graph Frequency of age	49
Figure 5.3	Frequency of Gender	50
Figure 5.4	Bar Graph Frequency of Gender	50
Figure 5.5	Frequency of Ethnicity	51
Figure 5.6	Bar Graph Frequency of Ethnicity	51
Figure 5.7	Frequency of Region	52
Figure 5.8	Bar Graph Frequency of Region	52
Figure 5.9	Frequency of Education	53
Figure 5.10	Bar Graph Frequency of Education	53
Figure 5.11	Frequency of Employment Status	54
Figure 5.12	Bar Graph Frequency of Employment Status	54
Figure 5.13	Bar Graph Frequency of Employment Status	55
Figure 5.14	Frequency of time spent on social media	56
Figure 5.15	Bar Graph Frequency of time spent on social media	56
Figure 5.16	Frequency of posting, sharing on social media	57
Figure 5.17	Bar Graph Frequency of posting, sharing on social media	57
Figure 5.18	Frequency of activity on social media	58
Figure 5.19	Bar Graph percentage of activity on social media	58
Figure 5.20	Frequency of awareness of online scams and hackers	59
Figure 5.21	Bar Graph Percentage of Awareness	59
Figure 5.22	Frequency of the Password Reuse	60

Figure 5.23	Bar Graph Parentage on the Password Reuse	60
Figure 5.24	Frequency of the utilisation of 2FA	61
Figure 5.25	Bar Graph Percentage of the utilisation of 2FA	61
Figure 5.26	Frequency of the Password Change	62
Figure 5.27	Bar Graph Frequency of the Password Change	62
Figure 5.28	Bar Graph Frequency of the online safety workshop	63
Figure 5.29	Bar Graph Frequency of the online safety workshop	63
Figure 5.30	Frequency of the installation of anti-virus	64
Figure 5.31	Bar Graph percentage on the installation of anti-virus	64
Figure 5.32	Bar Graph Frequency on the Social Media Compromise	65
Figure 5.33	Frequency of the Social Media Compromise	65

**LIST OF ABBREVIATIONS**

IT	Information Technology
MCMC	Malaysian Communications and Multimedia Commission
UKM	Universiti Kebangsaan Malaysia
PSYOP	Psychological Operations
PII	Personal Identifiable Information
UKM	Universiti Kebangsaan Malaysia

LIBRARY FETSM

## CHAPTER I

### INTRODUCTION

#### 1.1 RESEARCH BACKGROUND

In today's interconnected world, where technology permeates nearly every industry, Information Technology (IT) has reshaped global economic and cultural institutions by providing new and more efficient communication, collaboration, and information sharing. This transformation is especially evident on social media platforms, which have become integral to daily life. The proliferation of platforms such as Facebook, Instagram, X (Formerly known as Twitter), and TikTok has revolutionised how young people communicate, share information, and form social networks.

The diverse forms of social interaction facilitated by social media allow the medium to serve several essential user functions. These include enabling communication, fostering new relationships, maintaining existing ones, and providing a platform for sharing knowledge and information with others. These capabilities are treasured by community and social media users, particularly youth. Youth have been identified as active social media users, which is reported in different studies conducted by various institutes across the globe. For instance, based on Meltwater's 2024 digital report, 67% of Malaysian youth are active on social media platforms (Meltwater, 2024). In related studies, a survey of pre-university students aged 17-19 at Universiti Kebangsaan Malaysia (UKM) revealed that 92.7% of respondents used social media daily. In comparison, 52% used it more than seven times a day. (Chen, Noresafendy, Wong, 2022)

While the widespread adoption of social media has introduced innovative methods for individuals to communicate and access information and knowledge, it has also opened the door to numerous threats and malicious activities from various sources. As youths increasingly engage with social media and other online platforms, they face various cybersecurity risks. Among the cybersecurity risks include cyberbullying, online harassment, sexting, disinformation and victim to cognitive warfare (PSYOP).

