RESEARCH IN MANAGEMENT OF TECHNOLOGY AND BUSINESS
e-ISSN: 2773-5044

RMTB

Vol. 7 No. 1 (2026) 1077-1091
https://publisher.uthm.edu.my/periodicals/index.php/rmtb

The Relationship between Factors Influencing and Cybersecurity Awareness Among Youth Internet Users in Johor

Lim Jia Xuan[1], Nor Kamariah Kamaruddin[1*]

[1] *Department of Management and Technology, Faculty of Technology Management & Business, Universiti Tun Hussein Onn Malaysia, Batu Pahat, Johor, 86400, MALAYSIA*

*Corresponding Author: nkamariah@uthm.edu.my
DOI: https://doi.org/10.30880/rmtb.2026.07.01.081

Article Info

Received: 31March 2026
Accepted: 31 May 2026
Available online: 30 June 2026

Keywords

Cybersecurity awareness, Response efficacy, Self-efficacy, Perceived threats, Youth Internet users Johor

Abstract

Cybersecurity has emerged as a major concern within the modern digital environment, as the increasing rate of cybercrime is often linked to insufficient awareness and lack of cybersecurity knowledge among internet users. This study examines the relationships between response efficacy, self-efficacy, perceived threats, and cybersecurity awareness among youth internet users in Johor, Malaysia. The target population includes approximately 4,009,670 youth internet users in Johor. To obtain a reliable and representative sample, the Krejcie and Morgan sampling table was applied, resulting in a sample size of 384 respondents. A quantitative research design was implemented, with primary data gathered through an online questionnaire distributed via Google Forms. The collected responses were analyzed using the Statistical Package for the Social Sciences (SPSS). The findings demonstrated significant relationships between response efficacy, self-efficacy, perceived threats, and cybersecurity awareness among youth internet users in Johor. Based on these findings, this study aims to provide practical measures to improve cybersecurity awareness and minimize the risk of cybercrime among internet users.

1. Introduction

This study explores the relationship between self-efficacy, response efficacy, perceived threats, and cybersecurity awareness among youth internet users in Johor. This section presents the research background, problem statement, research objectives, research questions, scope, significance, and conclusion.

1.1 Problem Statement

Cybercrimes are increasingly at an alarming rate in Malaysia. Cybercrime and online scams are rising sharply in Malaysia, with nearly 34,497 cases reported in 2024, causing losses of up to RM1.2 billion (Malay Mail, 2024). In 2023, over 6,000 scam-related calls led to investigations involving RM105.4 million in losses (Malay Mail, 2024). Home Minister Datuk Seri Saifuddin reported a total of 35,368 cybercrime cases, resulting in losses of more than RM1.57 billion (Qistina Sallehuddin, 2025). These alarming figures highlight the urgent need for effective cybercrime prevention.

Furthermore, the issue is related to lack of awareness and cybersecurity knowledge among Malaysians. A study by CelcomDigi Berhad (2024) found that 65% of 10,983 respondents encountered scams, with generally low awareness of preventive measures. Prasad & Rohokale (2020) and Wang et al. (2020) emphasized that phishing and other cyber threats are worsened by poor awareness and insufficient mitigation strategies. Similarly,

Amanda Siddharta (2025) noted that cybersecurity awareness among Malaysians remains critically low, warranting targeted educational efforts for youth internet users.

Moreover, growing concern is the threat of deepfakes, powered by AI technology. Deepfakes are being misused for fraud and disinformation, with MCMC removing over 63,652 pieces of fake content in 2024, including impersonations and manipulated media (Selangor Journal, 2025). These AI-generated fakes make cyberattacks more convincing and harder to detect (Christopher Fam, 2024). So, it is increasingly critical for internet users to develop stronger literacy and critical thinking skills to identify and avoid falling victim to such sophisticated cyberthreats.

In addition, 27.4% of Malaysian internet users reported experiencing online fraud (Amanda Siddharta, 2023). With 28.68 million Malaysians on social media (83.1% of the population), users face increasing threats like spam, hacking, cyberbullying, and identity theft (Tahir Alfian, 2025). Therefore, this issue highlighted the urgent need to study cybersecurity awareness among internet users. As more individuals engage with digital platforms, they become more vulnerable to cybercrimes.

While previous studies have often focused on online banking (Jansen & van Schaik, 2018; Vafaei-Zadeh et al., 2024; Xuan et al., 2023) or specific populations like teachers and business managers (Ayanwale et al., 2024; Sharma, 2024; Ikpefan Ochei, 2023), few have explored cybersecurity awareness in the context of youth internet users. To address this gap, the current study focuses on youth, aiming to understand the factors influencing their cybersecurity behavior and awareness (Cele & Kwenda, 2024).

Therefore, to achieve the research objectives, the factors influencing cybersecurity awareness among youth internet users in Johor, namely response efficacy, self-efficacy, and perceived threats, are determined. Furthermore, the level of cybersecurity awareness among youth internet users in Johor is also identified. Consequently, the relationship between response efficacy, self-efficacy, perceived threats, and cybersecurity awareness among youth internet users in Johor is examined.

1.2 Scope of the Study

This study targets youth internet users in Johor, among the top three states with the highest cybercrime reports (Rashid Ating, 2022). The population includes individuals aged 15–40, who are increasingly targeted by cybercrimes (Yunus, 2007; Juremi, 2024). Johor's youth population is approximately 4,009,670 (Open DOSM, 2023), with a recommended sample size of 384 (Krejcie & Morgan, 1970). A quantitative approach using non-probability convenience sampling was applied, and data were analyzed with SPSS.

1.3 Significance of the Study

This study examines the factors influencing cybersecurity awareness among youth internet users in Johor, aiming to enhance awareness by educating them on cybercrimes such as phishing and online scams and promoting safer online behaviour. The findings support government agencies like MCMC and the Cyber Security Council in analyzing scam trends and improving cybersecurity policies, while also contributing to public education by encouraging preventive measures, community participation, and a more secure digital society.

