Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934

CYBER SCAM VICTIMIZATION RISK AMONG GENERATION Z AND ITS DETERMINANTS

Nurul Hafizah Azizan[1*]
Nor Asma Mohd Zin[2]
Nur Azureen Abd Hadi[3]
Nur Haslina Ramli[4]

[1] Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Cawangan Kelantan, Kampus Kota Bharu, 15050 Kota Bharu, Kelantan, Malaysia (E-mail: : hafizahaz@uitm.edu.my)
[2] Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Cawangan Kelantan, Kampus Machang, 18500 Machang, Kelantan, Malaysia (E-mail: norasma@uitm.edu.my)
[3] Faculty of Business and Management, Universiti Teknologi MARA Cawangan Kelantan, Kampus Machang, 18500 Machang, Kelantan, Malaysia (E-mail: azureen@uitm.edu.my)
[4] Faculty of Business and Management, Universiti Teknologi MARA Cawangan Kelantan, Kampus Machang, 18500 Machang, Kelantan, Malaysia (E-mail: haslina581@uitm.edu.my)
*Corresponding author: hafizahaz@uitm.edu.my

Article history
Received date : 7-9-2026
Revised date : 8-9-2026
Accepted date : 20-10-2026
Published date : 28-10-2026

To cite this document:
Azizan, N. H., Mohd Zin, N. A., Abd Hadi, N. A., & Ramli, N. H. (2026). Cyber scam victimization risk among Generation Z and its determinants. *International Journal of Accounting, Finance and Business (IJAFB),* 11 (69), 440-455.

Abstract: *The increasing prevalence of cyber scams has raised concerns about the vulnerability of Generation Z (Gen Z), who are highly engaged with digital technologies and online platforms. This study examined cyber scam victimization risk among Gen Z and its determinants, focusing on four cybersecurity behaviours: data privacy, password management, device and internet usage, and social media management. A cross-sectional quantitative design was employed involving 231 undergraduate students at Universiti Teknologi MARA (UiTM) Kelantan Branch, Kota Bharu Campus. Data were collected using a structured questionnaire and analysed using descriptive analysis, reliability analysis, Pearson correlation analysis, and multiple linear regression. The results revealed that data privacy, device and internet usage, and social media management were significant negative predictors of cyber scam victimization risk. In contrast, password management was not statistically significant when the other predictors were considered simultaneously. These findings indicate that better practices in protecting personal data, using devices and the internet safely, and managing social media responsibly are associated with lower cyber scam victimization risk among Gen Z. The study highlights the importance of strengthening cybersecurity education and digital safety practices among young adults, particularly in areas related to personal data protection, safe online behaviour, and responsible social media management.*

Keywords: *Cyber scam; cyber scam victimization risk; Generation Z; cybersecurity behaviour; data privacy; social media management*

Copyright © Academic Inspired Network - All rights reserved

This work is licensed under CC BY 4.0

Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934

Introduction

In the contemporary global landscape of interconnectedness, cybersecurity emerges as a significant apprehension that resonates throughout every facet of cyberspace (Ramakrishnan et al., 2022). While the digital realm presents numerous advantages to society, it also introduces various concerns. Due to inadequate regulations, the internet is deemed insecure. According to Ramakrishnan et al. (2022), the internet has significantly influenced Malaysia, with 80% of its users engaging in online activities for approximately eight hours daily. It is emphasized that privacy fundamentally revolves around safeguarding personal information from individuals with malicious intentions. According to the report done by Venessa James (2023), the Royal Malaysian Police (PDRM)'s Commercial Crime Investigation Department (JSJK) reported 9,258 instances in 2022 that involved victims who were at least 15 years old and older and were connected to online scam transactions.

Cybercrime stands out as a detrimental consequence of social media usage. So, that's why in the ongoing advancement of information technology and services, cybersecurity holds a crucial position. It represents users' efforts to safeguard both personal and professional data from internet-based attacks, ensuring their integrity and confidentiality (Das & Patel, 2017). This trend is corroborated by the Cybersecurity Malaysia department's projection of a global internet user base reaching 6 billion by 2020. According to the report done by Farhana (2020), in 2020, a total of 10,790 cybersecurity incidents of a general nature were reported. Furthermore, as outlined in the article by (Meikeng, 2020), there was a significant increase in cybersecurity incidents, soaring to 82.5 percent during the implementation of movement control orders (MCO) amidst the COVID-19 pandemic, in contrast to merely 12 percent in April 2019. Presently, with the imposition of MCO, individuals conduct virtually all aspects of their lives online, encompassing business transactions, educational pursuits, entertainment, social interactions, and remote work arrangements. Cybersecurity awareness is important to prevent us from cybercrimes.

In keeping with this seriousness, the researcher is particularly interested in Malaysian university students, who are referred to as the "Z generation" in the community. They're part of the younger generation that considers social media platforms to be necessities. In Malaysia, a significant number of students demonstrated a lack of consideration for computer ethics and security, frequently engaging in illicit activities while browsing the internet. This often involved sharing and downloading pirated software, TV shows, and movies without much thought to the consequences (Ramakrishnan et al., 2022). University students, being intellectually curious, frequently utilize the internet as a tool for their exploratory academic pursuits. The recurrence of these issues prompts the researchers to focus on this subject with Malaysian university students once more. According to Mohebzada et al. (2012), it has been noted that these students are susceptible to online risks. Furthermore, research reveals that students in tertiary institutions share similar demographics such as age, gender, and educational background, suggesting the need for inquiries into how these factors influence their cybersecurity practices.