First, youths that surf social media also open themselves to privacy (social and data) related concerns as a youth might provide his/her personally identifiable information (PII) to social media, which may be potential for information to be misused, stolen, or exploited by malicious actors, leading to identity theft, unauthorised access to personal accounts, and other security breaches. Additionally, cyberbullying is a significant cybersecurity risk associated with social media platforms. Cyberbullying involves deliberate and repeated harm inflicted through computers, cell phones, or other electronic devices. According to a survey conducted by the Malaysia Communications and Multimedia Commission (MCMC), among 14,000 school students, 70% of the respondents admitted to having been harassed online through improper images or messages posted and being called mean names on social media. (MCMC,2020). Meanwhile, The Star, one of the major newspaper outlets in Malaysia, has conducted a nationwide survey, which found that 8 out of 10 school children have experienced bullying in their schools and cyberspace.

Malaysian youth utilise social media for information seeking, the latest trends and educational purposes (Hamat, Embi, & Hassan, 2012; Yin, Agostinho, Harper, & Chicago, 2014). Based on a study conducted to investigate Malaysian university students' social media usage, the researcher identified that most respondents utilise social media for social learning purposes. Social media's communicative and collaborative features permit students to interact, work together and learn from one another (Hamat et al., 2012). Similarly, (Yin et al.,2014) also indicate that, aside from social activities, youth use social media to engage in educational learning. Malaysian youth surf social media, including Wikipedia, Facebook, and YouTube, to support their studies. (Yin et al., 2014)

## 1.2 PROBLEM STATEMENT

The Internet has become an essential aspect of life in Malaysia, with the country experiencing a significant increase in Internet penetration. According to the World Bank Group, in 2022, 97.4% of the total population had internet access, and the number of internet users in Malaysia is projected to rise by 1.7 million users (+5%) between 2024 and 2029 (Statista Research Department, 2024). This rapid growth of internet usage has also led to a surge in social media adoption among Malaysian youth, significantly transforming communication and information-sharing practices. Social media and internet use have become integral to daily life, enabling young individuals to connect, share, and engage in unprecedented ways. Despite the various benefits offered by social media, including enhanced connectivity, access to diverse information, and opportunities for socialisation, these platforms also pose significant cybersecurity risks. This study seeks to address the critical issue of cybersecurity awareness among Malaysian youths active on social media and provide solutions for tackling cybersecurity awareness issues in Malaysia, from policy formulation to implementation at the community level.

One major problem is the lack of comprehensive government policies and governance frameworks specifically tailored to address youths' cybersecurity challenges on social media. Although initiatives such as the Malaysia Cybersecurity Strategy 2020-2024 exist, current policies often fail to address the unique vulnerabilities of young users, particularly in the context of social media usage. Furthermore, the effectiveness of government interventions is hindered by inadequate enforcement and a lack of coordination among stakeholders, ranging from policymakers to local communities. This governance gap leaves Malaysian youths exposed to cyber threats and undermines efforts to promote a safe online environment.

In addition to policy-related issues, there are significant challenges related to people, processes, and technology in addressing cybersecurity concerns among youths. Studies have shown that Malaysian youths possess only a basic understanding of common cyber threats, such as phishing and malware, while their knowledge of more sophisticated cyberattacks remains limited (Lim & Tan, 2021). This gap in awareness increases their

susceptibility to identity theft, financial fraud, and data breaches. Globally, the cybersecurity risks faced by youths are also alarming. The Global Cybersecurity Forum (2023) and the DQ Institute (2023) reported that a large proportion of young internet users are exposed to online threats, including cyberbullying, inappropriate content, and security breaches. The United Nations (2023) further highlighted that one-third of young people across 30 nations have experienced cyberbullying, with some opting to skip school due to online harassment. These statistics underscore the urgency of implementing structured and proactive cybersecurity education tailored to younger populations.

The processes in place to promote cybersecurity awareness and education among Malaysian youths are also insufficient. While some initiatives exist, they are often fragmented and lack the coordination needed to be effective. Schools, parents, and communities play a crucial role in fostering cybersecurity awareness, yet these stakeholders frequently operate in silos. Parents may lack the necessary knowledge to guide their children, and schools may face resource constraints that prevent the implementation of comprehensive cybersecurity curricula. This disjointed approach hinders the development of a cohesive strategy to educate youths about cybersecurity risks and protective measures. Furthermore, Malaysian youths continue to engage in risky online behaviours, such as poor password management and excessive sharing of personal information on social media, highlighting the need for structured digital literacy programs (Kamarudin & Ismail, 2022). Despite existing awareness campaigns, their effectiveness remains limited due to engagement barriers and insufficient outreach (Rahim et al., 2020). Additionally, cybersecurity education is often reactive rather than proactive, with young individuals only becoming aware of security threats after falling victim to cyber incidents (Aziz & Mahmud, 2023).