2. Literature Review

The literature review provides a comprehensive summary of previous studies relevant to these variables, which clearly define the dependent variable and the independent variables. This section thoroughly examines existing research to deepen understanding of how these factors interact and influence cybersecurity awareness within the target population

2.1 Cybersecurity awareness

Cybersecurity protects digital systems, networks, and data from attacks and unauthorized access, serving as both a technical safeguard and strategic framework (Thakur & Raut, 2024). It includes network, application, and operational security, as well as disaster recovery and business continuity planning. Cybersecurity awareness helps individuals recognize threats and adopt safe behaviours (Sangwan, 2024; Maquosi, 2023), especially for social media users (Muhammad Agung Al Affan et al., 2025). Education on threats like phishing fosters preventive measures and promotes a culture of digital security (Tempestini et al., 2023; Dobák & Magyar, 2024).

2.1.1 Cybersecurity awareness among youth

Cybersecurity awareness is crucial for youth, who frequently use digital platforms and face risks such as phishing, identity theft, and data breaches. Studies show that youth with greater cybersecurity knowledge can better manage online threats (Kumar et al., 2024). In Malaysia, limited participation in awareness programs and lack of

adult guidance increase vulnerability, while community education and school-based curricula help reduce risks and promote safe online behaviour (Muhammad et al., 2024; B & Keerthana, 2024; Antunes et al., 2021).

2.2 Factors influencing cybersecurity awareness

Based on theory and past studies, there are a few factors that influence cybersecurity awareness. In this study, it focuses on the 3 variables as key factors such as response efficacy, self-efficacy and perceived threats which will be discussed in detail in the next sub-section.

2.2.1 Response Efficacy

Response efficacy, or belief in the effectiveness of recommended actions to reduce threats (Milne et al., 2000; Avery & Park, 2016), is key to cybersecurity awareness. When individuals trust that measures like security software or two-factor authentication protect them, they are more likely to adopt these practices. This belief motivates both immediate and future protective actions, helping translate cybersecurity knowledge into safe digital habits (Jalali, 2024; Alghazo & Humaidi, 2025). Thus, response efficacy positively impacts cybersecurity awareness and secure behavior adoption.

2.2.2 Self-efficacy

Self-efficacy, or an individual's belief in their ability to successfully perform actions (Bandura, 1977, 1982, 1986, 2004), is crucial for cybersecurity awareness. Individuals with high self-efficacy are more confident in managing cyber threats, following security protocols, and avoiding risky behaviors (Zadeh et al., 2024; Dodge et al., 2023). Higher self-efficacy promotes proactive knowledge seeking, responsible digital safety attitudes, and strengthens the link between knowledge, attitude, and behavior (Zainal et al., 2021). Training, education, and prior experience with cyber threats further enhance self-efficacy, fostering protective actions and effective threat responses (Dodge et al., 2023; Lee & Kim, 2023; Jalali, 2024).

2.2.3 Perceived Threats

Perceived threats, or an individual's assessment of the likelihood and severity of cyber risks, strongly influence motivation to adopt protective behaviors (Infante et al., 2019). Higher perceived threats encourage serious consideration of online risks and implementation of safety measures, while low perceived threats lead to vulnerability and poor cyber hygiene (Mkilia et al., 2023; Saleh et al., 2024; Kariuki et al., 2023). Psychological and sociocultural factors shape these perceptions, with those perceiving cyber risks as serious more likely to practice safe online behavior and engage in cybersecurity training (Sangwan, 2024; Hasan et al., 2024). Therefore, perceived threats are key in driving cybersecurity awareness and protective actions.

2.3 Past studies on relationship between response efficacy, self-efficacy, perceived threats and cybersecurity awareness

2.3.1 Relationship Between Response Efficacy and Cybersecurity Awareness

Empirical studies have found positive relationships between response efficacy and cybersecurity awareness (Hassan et al., 2024; Jalali, 2024; Khan et al., 2023; Latif et al., 2025; Vafaei-Zadeh et al., 2024). Khan et al. (2023) highlighted a positive relationship, showing that belief in protective measures like antivirus software promotes safer online behavior. Vafaei-Zadeh et al. (2024) also found a positive relationship in Malaysia, where individuals confident in their responses to cyber threats showed higher awareness. Similarly, Latif et al. (2025) and Hassan et al. (2024) reported a significant relationship among employees and e-service users in Malaysia, noting that belief in effective security tools like two-factor authentication improves engagement with cybersecurity practices. Jalali (2024) confirmed a positive relationship, showing that cues such as training increase users' confidence and awareness.

Therefore, the hypothesis is proposed as follows:

H1: There is a positive relationship between response efficacy and cybersecurity awareness.

2.3.2 Relationship Between Self-Efficacy and Cybersecurity Awareness

Past studies have shown a positive relationship between self-efficacy and cybersecurity awareness (Latif et al., 2025; Towhidi & Pridmore, 2022; Vafaei-Zadeh et al., 2024; Zainal et al., 2021). Towhidi and Pridmore (2022) found a positive relationship through cybersecurity labs that boosted students' self-efficacy and awareness. Vafaei-Zadeh et al. (2024) confirmed a positive relationship among online banking users in Malaysia. Zainal et al.

(2021) also reported that self-efficacy positively influenced teachers' cybersecurity awareness. Latif et al. (2025) found a positive relationship among Industry 4.0 employees, showing that high self-efficacy improves cybercrime preparedness. Similarly, Jalali (2024) showed a positive relationship, as confident individuals better recognize and manage cyber risks.