The human element is also a factor that contributes to the cybersecurity chain. University students exhibit a deficit in emotional maturity and a lack of caution regarding cybersecurity. According to the study by Ramakrishnan et al. (2022), It was said that 92% of students knew the basics of Cybersecurity. However, 84% of them weren't sure about Cybersecurity problems around them, and 95% didn't know how to deal with such issues. Due to the lack of knowledge, a large number of users are more vulnerable to cyber attacks and are unaware of the risks when

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934

sharing their personal information (Das & Patel, 2017). This study wants to find out what makes Gen Z more likely to fall victim to cyber scams by looking at their cyber security habits.

Literature Review

This chapter reviews existing literature to support the study. It presents the framework for the case study, highlighting the primary focus of the research. It has been adopted from secondary sources such as journals, articles and online newspapers. Detailed elaboration is provided on the risk factors of cyber scam victimization and its determinants. The key factors examined in this research include the risk of cyber scam victimization, cybersecurity related behaviors which are data privacy, password management, device and internet usage and social management factors.

Data Privacy

Data privacy is called personal data because it contains identifiable details such as a person's name or address, or because it holds information that could potentially lead to identifying an individual through alternate methods (Di Minin et al., 2021). According to Wijayanto & Prabowo (2020) the users of Android smartphones have also had their levels of data privacy and information security knowledge measured with 71% and 76% of users reporting high levels of privacy awareness, respectively and it measures using three dimensions such as behavior, knowledge, and attitude towards using a smartphone. It is very important for all students to be aware of their role in preventing and lowering cyber threats, whether it is by comprehending phishing emails or sensitive data. These hackers might also profit by giving competitors access to private data on the dark web, which would make cyberspace unsafe and pose serious risks to clients and companies (Alqahtani, 2022). They also give the malevolent attacker the chance to obtain money directly from the victims of the scam or take the victim's personal information (Halevi et al., 2013).

From the research, the respondents who regard their bank account, contact details, and photos as their most private information and most of the contact information is readily available online, individuals yet view their IP address or location as less private than their contact details (Moallem, 2018). The majority of people are unaware of how crucial it is to protect their personal information since it may easily be compromised by viruses. Next, the author evaluated the state of cyber security in the biggest and most significant technology environment since student behavior varies. College students were not aware that their data was not securely transferred between university networks, even when they were aware that their behaviors were being observed and monitored (Alqahtani, 2022). Consequently, educational establishments ought to provide frequent training sessions to impact students' conduct and heighten their comprehension of the fundamentals of cybersecurity and its hazards.

Password Management

Password is an encrypted string of letters or numbers used to verify user identity on computers and other digital platforms. One of the most important things when it comes to data and information security is a password, but it may be dangerous as it can be stolen (Knight-McCord et al., 2016). The security of passwords remains to be one of the primary problems with authentication such as the complexity of passwords and two-factor (Moallem, 2018). From this study, password management among college students appears to still require improvement in terms of adoption and use of better security practices. According to research, most people are aware of the requirements for effective password management and the research has shown that even when people are aware of security dangers, they are still prone to take chances because

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934

they have an overly optimistic outlook and think that bad things will not happen to them (Whitty et al., 2015).

In addition, given the growing number of passwords that users must remember, they either select default, simple passwords or reprocess their potentially strong password, sometimes making small changes or just carrying out preset construction tasks (Alqahtani, 2022). According to one survey, 81% of users kept their current passcodes whenever it was practical for them to do, therefore, 16% switched to one from a previous website, and 4% used passcodes that were essentially brand-new (Bang et al., 2012). Lastly, according to the Wijayanto and Prabowo (2020), the degree of vulnerability, respondents who use passwords for several accounts and store sensitive passwords in web browsers fall into the category of people who are vulnerable to cyberattacks.

Device and Internet Usage

Mobile devices permeate every aspect of daily life, serving purposes at home, for leisure, during study, and in professional settings. They are increasingly recognized as indispensable tools in learning for students. There is a growing diversity of computer hardware encompassing mobile devices, such as smartphones, tablets, netbooks, and laptops (Roberts & Rees, 2014). The rise of social networks and the advancements in mobile technology collectively contribute to an ideal setting for diverse forms of cybercrime and the distribution of illicit online content. Children and teenagers, being the most enthusiastic users of new technologies, are also the most vulnerable due to their relative naivety. Additionally, the overall public lacks adequate awareness of the gravity of this issue (Lapuh Bele et al., 2014).

The Internet is a social networking tool that presents a multidimensional threat spectrum (Ali et al., 2019). Internet browsers are often the portals through which people access the online world. Web browsers are used by people for the majority of their online activity, yet they seldom take control of them. They frequently accept the default settings without realising that they may be altered. Furthermore, an individual internet user can pose the cyber security risk in threat to confidential identity, privacy, and confidentiality (Mai & Tick, 2021). The precise methods used in the scam might differ; for instance, the cybercriminal may occasionally put malware on the victim's device or ask for personal or financial information. Usually, the scam involves the user giving the cybercriminal access to his or her SNS account, either knowingly or unknowingly. The application software then uses this account to spread the malicious application even more, and the cybercriminal may use it to obtain more information about the victim (Kirwan et al., 2018).