Another critical concern is youth vulnerability to data breaches. The National Cyber Security Alliance (2023) identified a disconnect between parental supervision and youths' actual online behaviours, with only a small fraction of teenagers adhering to parental safety guidelines. In 2022 alone, approximately 1.7 million children were victims of data breaches, underscoring the urgency of strengthening cybersecurity education and awareness efforts (StaySafeOnline, 2023). Moreover, social media

organisations must play a more proactive role in addressing cybersecurity issues affecting youths. These companies should implement more robust security features, provide clear and accessible information on protective measures, and ensure greater transparency and accountability in handling user data and responding to security breaches.

Despite increasing awareness of cybersecurity issues, critical knowledge gaps persist among youths. Addressing these challenges requires the implementation of structured digital literacy programs, targeted awareness campaigns, and collaborative efforts between educational institutions, policymakers, and cybersecurity experts. Without proactive measures, young individuals will remain at risk in an increasingly digitalised society, emphasising the urgent need for comprehensive interventions in cybersecurity education and awareness.

LIBRARY FTSM

### **1.3 RESEARCH OBJECTIVE**

The primary objective of this research is to investigate the level of awareness of cybersecurity issues among youths in Malaysia who actively use social media. Specifically, the study aims to:

1. Assess the current understanding and knowledge of cybersecurity risks among Malaysian youth, such as data and personal privacy issues, cyberbullying, misinformation, and online harassment, among Malaysian youths.
2. Identify the factors influencing cybersecurity awareness among youths, including demographic variables (age, gender, education level), and exposure to cybersecurity education.
3. Assess the current trends and characteristics of social media among Malaysian youth, such as preferred social media (Instagram, Facebook, X), duration and frequency of time spent on social media, and the purposes of surfing social media.

### **1.4 RESEARCH QUESTION**

The research aims to answer the following question:

1. What is the level of cybersecurity awareness among Malaysian youths who actively use social media, and how do demographic factors, social media usage patterns, and existing educational and governance frameworks influence their understanding and protective practices?

## 1.5 SIGNIFICANCE OF STUDY

The study on the awareness of cybersecurity issues and social media usage among youths in Malaysia holds substantial significance in multiple domains, including education, policymaking, community engagement, and the enhancement of digital safety practices. The findings from this research will provide critical insights and contribute to several key areas, as shown in the diagram below:

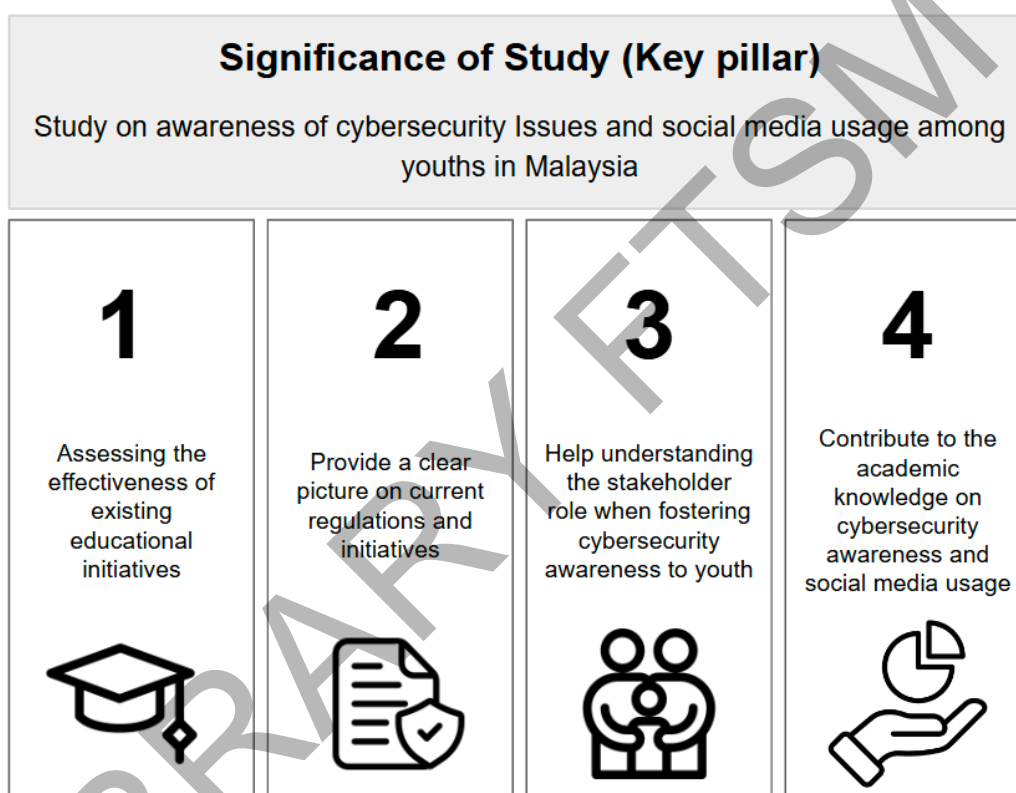


Figure 1.1 Key pillar of the significance of the study

Additionally, this study helps understand the role of parents, educators, and community organisations in fostering cybersecurity among Malaysian youth. It will provide valuable information on how these communities contribute to cybersecurity education and where their efforts fall short. The study can give an overview and assist the stakeholders in developing security awareness programs and parental guidance resources that support and enhance cybersecurity awareness among Malaysian youths.

This research study will contribute to the academic knowledge of cybersecurity awareness and social media usage among youths. The findings will be valuable for

scholars, researchers, and practitioners in cybersecurity, education, social sciences, and digital media. The study can serve as a foundation for future research and inspire further investigations into related areas, such as the psychological impact of cyber threats and general cybersecurity risk to Malaysian youth.

The significance of this study lies in its potential to inform and improve cybersecurity awareness and education among Malaysian youths. This study aims to foster a safer digital environment and equip young social media users with the tools they need to protect themselves online by addressing the gaps in cybersecurity knowledge, policy, and practice. The study's outcomes will benefit various stakeholders, ultimately leading to the overall digital well-being of Malaysian youth.

LIBRARY FTSM

## 1.6 NATURE OF CHALLENGE

The study examining cybersecurity awareness and social media usage among Malaysian youths faces several key hurdles that must be overcome to ensure the findings are accurate and comprehensive. These obstacles include the need for extensive data collection, the difficulty of securing reliable data, and the complexities associated with data analysis for subsequent research.

A significant challenge lies in collecting a sufficiently broad set of data. Gaining a representative picture of cybersecurity awareness among Malaysian youths requires gathering information from a diverse pool of participants. This involves obtaining quantitative data through surveys and questionnaires. Given the range of experiences and knowledge levels across different regions, educational backgrounds, ethnicities, and social groups, assembling this breadth of data is a significant undertaking.

Another issue is ensuring the reliability and validity of the data collected. Varying levels of familiarity and interest in cybersecurity amongst Malaysian youths can influence their willingness to take part and the accuracy of their responses. Additionally, social desirability bias can skew results, as participants may provide the answers they believe are expected rather than sharing their genuine experiences or knowledge.

Finally, the rapidly evolving nature of social media and cybersecurity adds another complexity layer. New platforms and technologies emerge frequently, reshaping the cybersecurity landscape and affecting how youths engage with social media. This ever-changing environment makes it challenging to keep the study entirely up to date, potentially affecting its relevance and ability to reflect the current level of cybersecurity awareness.

## 1.7 OUTLINE

This research, "Study on Awareness of Cybersecurity Issues and Social Media Usage Among Youths in Malaysia," has been aptly compiled with six chapters to investigate the essence of the interplay between social media usage patterns and cybersecurity awareness among Malaysian youths aged between 15 and 30. The orderly setup of the project navigated this report through the research objectives, from contextualising the issue to meaningful insight and recommendations.