Based on the above empirical findings, hypothesis is proposed as follows:

H2: There is a positive relationship between self-efficacy and cybersecurity awareness

2.3.3 Relationship Between Perceived Threats and Cybersecurity Awareness

There are a few studies that proved there is a positive relationship between perceived threats and cybersecurity awareness (Douha et al., 2023; Hassan et al., 2024; Zainal et al., 2021). For instance, Douha et al. (2023) found a significant relationship, showing that as perceived threats increase, individuals become more aware of cybersecurity risks and more motivated to adopt protective behaviors. Similarly, Hassan et al. (2024) discovered that students who recognize potential cyber risks are more inclined to learn and apply security measures, especially in digital learning settings. In contrast, Zainal et al. (2021), in their study on online banking users in Malaysia, reported no significant relationship. This may be due to users not perceiving threats as personally relevant, possibly influenced by optimism bias or lack of direct experience with cyberattacks.

Therefore, it is hypothesized that:

H3: There is a positive relationship between perceived threats and cybersecurity awareness.

2.4 Conceptual Framework

The conceptual framework for this study as shown in Figure 1 illustrates the hypothesized relationships between three key independent variables which are response efficacy, self-efficacy and perceived threats and the dependent variable which is cybersecurity awareness. This framework deceived based on the findings on empirical studies and hypothesis development in the previous sub-section.

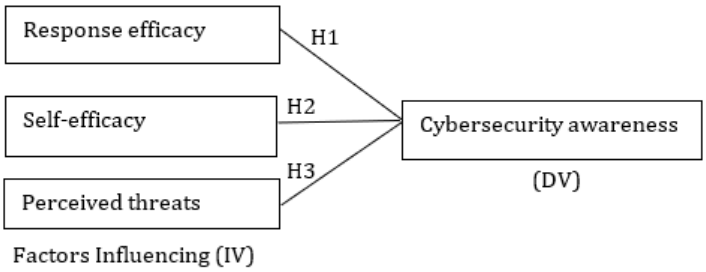

Fig. 1 *Conceptual Framework*

3. Research Methodology

The research methodology section outlines the essential procedures and information required to achieve the study's results. It provides comprehensive details on the research workflow, strategies, and approaches applied. The methodology employed in conducting the study must be clearly and systematically explained.

3.1 Research Design

This study adopts a quantitative research design to systematically examine relationships between independent and dependent variables using statistical techniques. Data are collected through an online questionnaire and analyzed using descriptive and correlational methods. A non-probability convenience sampling method is used to target youth internet users in Johor due to its practicality (Alex, 2024). Data analysis is conducted using the Statistical Package for the Social Sciences (SPSS).

3.2 Research Population and Sampling

3.2.1 Population

The target group of individuals who participate in or have been selected by the researcher for the study may be referred to as the population. The population size for this study consists of youth internet users in Johor. Based on the Department of Statistics Malaysia (DOSM), the population number of youth in Johor comprised of 4,009,670.

Research in Management of Technology and Business Vol. 7 No. 1 (2026) p. 1077-1091

3.2.2 Sampling

The sampling size is a noun that specifies the number of participants in sample size market research. Sampling size refers to the real population and provides a representative number for the research. Based on the table of Krejcie and Morgan (1970), the sample size of this research was 384. Hence, the researcher chose the respondents who were willing to participate in the research to take part in the study.

3.2.3 Sampling Technique

The respondents were youth internet users from Johor, selected using a convenience sampling technique, which involves choosing participants based on availability and willingness, as they are easily accessible rather than randomly selected from the population (Fleetwood, 2018).

3.3 Research Instrument

3.3.1 Survey Design

Table 1 examines factors influencing cybersecurity awareness among youth internet users in Johor, comprising three sections: Section A on demographics, Section B on influencing factors, and Section C on cybersecurity awareness. All questions are mandatory and use a five-point Likert scale from "Strongly Disagree" to "Strongly Agree."

Table 1 *Survey Design*

Section	Interpretation	Scale
A	Demographic	Nominal scale
B	Independent variables: - Response efficacy - Self-efficacy - Perceived Threats	Five-point Likert scale: (Strongly disagree to Strongly agree)
C	Cybersecurity awareness	

3.3.2 Item Measurement

Table 2 shows that measurement items for response efficacy, self-efficacy, perceived threats, and cybersecurity awareness were adapted from established sources for content validity. All variables used a 5-point Likert scale from "Strongly Disagree" to "Strongly Agree" to assess participants' agreement.

Table 2 *Item Measurement of AI Chatbot Attributes*

Sec.	Variables	Scale	References
B	Response efficacy	Five-point Likert scale: (Strongly disagree to Strongly agree)	Ifinedo (2012)
	Self-efficacy		Vrhovec and Mihelic (2021)
	Perceived threats		Vrhovec and Mihelic (2021)
C	Cybersecurity awareness		Nwankpa and Datta (2023)

3.4 Pilot Study

Pilot studies, or feasibility studies, are small-scale tests used to assess research design and feasibility (Simkus, 2023). In this study, a pilot survey involving 20 youth internet users in Johor (25th July–31st August 2025) was conducted to ensure clarity and reliability. The results, analyzed using SPSS and Cronbach's alpha, were used to refine the methodology for the main study.

3.5 Data Collection

Data collection involves systematically gathering information to meet research objectives (Simkus, 2023). This study used primary data from a Google Form survey of 384 youth internet users in Johor and secondary data from existing literature to support the findings.

3.6 Data Analysis

This study used the Statistical Package for the Social Sciences (SPSS) to analyze quantitative data. SPSS is widely utilized across disciplines for processing complex data and supports researchers by organizing results into tables and graphical formats (Williams, 2025). It simplifies calculations, improves accuracy, and reduces the complexity of traditional data analysis methods (Noels, 2018). For this research, SPSS was used to conduct descriptive analysis, reliability analysis, normality analysis, and correlation analysis, enabling efficient evaluation of the collected data (Williams, 2025).

4. Results and Discussion

This section presents the results of the data analysis, including demographic, reliability, descriptive, normality, and correlation analyses. It begins with an overview of the response rate and concludes with a summary of the key findings.