Social Media Management

According to López-Carril et al. (2020) social media can be defined as inventive teaching and learning methods that transform communication channels within educational institutions, empowering students to cultivate digital competencies beneficial for a prosperous professional journey of students. Furthermore, social media management involves a methodical and intentional approach to utilizing social media at appropriate locations, times, and in suitable proportions. While using social media is beneficial, it is more advantageous to regulate its usage to conserve time, resources, and energy, fostering a balanced execution of activities (Arop, 2019). Generally, according to Amin et al. (2016) social media worldwide is very popular because of the rapid advancements in technology. Not only celebrities, but also the general populace, have become significant users of these social media platforms.

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934

Other than that, students prefer utilizing social media platforms with the assistance of the internet, where channels like Facebook, Twitter, Instagram, WhatsApp, WeChat, Google Talk, Google+, Skype, and similar platforms are hosted and made available (Arop, 2019). As stated by Azlina et al. (2017), a significant portion of social media users lacks awareness of the significance of their privacy settings. Particularly, students tend to be nonchalant about configuring their social media privacy settings. In 2016, Facebook boasted more than 1.59 billion active users, whereas WhatsApp and Instagram, both owned by Facebook, had 1 billion and 400 million active users, respectively. This unequivocally demonstrates the increasing popularity of social media in contemporary times. It also underscores that the substantial number of social media users not only signifies their influence but also renders them more susceptible to becoming victims of hacking.

Methodology

This section covers the theoretical framework, target population and study design. Additionally, sampling design, research instrument, data collection procedure, and statistical methods employed to examine the contributing factors of cyber scam victimization risk among Gen Z and its contributing factors.

Theoretical Framework

Figure 1 shows the theoretical framework based on the factors that contribute to the factors of cyber security behavior's towards the risk of cyber scam victimization among Gen Z. The dependent variable for this study is the risk of cyber scam victimization while for the independent variables are data privacy, password management, device and internet usage and social management. The framework will be used to formulate the hypothesis for the study.

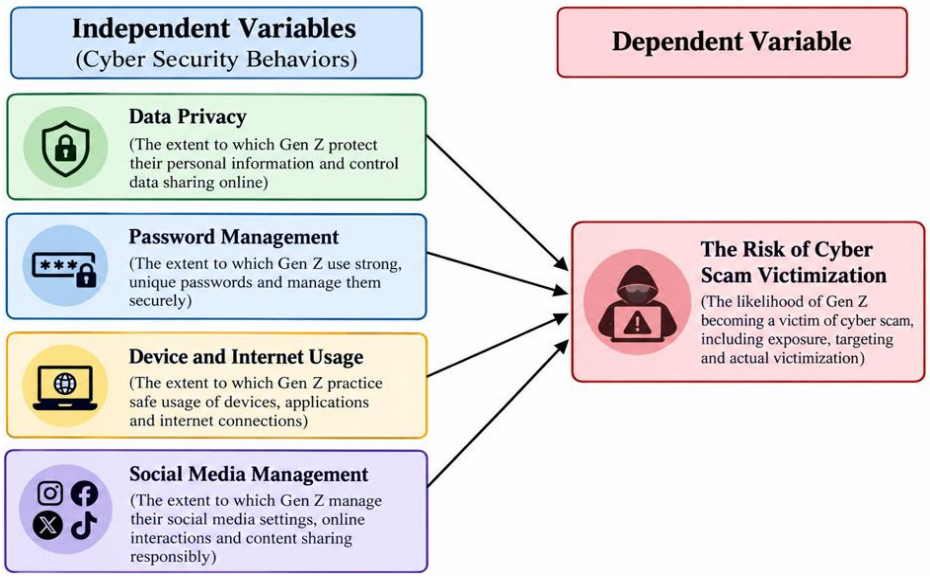


Figure 1: Theoretical Framework

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934

Based on the proposed model, the following hypotheses were formulated:

H11: Data privacy significantly influences the risk of cyber scam victimization among Gen Z.

H12: Password management significantly influences the risk of cyber scam victimization among Gen Z.

H13: Device and internet usage significantly influences the risk of cyber scam victimization among Gen Z.

H14: Social media management significantly influences the risk of cyber scam victimization among Gen Z.

Target Population and Study Design

This study employed a cross-sectional research design involving a target population of 870 full-time undergraduate students enrolled at Universiti Teknologi MARA (UiTM) Kelantan Branch, Kota Bharu Campus, during the March–August 2025 semester. The population comprised students from Semesters 2 to 6 across the Faculty of Business and Management and the College of Computing, Informatics and Mathematics, covering six-degree programmes. Eligible respondents were full-time undergraduate students enrolled in the selected programmes, while part-time students, students undergoing industrial training, postgraduate students, graduates, and students enrolled in non-degree programmes were excluded. The official student list obtained from the Academic Affairs Department (HEA) served as the sampling frame. Data were collected once using a structured questionnaire to examine the relationships between four cybersecurity behaviors—data privacy, password management, device and internet usage, and social media management—and the risk of cyber scam victimization. The questionnaire also captured respondents' demographic characteristics, while the study variables were measured using a 10-point Likert scale ranging from 1 (strongly disagree) to 10 (strongly agree).