The research undertaking was based on Chapter One, which introduced the study's background, objectives, and scope. The chapter has set a noble understanding of how relevant cybersecurity awareness will be in these digital times; social media enables communication and equally acts as a cybersecurity threat vector. Next, this project will discuss the key problem statement for this project; thereafter, the chapter sets out the research questions and objectives. This introductory chapter also gave an overview of the study, with details of the structures and purposes of subsequent chapters.

Chapter two was a critical review of the literature on cybersecurity awareness and the use of social media. It first defined cybersecurity awareness and the aims of achieving it, then the factors that influence its effectiveness. The chapter also described the trends and risks of social media usage in Malaysia, setting a critical backdrop for understanding the vulnerabilities and behaviours of the target demographic. This contextualising within the Malaysian setting from the literature review has shown lapses in knowledge and practices the study tried to fill.

Chapter three sets out the research methodology that will be used to investigate those issues. The chapter has elaborated on the approach that utilises quantitative analyses of cybersecurity awareness and practices about social media. It explained how descriptive statistics, chi-square tests, and Pearson correlation analyses have been used to test relationships between variables. The hypotheses set out in testing the research questions were also presented, and the methodology was elaborated step-by-step to ensure transparency and reproducibility.

Chapter Four described the study's implementation and data collection process. It covers the research design, which included developing and administering questionnaires, and

further elaborated on the participants' demographics. The chapter also outlined the methods used in processing the data, underlining the use of SPSS in statistical data analysis. This ensured strict observance of the derivation of meaningful insights from the data collected.

Next, chapter Five presented the study's results. It starts by showing a descriptive analysis of the demographics, social media usage, and level of cybersecurity awareness. The statistical analyses indicated significant relationships between patterns of social media use and cybersecurity vulnerabilities and demographic factors and levels of cybersecurity awareness. Aside chapter 5 also cover the findings considering existing initiatives on cybersecurity education and provided recommendations on how to enhance understanding and fill the gaps identified.

Lastly, chapter six summarises the research findings and their implications and concludes the study. The research found that while Malaysian youths substantially utilise social media, most usually do not have sufficient awareness of the risks and precautionary measures against cybersecurity. Finally, the findings also highlight the urgent need for targeted interventions, including integration into the formal curricula into Malaysia education system, cybersecurity public awareness campaigns, and collaborative policy-making efforts with social media platforms (e.g. X, Facebook, Instagram). This chapter also cover the study's limitations, such as the reliance on self-reported data. It gave ways to conduct future research, including longitudinal studies and experimental interventions.

## **CHAPTER II**

### **LITERATURE REVIEW**

#### **2.1 INTRODUCTION**

Interaction between individuals (including young individuals) and the online world has been significantly transformed by the rapid evolution of digital technology and the expansion of social media platforms. This development has opened doors to previously unimaginable educational, recreational, and communicative opportunities. But technology has also made the world more vulnerable to new threats and vulnerabilities and makes a compelling case for why cybersecurity knowledge is necessary. To protect personal information and guarantee safer online experiences when cyber threats are becoming more complex, it is essential to comprehend the dynamics of cybersecurity and the elements influencing awareness.

This chapter presents an overview of the literature on cybersecurity awareness and social media practice among Malaysian youth. It starts by defining cybersecurity awareness and its scope and importance within the digital environment. The main goals of driving cybersecurity awareness are then discussed to demonstrate different awareness programs' goals and desired results.

Chapter 2 discusses some of the impactful influences on the effectiveness of cybersecurity awareness campaigns, that address the role of education, resource availability, and societal influences in individuals' everyday cybersecurity practices, especially in Malaysian youth. A report on social media consumption and patterns in Malaysia is used as a key for understanding Malaysian youth's daily lives, make sure the digital landscape's key platforms and screen time.

Moreover, the definition of "youth" has focused the demographic interest of this work by conferring clarity on the target population. The chapter ends by considering the threats and risks of social media, exploring youths' possible risks and, consequentially, its digital security threat. Through an integrative overview of these multiple issues, this literature review provides a foundation to enable the extensive examination of the relationship between cybersecurity literacy and social media usage among Malaysian youth, which leads to the following analysis and results.