4.1 Response Rate

A total of 384 online questionnaires were distributed to youth in Johor via social media platforms such as Facebook and WhatsApp using Google Forms. Table 3 shows the survey obtained 230 valid responses, resulting in a response rate of 59.89%. This rate exceeds the typical response rate of approximately 14% among Malaysian youth reported in the National Survey of Malaysia Youth Public Opinion (2019) and is therefore considered acceptable for this study.

Table 3 *Response Rate*

Sample size	Questionnaire Distributed	Returned Questionnaire	Percentage
384	384	230	59.89%

4.2 Reliability Analysis

Reliability analysis was conducted to assess the consistency of the research instruments. The Statistical Package for the Social Sciences (SPSS) will be used to evaluate internal consistency using Cronbach's alpha.

4.2.1 Pilot Study

A pilot study with 20 respondents was conducted using SPSS to assess questionnaire reliability. As shown in Table 4, all variables demonstrated excellent internal consistency, with Cronbach's alpha values of 0.897 (response efficacy), 0.905 (self-efficacy), 0.955 (perceived threats), and 0.945 (cybersecurity awareness).

Table 4 *Reliability for Pilot Study Result*

Variables	No items	Cronbach's Alpha value for the pilot study (20 respondents)	Interpretation
Independent Variable:			
Response efficacy	3	0.897	Very Good
Self-efficacy	3	0.905	Excellent
Perceived Threats	4	0.955	Excellent
Dependent Variable:			
Customer Experience	9	0.951	Excellent

4.2.2 Actual Study

Following the pilot study, the actual study confirmed the reliability of the survey instruments. As shown in Table 5, all variables demonstrated very good to excellent internal consistency, with Cronbach's alpha values of 0.828 for response efficacy, 0.801 for self-efficacy, 0.910 for perceived threats, and 0.867 for cybersecurity awareness. These results indicate that the instruments used were reliable.

Table 5 *Reliability for Actual Study Result*

Variables	No items	Cronbach's Alpha value for the actual study (230 respondents)	Interpretation

Independent Variable:			
Response efficacy	3	0.828	Very Good
Self-efficacy	3	0.801	Very Good
Perceived threats	4	0.910	Excellent
Dependent Variable:			
Cybersecurity awareness	9	0.867	Very Good

4.3 Demographic Analysis

A demographic analysis was conducted to examine the frequency and percentage of participants' responses across key characteristics. Table 6 presents the demographic and cybersecurity-related characteristics of the respondents. It includes information on gender, age, race, educational level, experience with cybercrimes, usage of cybersecurity tools or measures, and exposure to formal cybersecurity education or training.

Table 6 *Demographic information of respondents*

Demographic	Item	Frequency	Percentage (%)
Gender	Male	68	29.6
	Female	162	70.4
Age	Between 15 and 24 years old	117	50.9
	Between 25 and 34 years old	61	36.5
	Between 35 and 40 years old	52	22.6
Race	Malay	36	15.7
	Chinese	173	75.2
	Indian	21	9.1
Educational level	Primary / Secondary	68	29.6
	Diploma	63	27.4
	Bachelor's Degree	92	40.0
	Master's Degree	7	3.0
Have you ever encountered cybercrimes?	Yes	158	68.7
	No	72	31.3
Do you regularly use cybersecurity tools or measures? (e.g., antivirus, two factor authentication)	Yes	158	68.7
	No	72	31.3
Have you received any formal education or training in cybersecurity awareness?	Yes	83	36.1
	No	147	63.9

4.4 Descriptive Analysis

This section uses descriptive analysis to examine study variables, calculating the mean and standard deviation for response efficacy, self-efficacy, perceived threat, and cybersecurity practices to show average responses and the variation around them.

4.4.1 Response Efficacy

Table 7 shows respondents' beliefs in the effectiveness of security measures. The statements on protecting personal information and preventing hacker access both recorded the highest mean of 3.85 (σ = 1.02 and 1.06), while detecting hacker attacks scored 3.83 (σ = 0.99). Overall, Response Efficacy had a high total mean of 3.84 with a standard deviation of 1.02 which the level of response efficacy was high.

Table 7 *Descriptive Analysis for Response Efficacy*

Statement	Mean	Std.Deviation	Interpretation
1. Enabling the security measures on my device is an effective way to detect hacker attacks	3.83	0.99	High

2. Enabling security measures at my device will prevent hackers from gaining access to important personal information	3.85	1.06	High
3. The effectiveness of available measures to protect my personal information from security violations	3.85	1.02	High
Total average score	3.84	1.02	High

4.4.2 Self-efficacy

Table 8 shows respondents' confidence in performing protective actions against cyberthreats. The statement on having no problems using protective measures scored the highest mean of 3.73 (σ = 0.98), while taking measures under one's control and having the necessary resources scored 3.56 (σ = 1.08) and 3.53 (σ = 1.08), respectively. Overall, self-efficacy had a high total mean of 3.61 with a standard deviation of 1.05 so the level of self-efficacy was high.

Table 8 *Descriptive Analysis for Responsiveness*

Statement	Mean	Std.Deviation	Interpretation
1. I have no problems using protective measures against cyberattacks.	3.73	0.98	High
2. Taking a protective measure against cyberattacks is entirely under my control.	3.56	1.08	Moderate
3. I have all resources and skills needed to take protective measures against cyberattacks.	3.53	1.08	Moderate
Total average score	3.61	1.05	High

4.4.3 Perceived Threats

Table 9 shows respondents perceived threats toward cybersecurity issues. The highest mean score was recorded for the importance of protecting information on personal devices (M = 4.33, σ = 0.84), followed by concerns over unauthorized access to confidential information (M = 4.23, σ = 0.92). Perceptions of cyberattacks and their consequences as serious threats also reported high mean scores above 4.00. Overall, perceived threats demonstrated a high total mean of 4.20 with a standard deviation of 0.89 which indicates the respondents have a high level of perceived threats.