Sampling Design and Sample Size Determination

A proportionate stratified random sampling technique was employed to select respondents from the target population of 870 full-time undergraduate students at UiTM Kelantan Branch, Kota Bharu Campus. The population was stratified by gender to ensure representation of both male and female students, and respondents were randomly selected from each stratum using the official student list obtained from the Academic Affairs Department (HEA) as the sampling frame. Following the data collection and screening process, 231 complete and usable responses were retained for the final analysis, representing approximately 26.6% of the target population. The final sample comprised 68 male (29.44%) and 163 female (70.56%) respondents. These 231 valid responses constituted the final analytical sample used for the descriptive, reliability, and multiple linear regression analyses reported in this study. Accordingly, a sample size of 231 respondents was deemed adequate for the present survey, as it met the calculated minimum sample size requirement and was considered sufficient to support reliable statistical analysis, consistent with the findings of Azizan et al. (2020).

Research Instrument and Data Collection

Data were collected using a structured questionnaire comprising six sections, as presented in Table 1. Section A consisted of five items on respondents' demographic profiles. Section B measured cyber scam victimization risk using seven items adapted from Ishak et al. (2012) and Muniandy et al. (2017). Section C measured data privacy using five items adapted from Wijayanto and Prabowo (2020) and Muniandy et al. (2017). Section D assessed password management using five items adapted from Wijayanto and Prabowo (2020) and Muniandy et al. (2017), while Section E measured device and internet usage using five items adapted from

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934

the same sources. Finally, Section F measured social media management using five items adapted from Chandarman and Van Niekerk (2017) and Ishak et al. (2012). All items measuring the study constructs were assessed using a 10-point Likert scale ranging from 1 (Strongly Disagree) to 10 (Strongly Agree).

Table 1: Summary of the Number of Items for each Section

Section	Questions	Type of Scale	No. of Items	Sources
A	**Demographic profile**	All variables are categorical	5	None
B	**Risky Cyber Scam Victimization**	A ten-point Likert scale from (1) "Strongly Disagree" to (10) "Strongly Agree"	5	Adapted from: Ishak et al. (2012) Muniandy et al. (2017)
C	**Data Privacy**		5	Adapted from : Wijayanto and Prabowo (2020) Muniandy et al. (2017)
D	**Password Management**		5	Adapted from: Wijayanto and Prabowo (2020) Muniandy et al. (2017)
E	**Device and Internet Usage**		5	Adapted from : Wijayanto and Prabowo (2020) Muniandy et al. (2017)
F	**Social Media Management**		5	Adapted from : Chandarman and Van Niekerk (2017) Ishak et al. (2012)

Method of Data Analysis

The collected data were analysed using descriptive and inferential statistical methods to examine cyber scam victimization risk among Gen Z and its determinants. The analysis comprised descriptive analysis, reliability analysis, Pearson correlation analysis, and multiple linear regression analysis. Descriptive analysis was used to summarise the respondents' demographic characteristics and the study variables, while Cronbach's alpha was employed to assess the internal consistency of the measurement items. Pearson correlation analysis was subsequently conducted to examine the relationships between the four cybersecurity behaviors, which are data privacy, password management, device and internet usage, and social media management, and cyber scam victimization risk. Finally, multiple linear regression analysis was performed to determine the simultaneous and individual effects of the four cybersecurity behaviors on cyber scam victimization risk and to test the hypotheses formulated in the theoretical framework.

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under CC BY 4.0

Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934

Descriptive Analysis

Descriptive analysis was conducted to summarise the characteristics of the respondents and provide an overall description of the study variables. Frequencies and percentages were used to describe the respondents' categorical demographic characteristics. This analysis provided an initial overview of the respondents prior to conducting the inferential analyses.

Reliability Analysis

Reliability analysis was conducted to assess the internal consistency of the measurement items representing the five constructs in the study. Cronbach's alpha coefficients were calculated separately for data privacy, password management, device and internet usage, social media management, and cyber scam victimization risk. A higher Cronbach's alpha coefficient indicates greater consistency among the items measuring the same construct. The reliability assessment was conducted prior to the inferential analyses to ensure that the items used to measure each construct demonstrated satisfactory internal consistency.

Multiple Linear Regression Analysis

Multiple linear regression analysis was employed to examine the simultaneous effects of data privacy, password management, device and internet usage, and social media management on cyber scam victimization risk among Gen Z. Cyber scam victimization risk served as the dependent variable, while the four cybersecurity behaviors were entered simultaneously as the independent variables. The multiple linear regression model was specified as:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \varepsilon$$

where:

Y = Cyber Scam Victimization Risk
X_1 = Data Privacy
X_2 = Password Management
X_3 = Device and Internet Usage
X_4 = Social Media Management
β_0 = Intercept
$\beta_1, \beta_2, \beta_3, \beta_4$ = Regression coefficients
ε = Error term

The coefficient of determination (R^2) and adjusted R^2were used to determine the proportion of variation in cyber scam victimization risk collectively explained by the four cybersecurity behaviors. The overall F-test was used to assess whether the regression model was statistically significant, while individual t-tests were used to determine whether each independent variable significantly contributed to the prediction of cyber scam victimization risk at the 5% significance level ($\alpha = 0.05$). Accordingly, the regression coefficients for data privacy, password management, device and internet usage, and social media management were used to test H11, H12, H13, and H14, respectively.