## **2.2 DEFINITION OF YOUTH**

Because youth is a complicated concept that changes between countries and crosses the fields of psychology, sociology, and culture, there is no universally accepted definition. According to Arnett and Bynner (2000, 2005), youth is typically characterised as a period of transition between childhood and adulthood. Although each country defines its youth age and age limit, from a sociological standpoint, the definition of youth is not based on age bracket but a socially constructed stage characterised by specific roles, expectations, and transitions. (Wyn and White, 1997).

From a sociological perspective, the perspective underscores the dependence on youth family structure to the pursuit of employment, education and eventual independence. (Holdsworth and Morgan, 2005). Youth, therefore, represents a period of "emerging adulthood," wherein individuals explore identity-related aspects, including career, relationships, and social responsibilities (Arnett, 2000). Aside from academia, expertise in sociology argues that the limit of youth has expanded in recent decades due to shifting economic conditions and extended educational pathways provided in recent years (Bynner, 2005; Furlong, 2013). To extend a clear picture, labour market uncertainties can prolong dependency on parental support, which has led to the expansion of the sociological concept of youth well beyond the late twenties (Wyn, 2014).

Aside from a sociological standpoint, culture does play an essential role in shaping and defining the age limit of youth. For example, in collectivist cultures, familial expectations and community obligations may define youth differently compared to Western-based societies that emphasise individual autonomy (Kagitcibasi, 2007).

Traditional rites such as religious ceremonies and marriage events may affect and complicate the definition of youth, as these cultural events may occur at ages outside the standard legal definitions. (Nilan and Feixa, 2006).

As different countries have their sociologies and cultures that define the age limit of youth, the global context reflects variations in the age limits for youth, which are developed differently across many countries to account for their cultural, psychological, and socio-economic circumstances (UNESCO, 2020). For clear distinction, African Union member states define youth as ranging from 15 to 35 years old (African Union, 2006). In contrast, several European policies align more closely with United Nations (UN) standards, which typically define the youth age limit as 29 (European Commission, 2018). From Malaysia's perspective, the Malaysian National Youth Policy (MYP) 2019, released by the Ministry of Youth and Sports of Malaysia (KBS), defines youth as individuals between the ages of 15 and 30.

### **2.3 DEFINITION OF CYBERSECURITY AWARENESS**

Cybersecurity awareness is a crucial element within the broader framework of Information Security and Risk Management. All cybersecurity practitioners widely acknowledge and understand that human error frequently constitutes the weakest link in cybersecurity defences.

The National Institute of Standards and Technology (NIST) Special publication 800-16, Information Technology Security Training Requirements: a Role- and Performance-Based Model, awareness is detailed and elaborate as follows:

“Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations allow individuals to recognise IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance.” (Wilson and Hash, 2003).

The Professional Evaluation and Certification Board (PECB) defines cybersecurity awareness as follows:

“Cybersecurity awareness is the understanding of online threats, risks, and vulnerabilities, along with the skills needed to protect individuals and organisations. This awareness involves educating individuals on cybersecurity best practices, such as identifying phishing attempts, setting strong passwords, securely managing sensitive information, and continuously updating your software.” (Vesa, 2024).

#### **2.4 PRIMARY OBJECTIVE OF CYBERSECURITY AWARENESS**

The primary reason for promoting cybersecurity awareness is to reduce the mistakes people make when interacting with any technology. Human error is often labelled as one of the most significant weaknesses in the cybersecurity chain. A recent study conducted by cybersecurity researchers found that human (employee) mistakes cause nine out of 10 (88 per cent) data breach incidents. (Glorin, 2021). The reason behind this is that the attackers exploit the victim’s “lack of knowledge” in cybersecurity awareness, which is more effective than a technical perspective.