Table 9 *Descriptive Analysis for Perceived Threats*

Statement	Mean	Std.Deviation	Interpretation
1. Cyberattacks pose a serious threat to my personal information.	4.07	0.92	High
2. Consequences of successful cyberattacks would highly threaten my personal information.	4.17	0.88	High
3. Having my confidential information on my device accessed by someone without my consent or knowledge would be a serious problem for me.	4.23	0.92	High
4. I believe that protecting the information on my device is important.	4.33	0.84	High
Total average score	4.20	0.89	High

4.4.4 Cybersecurity Awareness

Table 10 shows a high level of agreement for Cybersecurity Awareness, with all seven items scoring above 4.00 and a total mean of 4.18 (σ = 0.78). The highest agreement was for "I understand that safe security practices are essential to protect my personal data against cyberattacks" (μ = 4.32, σ = 0.72), followed by "I recognize that I have to take security protection measures to protect my personal information assets against cyberattacks" (μ = 4.31, σ = 0.69) and "I recognize that safe security practices are needed to deal with cybersecurity risks" (μ = 4.23, σ = 0.79). Other items also indicate strong awareness and capability, confirming respondents' high perception of cybersecurity knowledge and practices. Thus, the level of cybersecurity was high.

Research in Management of Technology and Business Vol. 7 No. 1 (2026) p. 1077-1091

Table 10 *Descriptive Analysis for Cybersecurity awareness*

Statement	Mean	Std.Deviation	Interpretation
1. I recognize that safe security practices are needed to deal with cybersecurity threats.	4.09	0.89	High
2. I recognize that safe security practices are needed to deal with cybersecurity risks.	4.23	0.79	High
3. I understand that safe security practices are essential to protect my personal data against cyberattacks.	4.32	0.72	High
4. I have the knowledge to recognize and respond to cybersecurity threats and risks.	4.12	0.79	High
5. I have the capability to recognize and respond to cybersecurity threats and risks.	4.05	0.82	High
6. I am aware of the cybersecurity threats and risks I face when doing my job	4.13	0.77	High
7. I recognize that I have to take security protection measures to protect my personal information assets against cyberattacks	4.31	0.69	High
Total average score	4.18	0.78	High

4.5 Normality Analysis

Table 11 shows that all p-values for the independent variables (response efficacy, self-efficacy, perceived threats) and the dependent variable (cybersecurity awareness) are < 0.001, indicating non-normal distribution. Therefore, Spearman's rank-order correlation analysis was used.

Table 11 *Kolmogorov-Smirnov Test of Normality*

	Kolmogorov-Smirnov[a]		
Independent Variables	Statistic	df	Sig.
Response Efficacy	0.205	230	<.001
Self-efficacy	0.123	230	<.001
Perceived Threats	0.259	230	
Dependent Variable			
Cybersecurity awareness	0.119	230	<.001

4.6 Correlation Analysis and Hypothesis Testing

Table 12 presents Spearman's correlation between response efficacy, self-efficacy, perceived threats, and cybersecurity awareness among youth in Johor. Response efficacy shows a moderate positive correlation (r = 0.489, p < .001), self-efficacy is a moderately strong correlation (r = 0.576, p < .001), and perceived threats a strong correlation (r = 0.628, p < .001). All hypotheses are accepted, indicating that higher levels of these factors correspond to higher cybersecurity awareness.

Table 12 *Result of Spearman's Correlation*

Correlation Analysis Spearman's rho		Cybersecurity Awareness	Hypothesis Result
Response Efficacy	Correlation Coefficient	0.489**	Accepted
	Sig. (2-tailed)	<.001	
	N	230	
Self-efficacy	Correlation Coefficient	0.576**	Accepted
	Sig. (2-tailed)	<.001	
	N	230	
Perceived Threats	Correlation Coefficient	0.628**	Accepted
	Sig. (2-tailed)	<.001	
	N	230	
Cybersecurity Awareness	Correlation Coefficient	1.000	

	Sig. (2-tailed)	.
	N	230

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

5. Discussion, Recommendations and Conclusion

5.1 Overview of Study

This study aimed to examine the relationship between response efficacy, self-efficacy, perceived threats and cybersecurity awareness among youth internet users in Johor. This discussion has been divided into three objectives of this study.

5.2 Discussion Based on Research Objectives

This study aimed to identify the level of AI chatbot attributes (usability and responsiveness) in the e-commerce industry among Gen Y in Selangor, identify the level of customer experience in the e-commerce industry among Gen Y in Selangor, and examine the relationship between AI chatbot attributes and customer experience in the e-commerce industry among Gen Y in Selangor.

5.2.1 To identify the level of factors (response efficacy, self-efficacy, perceived threats) influence cybersecurity awareness among youth internet users in Johor

Research Objective 1 identifies the levels of response efficacy, self-efficacy, and perceived threats among youth internet users in Johor. The descriptive analysis indicates moderate to high mean values for response efficacy (mean = 3.84), self-efficacy (mean = 3.61), and perceived threats (mean = 4.20), with perceived threats being the highest, reflecting strong awareness of cybersecurity risks.

Youth internet users generally perceive cyber threats as serious, particularly in relation to personal information protection. High mean scores for items related to data misuse, privacy breaches, and online fraud indicate heightened concern over cyber risks. This pattern is consistent with Douha et al. (2023) and Hassan et al. (2024), who reported similarly high levels of perceived threats among internet users. The moderately high level of response efficacy suggests that respondents believe cybersecurity measures are effective in reducing risks, aligning with findings by Khan et al. (2023), Vafaei-Zadeh et al. (2024), and Latif et al. (2025).

In addition, self-efficacy recorded a moderate level, indicating reasonable confidence in applying protective measures, though lower than perceived threats. This finding aligns with Towhidi and Pridmore (2022) and Jalali (2024), which also reported moderate self-efficacy among internet users, suggesting that awareness of risks may be higher than confidence in consistently applying cybersecurity practices. Overall, youth internet users in Johor demonstrate moderate to high cybersecurity awareness, with scope to further strengthen confidence in protective practices.