Prior to interpreting the regression results, the assumptions underlying multiple linear regression were assessed to establish the adequacy of the fitted model. Linearity was examined through the relationships between the independent variables and cyber scam victimization risk, while normality of residuals was assessed using appropriate graphical diagnostics. Homoscedasticity was evaluated using a scatterplot of standardised residuals against standardised predicted values. Multicollinearity among data privacy, password management,

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934

device and internet usage, and social media management was assessed using tolerance and variance inflation factor (VIF) statistics. These diagnostic procedures were conducted before interpreting the regression coefficients to ensure that the assumptions of the multiple linear regression model were adequately satisfied.

Findings

Descriptive Analysis

A total of 231 respondents were included in the study. As presented in Table 2, the majority of the respondents were female (70.56%), while 29.44% were male. In terms of age, the largest proportion of respondents were aged 21–23 years (48.48%), followed by those aged 18–20 years (29.00%) and 24–26 years (22.51%). The respondents represented all six academic programmes included in the study. The largest proportion was from BA250/BA280 (25.11%), followed by CS241/CDCS241 (24.24%), BA249/BA279 (21.21%), BA242/BA272 (17.32%), CS291/CDCS291 (6.93%), and BA240/BA270 (5.19%). With respect to semester of study, Semester 4 recorded the highest proportion of respondents (29.00%), followed by Semester 3 (27.71%), Semester 2 (24.24%), Semester 5 (10.82%), and Semester 6 (8.23%). Overall, the demographic profile indicates that the sample was predominantly female and aged between 21 and 23 years, with representation across all six academic programmes and Semesters 2 to 6.

Table 2: Demographic Profile

Variable	n	%
Gender		
Male	68	29
Female	163	71
Age		
18-20 years old	67	29
21-23 years old	112	48
24-26 years old	52	23
Course		
BA240/BA270	12	5
BA242/BA272	40	17
BA249/BA279	49	26
BA250/BA280	58	25
CS241/CDCS241	56	24
CS291/CDCS291	16	6.93
Semester		
2	56	20
3	64	25
4	67	30
5	25	15
6	19	10

Reliability Analysis

Table 3 presents the results of the reliability analysis for the five constructs examined in this study. The Cronbach's alpha coefficients ranged from 0.651 to 0.895, indicating varying levels of internal consistency across the measurement scales. Device and internet usage recorded the highest Cronbach's alpha coefficient ($\alpha = 0.895$), closely followed by data privacy ($\alpha = 0.894$). Social media management also demonstrated good internal consistency with a Cronbach's

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934

alpha coefficient of 0.804, while password management recorded a coefficient of 0.763. The risk of cyber scam victimization recorded the lowest Cronbach's alpha coefficient ($\alpha = 0.651$). Although this value was lower than those obtained for the other constructs, it indicated a moderate level of internal consistency. Overall, the reliability results showed that the cybersecurity behaviour constructs demonstrated satisfactory internal consistency and were considered sufficiently reliable for subsequent statistical analysis.

Table 3: Summary of Reliability Analysis for each Construct

Construct	Number of Items	Cronbach's Alpha Coefficient
The Risk of Cyber Scam Victimization	5	0.651
Data Privacy	5	0.894
Password Management	5	0.763
Device and Internet Usage	5	0.895
Social Media Management	5	0.804

Stepwise Multiple Linear Regression Analysis

Multiple linear regression analysis was conducted to determine whether data privacy, password management, device and internet usage, and social media management significantly influenced the risk of cyber scam victimization among Gen Z. Cyber scam victimization risk was treated as the dependent variable, while the four cybersecurity behaviours were entered as independent variables. This analysis was consistent with the hypotheses proposed in the theoretical framework.

As presented in Table 4, the multiple linear regression model produced an R^2 of 0.319 and an adjusted R^2 of 0.307. This indicates that approximately 31.9% of the variation in cyber scam victimization risk among Gen Z was collectively explained by data privacy, password management, device and internet usage, and social media management. The remaining 68.1% of the variation in cyber scam victimization risk may be attributable to other factors that were not included in the present regression model. The relatively small difference between R^2 and adjusted R^2 also indicates that the explanatory ability of the model remained relatively stable after adjustment for the number of predictors included.