Another critical aspect of cybersecurity awareness is improving the resiliency that ensures young people can respond effectively when faced with cyberattacks. As current youth are marked as digital natives, youths rely heavily on online and social media platforms for communication, education, and entertainment. When their digital accounts are compromised, or personal data is leaked (data theft) by attackers, the consequences can affect their mental health, academic performance, and future opportunities (Aldawood & Skinner, 2019). Aside from that, a recent study conducted by Alotaibi found that awareness campaigns focused on password security, privacy settings, and reporting cyber incidents empower young people to act, reducing the impact of breaches. Youths who understand how to secure their devices and recognise suspicious activity are less likely to become repeat victims of cyberattacks. (Alotaibi, 2020).

Protecting digital assets is also one of the primary goals for cybersecurity awareness for the public, especially youth, as they often handle and share their own sensitive personal data and/or personally identifiable information (PII) without realising its value and the consequences when someone misuses it. From social media profiles to online banking and educational accounts, young people manage much personal information that can be exploited if not properly secured (Kaspersky, 2020). In Malaysia's context, Cybersecurity Malaysia (CSM) has initiated a CyberSAFE program to educate youths on the importance of protecting their digital footprint and practising responsible online behaviour (CyberSecurity Malaysia, 2021). In the global context, similar initiatives across the globe focus on teaching young people how to create strong passwords, avoid oversharing on social media, and secure their online accounts. The European Union (EU) Agency for Cybersecurity (2020) also highlighted that promoting cybersecurity skills among youths is essential for developing our future generations of informed, responsible digital citizens.

## **2.5 FACTORS AFFECTING THE EFFECTIVENESS OF CYBERSECURITY AWARENESS**

Various factors affect the effectiveness of cybersecurity awareness. One of the primary factors is individual factors, such as age, gender, education level, and personal experience with technology, which significantly influence cybersecurity awareness. A recent study found that younger-generation individuals with higher educational attainment tend to show greater cybersecurity awareness. Reversely, a lack of personal experience in cyber threats can lead to a lower awareness. For example, the De Bruin and Mersinas (2024) study found that demographics, including age and gender, alongside security-specific factors like prior experience with security incidents, are influential variables of security behaviour at the individual level. (Martin, 2024).

Aside from demographics, the rapid advancement of technology introduces more challenges that will affect cybersecurity awareness's effectiveness. Internet of Things (IoT) devices have expanded the attack surface, requiring additional awareness of potential vulnerabilities. A recent study by Mazhar found the security challenges posed by IoT devices and the need for artificial intelligence solutions to address these issues,

underscoring the importance of staying informed about technological developments (Mazhar, 2023).

Another key factor that affects cybersecurity awareness's effectiveness is the quality of education and training on cybersecurity awareness. Regarding cybersecurity awareness, a strong security culture is always characterised by management (government) support, clear, comprehensive policies and continuous training to follow the latest cybersecurity threats and trends. This has been proven by researchers Al-Nuaimi and Khan (2022), who find that human factors, including organisational culture, significantly impact cybersecurity in higher education institutions, emphasising the need for a robust security culture to mitigate risks.

## **2.6 SOCIAL MEDIA USAGE AND TRENDS IN MALAYSIA**

Over the past decade, social media use has spread across Malaysia to different age groups, from toddlerhood to old age. Malaysia's digital landscape has transformed significantly over the past decade, fueled by widespread internet access, the rising popularity of smartphones, and a growing dependence on social media. For many Malaysians, particularly the youth, social media has become an essential part of their day-to-day life—whether for staying connected with friends, seeking entertainment, learning, or even conducting self-business. With social media playing such a vital role, it's increasingly important to explore how young people engage with these platforms, what drives their usage, and the potential risks they may encounter, especially from a cybersecurity perspective.

To better understand social media penetration and platform popularity among Malaysians, Simon Kemp's 2024 DataReportal research provides the most up-to-date data, insights, and trends on how Malaysians engage with digital devices and services. The report estimates that Malaysia's internet penetration rate will reach 97.4% in 2024, with social media users making up nearly 28 million, or 83.1% of the total population (Simon, 2024). The survey indicates that the most popular platforms among Malaysian youth are Facebook, YouTube, Instagram, TikTok, LinkedIn, and X (formerly known as Twitter). The Malaysia Digital Report 2024 also highlighted that ChatGPT has seen