5.2.2 To identify the level of cybersecurity awareness among youth internet users in Johor

Research Objective 2 examines the level of cybersecurity awareness among youth internet users in Johor. The descriptive analysis shows a high level of cybersecurity awareness (mean = 4.18, SD = 0.78), indicating that respondents generally understand cybersecurity issues and the importance of safe online practices.

This high awareness is reflected in respondents' agreement that safe security practices are essential for protecting personal data and that they possess the knowledge to recognize and respond to cyber threats. This finding supports Kumar et al. (2024), who noted that youths with adequate cybersecurity knowledge are better able to detect threats and take protective actions.

Despite frequent exposure to cyber risks such as phishing, identity theft, and data breaches, the findings indicate that youth internet users in Johor have developed relatively high cybersecurity awareness. This may be attributed to increased public discussion on online scams, awareness campaigns, and access to digital safety information, aligning with B and Keerthana (2024).

The findings are also consistent with Antunes et al. (2021), who emphasized the role of education in preparing youth to manage digital risks. Overall, youth internet users in Johor demonstrate a high level of cybersecurity awareness, although continuous educational and community-based efforts remain important to sustain and further enhance this awareness.

5.2.3 To Examine the Relationship Between AI Chatbot Attributes (Usability and Responsiveness) and Customer Experience in the E-Commerce Industry among Gen Y in Selangor

This study examines the relationship between response efficacy, self-efficacy, perceived threats, and cybersecurity awareness among youth internet users in Johor. The correlation analysis shows that all three factors have positive relationships with cybersecurity awareness, with perceived threats showing the strongest relationship (r = 0.628), followed by self-efficacy (r = 0.576) and response efficacy (r = 0.489).

The findings show that response efficacy is positively related to cybersecurity awareness, as youth who believe in the effectiveness of security measures tend to demonstrate higher awareness. The findings align with Khan et al. (2023), Vafaei-Zadeh et al. (2024), and Latif et al. (2025).This suggests that when youth believe security measures are effective, they are more likely to pay attention to cybersecurity issues and practise safer online behaviours, thereby strengthening their overall awareness.

Similarly, self-efficacy demonstrates a positive relationship with cybersecurity awareness, indicating that youth who feel confident in taking protective actions have higher awareness levels. The findings align with Towhidi and Pridmore (2022), Zainal et al. (2021), and Latif et al. (2025).This suggests that youth who believe in their own ability to recognise threats, avoid scams, and respond appropriately to cyber risks are more attentive to cybersecurity information. Higher self-efficacy empowers individuals to actively apply security knowledge in real-life situations, reinforcing their awareness and preparedness against online threats.

Among the three factors, perceived threats show the strongest positive relationship with cybersecurity awareness, suggesting that youth who perceive cyber risks as serious are more alert to online threats. The findings align with Douha et al. (2023) and Hassan et al. (2024). This implies that recognizing the severity and potential consequences of cyber threats, such as identity theft or financial loss, enhances alertness among youth internet users. Perceiving cyber risks as serious and personally relevant motivates individuals to seek information and practice caution online, thereby strengthening cybersecurity awareness.

Overall, the findings indicate that response efficacy, self-efficacy, and perceived threats are significantly related to cybersecurity awareness among youth internet users in Johor, with perceived threats emerging as the strongest influencing factor.

5.3 Implications of the Study

The study highlights the need to enhance cybersecurity awareness among youth in Johor by addressing response efficacy, self-efficacy, and perceived threats. Authorities, schools, and organizations can implement targeted programs, such as workshops, online training, and interactive activities, to teach safe online practices and reinforce confidence in handling cyber threats. Participatory approaches like simulations and gamified learning can further improve engagement and knowledge retention, fostering a proactive and secure online behaviour among youth

5.4 Research Limitation

Several limitations were identified in this study. First, the scope was limited to youth internet users in Johor, which may affect the generalizability of the findings to other populations. Second, using only a quantitative approach with structured questionnaires restricted the depth of insights, as respondents could not elaborate on their experiences or views. Lastly, the cross-sectional design captures data at a single point in time, limiting the ability to examine changes in cybersecurity awareness or establish causal relationships over time.

5.5 Recommendations

To address the study's limitations, future research should expand the target population to include a broader demographic across Johor, capturing respondents of different ages, occupations, and backgrounds for more representative findings. Researchers are also encouraged to adopt a mixed-method approach, combining surveys with interviews or focus groups, to gain deeper and more contextualized insights into cybersecurity experiences. Additionally, implementing a longitudinal design would allow the monitoring of changes in cybersecurity awareness and behaviour over time, providing stronger evidence of trends and causal relationships and enhancing understanding of cybersecurity issues among internet users.

5.6 Conclusion

In conclusion, this study provides valuable insights into factors influencing cybersecurity awareness among youth internet users in Johor, emphasizing the roles of response efficacy, self-efficacy, and perceived threats. Targeted strategies addressing these factors can enhance awareness and reduce cyber risks. As digital threats

evolve, stakeholders must proactively promote cybersecurity education and preventive measures to foster informed, vigilant, and responsible internet users, ensuring a safer online environment.

Acknowledgement

The author would like to thank the person who helped with this research. The author would also like to thank the supervisor and the Faculty of Technology Management and Business for their support.