Table 4: Goodness of Fit

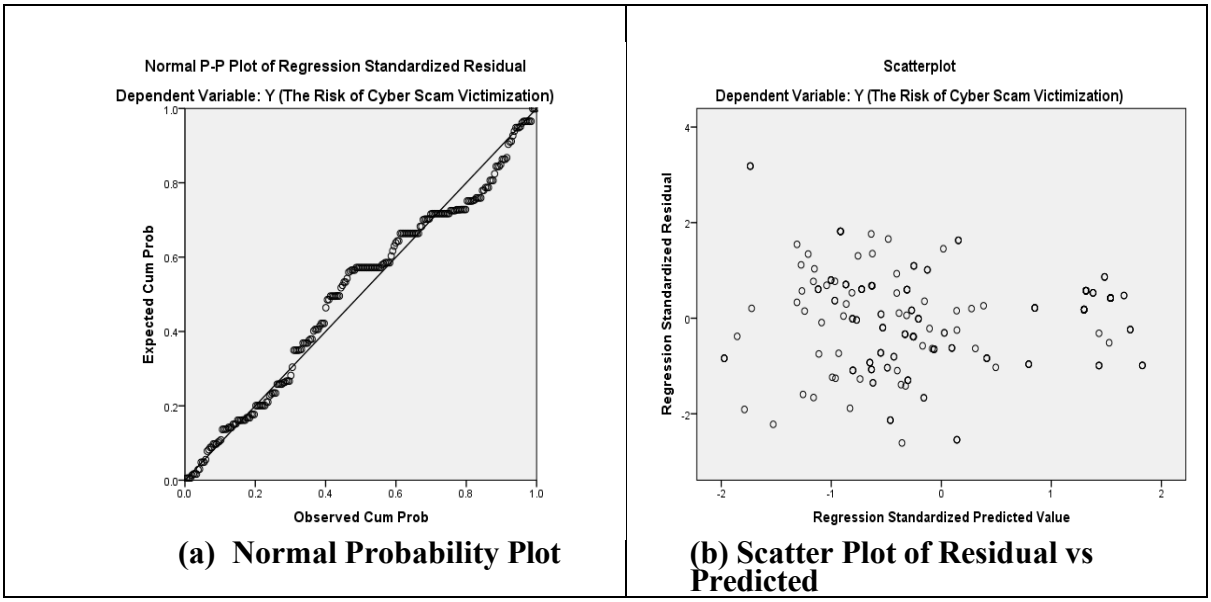
R-Square	Adjusted R-Square
0.319	0.307

Prior to interpreting the regression coefficients, the assumptions underlying multiple linear regression were assessed. Figure 2(a) presents the normal probability plot, while Figure 2(b) presents the scatterplot of residuals against predicted values. Based on the normal probability plot, the standardised residuals were distributed approximately along the diagonal reference line, indicating that the normality assumption was reasonably satisfied. In addition, the scatterplot of standardised residuals against standardised predicted values did not display a clear systematic pattern, suggesting that the homoscedasticity assumption was adequately met.

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934



(a) Normal Probability Plot **(b) Scatter Plot of Residual vs Predicted**

Figure 2: Normality and Homoscedasticity Assumptions

Multicollinearity was further assessed using the tolerance and variance inflation factor (VIF) values. As presented in Table 5, the tolerance values ranged from 0.449 to 0.588, while the VIF values ranged from 1.702 to 2.225. Specifically, the VIF values were 2.149 for data privacy, 1.711 for password management, 2.225 for device and internet usage, and 1.702 for social media management. These values indicate that serious multicollinearity was not evident among the four independent variables, supporting the suitability of including the predictors simultaneously in the regression model.

Table 5: Multicollinearity Assumption

Construct	Tolerance	VIF
Data Privacy	0.465	2.149
Password Management	0.584	1.711
Device and Internet Usage	0.449	2.225
Social Media Management	0.588	1.702

The ANOVA results showed that the overall multiple linear regression model was statistically significant, $F(4, 226) = 26.440$, $p < 0.001$. This indicates that data privacy, password management, device and internet usage, and social media management, when considered collectively, significantly explained variation in the risk of cyber scam victimization among Gen Z. Therefore, the regression model was statistically significant and appropriate for examining the individual contributions of the four cybersecurity behaviour variables to cyber scam victimization risk.

Table 6: Test for Significance of Regression Model

Model	Sum of Square	df	Mean Square	F Statistics	Sig.
Regression	5808.156	4	1452.039	26.440	$.000^b$
Residual	12411.411	226	54.918		
Total	18219.567	230			

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under CC BY 4.0

Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934

The regression coefficient results indicate that the cybersecurity behaviour variables differed in their individual contributions to cyber scam victimization risk. Data privacy had a negative and statistically significant influence on cyber scam victimization risk (B = −0.180, t = −3.078, p = 0.002). Holding the other predictors constant, a one-unit increase in data privacy was associated with an estimated 0.180-unit decrease in cyber scam victimization risk. Therefore, the findings provide support for H_{11}, indicating that data privacy significantly influences the risk of cyber scam victimization among Gen Z.

Password management, however, did not have a statistically significant influence on cyber scam victimization risk (B = −0.050, t = −0.837, p = 0.404). Although the coefficient was negative, the relationship was not statistically significant at the 5% significance level. Therefore, H_{12} was not supported. This indicates that password management did not make a statistically significant unique contribution to cyber scam victimization risk after the effects of the other cybersecurity behaviours were taken into account. Device and internet usage had a negative and statistically significant influence on cyber scam victimization risk (B = −0.162, t = −2.896, p = 0.004). Holding the other predictors constant, a one-unit increase in safer device and internet usage behaviour was associated with an estimated 0.162-unit decrease in cyber scam victimization risk. Therefore, H_{13} was supported. According to the results, social media management also significantly influenced cyber scam victimization risk, and therefore H_{14} was supported. Thus, three of the four hypotheses were supported. Data privacy, device and internet usage, and social media management significantly influenced cyber scam victimization risk among Gen Z, whereas password management did not demonstrate a statistically significant unique influence when the effects of the other predictors were considered simultaneously.