Conflict of Interest

Authors declare that there is no conflict of interests regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: ***study conception and design:*** *L.J.X., N.K.K.;* ***data collection:*** *L.J.X., N.K.K.;* ***analysis and interpretation of results:*** *L.J.X., N.K.K.;* ***draft manuscript preparation:*** *L.J.X., N.K.K. All authors reviewed the results and approved the final version of the manuscript.*

References

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, Challenges and Future Directions. *Cyber Security and Applications*, *2*(2). https://doi.org/10.1016/j.csa.2023.100031

Amanda Siddharta. (2023, November 3). *Malaysia: cyber crime experience 2022*. Statista. https://www.statista.com/statistics/901448/malaysia-cyber-crime-experience/

Amanda Siddharta. (2024, December 12). *Malaysia number of internet users 2014-2019*. Statista; Statista. https://www.statista.com/statistics/553752/number-of-internet-users-in-malaysia/

Amanda Siddharta. (2025, January 2). *Malaysia: cyber crime incidents 2024*. Statista. https://www.statista.com/statistics/1043272/malaysia-cyber-crime-incidents/

Amanda Siddharta. (2023, December 21). *Internet usage in Malaysia*. Statista. https://www.statista.com/topics/11756/internet-usage-in-malaysia/#topicOverview

Antunes, M., Silva, C., & Marques, F. (2021). An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context. *Applied Sciences*, *11*(23), 11269. https://doi.org/10.3390/app112311269

Asaad, R. R., & Saeed, V. A. (2022). A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution. *Applied Computing Journal*, *2*(4), 227–244. https://doi.org/10.52098/acj.202260

Avery, E., & Park, S. (2016). Effects of crisis efficacy on intentions to follow directives during crisis. *Journal of Public Relations Research*, *28*(2), 72–86. https://doi.org/10.1080/1062726x.2016.1165681

B, P., & Keerthana, J. S. (2024). A STUDY ON AWARENESS OF ONLINE EMPLOYMENT SCAM. *EPRA International Journal of Multidisciplinary Research (IJMR)*, *10*(4), 1–1. https://eprajournals.com/IJMR/article/12721

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*, *37*(2), 122–147. https://doi.org/10.1037/0003-066X.37.2.122

Bandura, A. (1986). The explanatory and predictive scope of self-efficacy theory. *Journal of Social and Clinical Psychology*, *4*(3), 359–373. https://doi.org/10.1521/jscp.1986.4.3.359

Bandura, A. (2004, April 1). *Health Promotion by Social Cognitive Means*. Health Education & Behavior : The Official Publication of the Society for Public Health Education. https://pubmed.ncbi.nlm.nih.gov/15090118/

BERNAMA. (2024, July 17). *High Cases Of Scam Victims, Low Resilience In Malaysia - National Scam Awareness Survey 2024*. BERNAMA. https://www.bernama.com/en/news.php?id=2318397

Bhat, A. (2021, February 17). *Online questionnaire: Definition, advantages and examples*. QuestionPro. https://www.questionpro.com/blog/online-questionnaire/

Cele, N. N., & Kwenda, S. (2024). Do Cybersecurity Threats and Risks Have an Impact on the Adoption of Digital banking? a Systematic Literature Review. *Journal of Financial Crime*, *32*(1). https://doi.org/10.1108/jfc-10-2023-0263

Editor Selangor Journal. (2025, January 14). *Cybersecurity predictions for 2025: Insights for local businesses*. Media Selangor. https://selangorjournal.my/2025/01/cybersecurity-predictions-for-2025-insights-for-local-businesses/

Fleetwood, D. (2018). *Convenience Sampling: Definition, Method and Examples | QuestionPro*. QuestionPro. https://www.questionpro.com/blog/convenience-sampling/

Hasan, S. A., AlJazeeri, F. H., Abdulla, H. H., AlMahafdha, Z. S., & AlAmmary, J. H. (2024). A Systematic Literature Review of Models and Factors Influencing E-Learning Cybersecurity Awareness Among University Students. *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 405–412. https://doi.org/10.1109/3ict64318.2024.10824546

Hassan, S., Ahmad, R., Norliza Katuk, Norhasyimatul Naquiah Ghazali, Jazzanul Azriq Aripin, & Ali, F. (2024). Staying One Step Ahead: Exploring Protection Motivation Theory to Combat Cyber-fraud Among E-services Users. *Procedia Computer Science*, *234*, 1364–1371. https://doi.org/10.1016/j.procs.2024.04.011

Hillier, W. (2022, November 30). *What is Secondary Data? [Examples, Sources & Advantages]*. CareerFoundry. https://careerfoundry.com/en/blog/data-analytics/what-is-secondary-data/

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

ikpefan Ochei. (2023). *Cybersecurity Issues Affecting Online Banking and Transactions in Nigeria*. https://www.academia.edu/97390153/CYBERSECURITY_ISSUES_AFFECTING_ONLINE_BANKING_AND_TRANSACTIONS_IN_NIGERIA

Jalali, F. (2024). Cybersecurity Behavior During COVID-19 and the Impact of Policy Awareness and Demographics on Information Security Behavior and Its Determinants. *OPAL (Open@LaTrobe) (La Trobe University)*. https://doi.org/10.32920/25418173.v1

Jansen, J., & van Schaik, P. (2018). Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior*, *87*, 371–383. https://doi.org/10.1016/j.chb.2018.05.010

John, N. (2018, September 17). *What is SPSS and its importance in research & data analysis?* Medium. https://johnnoels.medium.com/what-is-spss-and-its-importance-in-research-data-analysis-5f109ab90da1

Jones, S. L., Collins, E. I. M., Levordashka, A., Muir, K., & Joinson, A. (2019). What is "Cyber Security"?. *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3290607.3312786

Julia, S. (2023, July 31). *What is a Pilot Study?* SimplyPsychology. https://www.simplypsychology.org/pilot-studies.html

JUREMI, J. (2024, November 24). *Target: The young and vulnerable*. The Star. https://www.thestar.com.my/news/focus/2024/11/24/target-the-young-and-vulnerable

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Computers & Security*, *125*, 103049. https://doi.org/10.1016/j.cose.2022.103049

Krejcie, R. V., & Morgan, D. W. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement*, *30*(3), 607–610. https://doi.org/10.1177/001316447003000308

Latif, A., Sulaiman, N. S., Nur, Yacob, A., & Nasir, A. (2025a). Development of Cybersecurity Awareness Model Based on Protection Motivation Theory (PMT) for Digital IR 4.0 in Malaysia. *International Journal of Advanced Computer Science and Applications*, *16*(3). https://doi.org/10.14569/ijacsa.2025.01603117