Table 7: Test for Significance of Individual Predictor Variable

Variable	Coefficient Value	t-Statistics	Sig.
Constant	-18.939	-10.295	0.000
Data Privacy	-0.180	-3.078	0.002
Password Management	-0.050	-0.837	0.404
Device and Internet Usage	-0.162	-2.896	0.004
Social Media Management	-0.192	-3.164	0.002

Table 8: Summary of Hypotheses and Results

Hypothesis	Result
H_{11}: Data privacy significantly affect the risks of cyber scam victimization	Supported
H_{12}: Password management not significantly affect the risks of cyber scam victimization	Not Supported
H13: Device and internet usage significantly affect the risks of cyber scam victimization	Supported
H_{14}: Social Media Management significantly affect the risks of cyber scam victimization	Supported

Based on the estimated regression coefficients, the final multiple linear regression model can be expressed as:

$$\hat{Y} = -18.939 - 0.180X_1 - 0.050X_2 - 0.162X_3 - 0.192X_4$$

where $\hat{Y}$represents the predicted level of cyber scam victimization risk among Gen Z, X_1represents data privacy, X_2represents password management, X_3represents device and

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934

internet usage, and X_4represents social media management. The negative regression coefficients indicate that higher levels of data privacy, password management, device and internet usage, and social media management were associated with lower predicted levels of cyber scam victimization risk. However, password management was not statistically significant ($p = 0.404$), indicating that it did not make a statistically significant unique contribution to predicting cyber scam victimization risk after the effects of the other predictors were taken into account. In contrast, data privacy, device and internet usage, and social media management were statistically significant predictors of cyber scam victimization risk.

Conclusion

This study examined the determinants of cyber scam victimization risk among Gen Z, focusing on four cybersecurity behaviours: data privacy, password management, device and internet usage, and social media management. The findings demonstrated that these factors collectively contributed significantly to explaining variations in cyber scam victimization risk. The multiple linear regression model explained 31.9% of the variation in cyber scam victimization risk, indicating that cybersecurity behaviours play an important role in understanding vulnerability to cyber scams among Gen Z.

At the individual predictor level, data privacy, device and internet usage, and social media management were found to be statistically significant predictors of cyber scam victimization risk. All three variables exhibited negative regression coefficients, indicating that better practices in protecting personal data, using devices and the internet safely, and managing social media responsibly were associated with lower levels of cyber scam victimization risk. Among these predictors, social media management recorded a coefficient of −0.192, followed by data privacy (−0.180) and device and internet usage (−0.162). In contrast, password management was not statistically significant, suggesting that it did not provide a significant unique contribution to predicting cyber scam victimization risk when the other cybersecurity behaviours were considered simultaneously.

The findings highlight the importance of strengthening cybersecurity practices among Gen Z, particularly in relation to personal data protection, safe device and internet usage, and responsible social media management. Cybersecurity awareness and educational initiatives for young adults should therefore extend beyond password-related practices and place greater emphasis on how personal information is shared, how digital devices and online connections are used, and how interactions and privacy are managed on social media platforms. Such efforts may contribute to reducing behaviours associated with vulnerability to cyber scams.

This study provides empirical evidence on cybersecurity behaviours associated with cyber scam victimization risk among undergraduate students at UiTM Kelantan Branch, Kota Bharu Campus. Nevertheless, the findings should be interpreted within the context of the study, as the sample was limited to 231 undergraduate students from a single university campus and the study employed a cross-sectional design. Future research could extend the investigation to Gen Z populations from different universities, geographical locations, educational backgrounds, and employment groups. Additional individual, psychological, technological, and situational factors could also be examined to provide a more comprehensive understanding of cyber scam victimization risk among Gen Z.

Overall, the findings suggest that safer cybersecurity behaviours are associated with lower cyber scam victimization risk among Gen Z, particularly in the areas of data privacy, device

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934

and internet usage, and social media management. Strengthening these practices may therefore be an important component of efforts to enhance digital safety and reduce vulnerability to cyber scams among young adults.

Acknowledgements
The authors would like to express their sincere appreciation to all respondents who participated in this study and provided valuable information for the research. The authors also gratefully acknowledge Universiti Teknologi MARA (UiTM), particularly UiTM Kelantan Branch, for the institutional support provided throughout the completion of this study.

Conflict of Interest Statement
The authors declare that there are no conflicts of interest regarding the research, authorship, or publication of this manuscript.

AI Usage Declaration
Generative artificial intelligence (AI) tools were used during the preparation of this manuscript solely to assist in generating the visual representation of the theoretical framework and improving sentence structure, grammar, and overall language clarity. AI was not used to generate, manipulate, or fabricate the research data or statistical results. All data used in this study were collected by the researchers, and all statistical analyses, findings, interpretations, and conclusions were derived from the actual research data. The authors reviewed and verified all AI-assisted content and take full responsibility for the accuracy, integrity, and final content of the manuscript.

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934

References

Ali, A., Kamran, A., Ahmed, M., Raza, B., & Ilyas, M. (2019). Privacy Concerns in Online Social Networks: A Users' Perspective. *International Journal of Advanced Computer Science and Applications*, *10*(7). https://doi.org/10.14569/ijacsa.2019.0100780

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

Amin, Z., Mansoor, A., Rabeet, S., And, H., & Hashmat, F. (2016). Impact of Social Media of Student's Academic Performance. *International Journal of Business and Management Invention ISSN*, *5*(4), 22–29. https://www.ijbmi.org/papers/Vol(5)4/version-2/D050402022029.pdf

Arop, F. O. (2019). *Tertiary students' social media management attitudes and academic performance in Cross River State*. https://philpapers.org/rec/AROTSS-2

Azizan, N. H., Mahmud, Z., & Rambli, A. (2020). Rasch rating scale item estimates using maximum likelihood approach: Effects of sample size on the accuracy and bias of the estimates. International Journal of Advanced Science and Technology, 29(4s), 2526–2531.