Latif, A., Sulaiman, N. S., Nur, Yacob, A., & Nasir, A. (2025b). Development of Cybersecurity Awareness Model Based on Protection Motivation Theory (PMT) for Digital IR 4.0 in Malaysia. *International Journal of Advanced Computer Science and Applications*, *16*(3). https://doi.org/10.14569/ijacsa.2025.01603117

Li, Y., Wang, J., & H, R. R. (2017). *AIS Electronic Library (AISeL) - AMCIS 2017 Proceedings: Adoption of Identity Protection Service: An Integrated Protection Motivation – Precaution Adoption Process Model*. Aisnet.org. https://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/23/

Malaysia, D. of S. (n.d.). *Johor Kawasanku | OpenDOSM*. Open.dosm.gov.my. https://open.dosm.gov.my/dashboard/kawasanku/Johor

Mukhtar, A. M. (2024, January 24). *Youngsters not immune to online scams, says criminal analyst | New Straits Times*. NST Online. https://www.nst.com.my/news/nation/2024/01/1005209/youngsters-not-immune-online-scams-says-criminal-analyst

National Survey of Malaysia Youth Public Opinion. (2019). https://www.iri.org/wp-content/uploads/2019/10/malaysia_youth_national_survey_july_2019.pdf

New Straits Times. (2023, November 2). *Malaysia ranks 3rd in world for spending most time online*. NST Online. https://www.nst.com.my/lifestyle/bots/2023/11/974088/malaysia-ranks-3rd-world-spending-most-time-online

Nwankpa, J. K., & Datta, P. (2023). Remote Vigilance: The Roles of Cyber Awareness and Cybersecurity Policies Among Remote Workers. *Computers & Security*, *130*(1), 103266–103266. https://doi.org/10.1016/j.cose.2023.103266

Rashid Ating. (2022, March). *Patterns And Types Of Cybercrime In Malaysia From 2016 To 2021: Part 2*. Smart Investor Malaysia; Smart Investor. https://smartinvestor.com.my/patterns-and-types-of-cybercrime-in-malaysia-from-2016-to-2021-part-2/

Saleh, T., Kanaan, R., Alzubaidi, R., Kanaan, G. G., & Nino, M. (2025). Factors affecting cybersecurity awareness: A qualitative study in Saudi Arabia. *Uncertain Supply Chain Management*, *13*(4), 751–762. https://doi.org/10.5267/j.uscm.2024.12.005

Tan, B. (2023, September 21). *Report: Malaysia's data breach cases hit all-time high, with four-fold increase recorded in 2023*. Malay Mail. https://www.malaymail.com/news/malaysia/2023/09/21/report-malaysias-data-breach-cases-hit-all-time-high-with-four-fold-increase-recorded-in-2023/92075

The scamdemic targeting the young and vulnerable . (2024). Astroawani.com. https://international.astroawani.com/malaysia-news/scamdemic-targeting-young-and-vulnerable-497309

The Star Online. (2024, November 18). *Malaysia tops Asia in scam revictimisation rate*. The Star. https://www.thestar.com.my/news/nation/2024/11/18/malaysia-tops-asia-in-scam-revictimisation-rate

Total of 34,497 online scam cases reported, losses estimated at RM1.2b last year, Dewan Negara told. (2024, March 18). Malay Mail. https://www.malaymail.com/news/malaysia/2024/03/18/total-of-34497-online-scam-cases-reported-losses-estimated-at-rm12b-last-year-dewan-negara-told/124108

Towards a Safe and Resilient Digital Malaysia National Scam Awareness Survey 2024 Report. (2024). Celcomdigi.com. https://corporate.celcomdigi.com/news/2024-scam-report-malaysians-are-still-susceptible-to-scams-despite-high-awareness

Towhidi, G., & Pridmore, J. (2022). Increasing cybersecurity interest and self-efficacy through experiential labs . *Issues in Information Systems*, *23*(2). https://doi.org/10.48009/2_iis_2022_110

Vafaei-Zadeh, A., Davoud Nikbin, Teoh, K. Y., & Haniruzila Hanifah. (2024). Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia. *International Journal of Bank Marketing*. https://doi.org/10.1108/ijbm-03-2024-0138

Vrhovec, S., & Blaž Markelj. (2024). We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers. *PLoS ONE*, *19*(10), e0312266–e0312266. https://doi.org/10.1371/journal.pone.0312266

Vrhovec, S., & Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Computers & Security*, *106*, 102309. https://doi.org/10.1016/j.cose.2021.102309

Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, *62*, 100415. https://doi.org/10.1016/j.ijlcj.2020.100415

Williams, K. (2024, May 23). *Master Survey Design: A 10-step Guide with Examples*. SurveySparrow. https://surveysparrow.com/blog/survey-design/

Williams, K. (2025, March 17). *What is SPSS? Definition, Features, Types, and Use Cases*. SurveySparrow. https://surveysparrow.com/blog/what-is-spss/

Yunus, F. (2007). *Youth Employment and Employability in Malaysia*. https://www.iyres.gov.my/jdownloads/kertaskerja/youth-employment-and-employability-in-malaysia.pdf

Zainal, N. C., Puad, M. H. M., & Sani, N. F. M. (2021). Moderating Effect of Self-Efficacy in the Relationship Between Knowledge, Attitude and Environment Behavior of Cybersecurity Awareness. *Asian Social Science*, *18*(1), 55. https://doi.org/10.5539/ass.v18n1p55

Zhang, W., Xiong, S., Zheng, Y., & Wu, J. (2022). Response Efficacy and Self-Efficacy Mediated the Relationship between Perceived Threat and Psychic Anxiety among College Students in the Early Stage of the COVID-19 Pandemic. *International Journal of Environmental Research and Public Health*, *19*(5), 2832. https://doi.org/10.3390/ijerph19052832