Azlina, N., Rahman, A., Permatasari, F., & Hafsari, Y. (2017). A Review on Social Media Issues and Security Awareness among the users. *Journal of Applied Technology and Innovation*, *1*(1), 28–36. https://jati.sites.apiit.edu.my/files/2018/07/2017_Issue1_Paper3.pdf

Bang, Y., Lee, D.-J., Bae, Y.-S., & Ahn, J.-H. (2012). Improving information security management: An analysis of ID–password usage and a new login vulnerability measure. International Journal of Information Management, 32(5), 409–418. https://doi.org/10.1016/j.ijinfomgt.2012.01.001

Chandarman, R., & Van Niekerk, B. (2017). Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. *The African Journal of Information and Communication*, *20*(20), 133–155. https://doi.org/10.23962/10539/23572

Das, R., & Patel, M. (2017). Cyber Security for Social Networking Sites: Issues, Challenges and Solutions. *International Journal for Research in Applied Science and Engineering Technology*, *V*(IV), 833–838. https://doi.org/10.22214/ijraset.2017.4153

Di Minin, E., Fink, C., Hausmann, A., Kremer, J., & Kulkarni, R. (2021). How to address data privacy concerns when using social media data in conservation science. *Conservation Biology*, *35*(2), 437–446.

Farhana, S. (2020, Oct). Retrieved from https://www.astroawani.com/berita -malaysia/rise-cybercrime malaysian-what-you-need-avoid-264890

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. Proceedings of the 22nd International Conference on World Wide Web - WWW '13 Companion. https://doi.org/10.1145/2487788.2488034

Ishak, I., Sidi, F., Jabar, M., Fazlida, N., Sani, M., Mustapha, A., Siti, R., & Supian. (2012). A Survey on Security Awareness among Social Networking Users in Malaysia. *Australian Journal of Basic and Applied Sciences*, *6*(12), 23–29. https://www.ajbasweb.com/old/ajbas/2012/Nov%202012/23-29.pdf

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

Knight-McCord, J., Cleary, D., Grant, N., Herron, A., Jumbo, S., Lacey, T., Livingston, T., Robinson, S., Smith, R., & Emanuel, R. (2016). What social media sites do college students use most? Journal of Undergraduate Ethnic Minority Psychology, 2(2016). https://juempsychology.com/wp-content/uploads/2022/08/Knight-McCord_et-al_JUEMP_2016.pdf

Copyright © Academic Inspired Network - All rights reserved

This work is licensed under CC BY 4.0

Volume: 11 Issues: 69 Special Issue [October, 2026] pp. 440-455
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116934

Lapuh Bele, J., Dimc, M., Rozman, D., & Sladoje, A. (2014). *RAISING AWARENESS OF CYBERCRIME -THE USE OF EDUCATION AS A MEANS OF PREVENTION AND PROTECTION*. https://files.eric.ed.gov/fulltext/ED557216.pdf

López-Carril, S., Anagnostopoulos, C., & Parganas, P. (2020). Social media in sport management education: Introducing LinkedIn. *Journal of Hospitality, Leisure, Sport & Tourism Education*, *27*, 100262. https://doi.org/10.1016/j.jhlste.2020.100262

Mai, P. T., & Tick, A. (2021). Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam. Acta Polytechnica Hungarica, 18(8), 67–89. https://doi.org/10.12700/aph.18.8.2021.8.4

Meikeng, Y. (2020, Apr). Cybersecurity cases rise by 82.5 percent. Retrieved from https://www.thestar.com.my/news/focus/2020/04/12/cybersecurity -cases-rise-by-825

Moallem, A. (2018). Cyber Security Awareness Among College Students. Advances in Intelligent Systems and Computing, 79–87. https://doi.org/10.1007/978-3-319-94782-2_8

Mohebzada, J. G., Zarka, A. E., Bhojani, A. H., & Darwish, A. (2012). Phishing in a university community: Two large scale phishing experiments. *2012 International Conference on Innovations in Information Technology (IIT)*. https://doi.org/10.1109/innovations.2012.6207742

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber Security Behaviour among Higher Education Students in Malaysia. Journal of Information Assurance & Cybersecurity, 1–13. https://doi.org/10.5171/2017.800299

Ramakrishnan, K., Norizan Mohd Yasin, & Jeyarani Periasamy. (2022). Digital divide on cybersecurity awareness among the Malaysian higher learning institution students. *Nucleation and Atmospheric Aerosols*. https://doi.org/10.1063/5.0092796

Roberts, N., & Rees, M. (2014). Student use of mobile devices in university lectures. *Australasian Journal of Educational Technology*, *30*(4). https://doi.org/10.14742/ajet.589

Venessa James. (2023, June 9). - *Who Is To Blame For Online Fraud?* Retrieved form https://www.bernama.com/en/bfokus/news.php?current&id=2196476

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. Cyberpsychology, Behavior, and Social Networking, 18(1), 3–7. https://doi.org/10.1089/cyber.2014.0179

Wijayanto, H., & Prabowo, I. A. (2020). Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. Jurnal Sisfokom (Sistem Informasi Dan Komputer), 9(3), 395–399. https://doi.org/10.32736/sisfokom.v9i3.1021

Copyright © Academic Inspired Network - All rights reserved

This work is licensed under CC BY 4.0