Cawangan Terengganu

Available online at
http://journale-academiauitmt.uitm.edu.my

e-Academia Journal

e-Academia Journal of UiTM Cawangan Terengganu 11 (1) 1-13, May 2022

Awareness of Cybersecurity: A Case Study in UiTM Negeri Sembilan Branch, Seremban Campus

Adlina Kamalulail [1], Nur Ezzatul Nadia Abdul Razak [1], Siti Aisyhah Omar [1] &
***Noreha Mohamed Yusof[1]**

[1]Center of Statistical and Decision Science Studies,
Faculty of Computer and Mathematical Sciences,
Universiti Teknologi MARA Cawangan Negeri Sembilan,
Persiaran Seremban Tiga/1, Seremban 3, 70300 Seremban,
Negeri Sembilan,Malaysia.

*Corresponding author's email: noreh144@uitm.edu.my

Submission date: 24 February 2022 Accepted date: 28 April 2022 Published date: 30 May 2022

ABSTRACT

Cybersecurity is a problem that is rarely discussed by the public, especially among university students in Malaysia. This study aims to determine the significant differences of cybersecurity awareness between genders and to investigate the significant predictors of the cybersecurity awareness. This study adopts a cross-sectional methodology among UiTM Negeri Sembilan, Seremban Campus students (n=201, 19 to 25 years old) using a questionnaire. The results show that male and female students have the same level of cybersecurity awareness. Meanwhile, gender, age, marital status, faculty, type of social media used, hours spent on social media, attitude and environmental factors do not in any way affect the awareness of cybersecurity among students. The results further show that it is only the knowledge factors that differentiate cybersecurity awareness among them.

Keywords: *Cybersecurity; Cybersecurity Awareness; Social Media; Multiple Linear Regression*

1.0 INTRODUCTION

Social media allows the sharing of opinions, thoughts, and information via the building of virtual networks and the variation of platforms as defined by Dollarhide (2021). According to Fumudoh and Viswanathan (2014), with the information that is now publicly available on the internet, the issue of privacy has always been debated. They also mentioned that it is important to know that privacy relates to keeping personal information private and away from someone who has malicious intent.

One of the negative impacts of social media is cybercrime. Cybercrime was defined by Das and Patel (2017) as crimes committed on the internet that involve the use of a computer as either a weapon or a targeted victim. Computers could be used to commit a crime or it could be the target and cybercrimes can jeopardise a person's security and financial well-being. Cybersecurity awareness is important to prevent us from cybercrimes.

Hence, this study intends to discover the awareness of cybersecurity among students in UiTM Negeri Sembilan Branch, Seremban Campus. Cybersecurity preserves and enables many of the modern services. The phrase cyber, and cybersecurity are frequently mentioned in the news, especially when something bad occurs. In fact, according to Al-Mohannadi et al. (2018), since awareness is very important, the researchers suggested that all organisation take the necessary steps to build knowledge and awareness about cybersecurity among their employees.

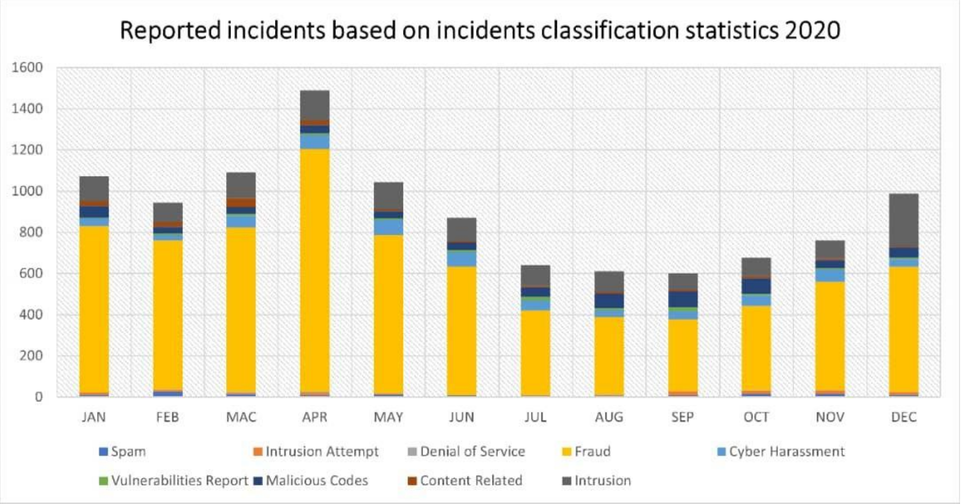

Figure 1: Reported Incidents based on General Incident Classification Statistics in Malaysia

Based on the data from Malaysia Computer Emergency Response Team (MyCERT), 2020, Figure 1 shows the reported cases in Malaysia, most of which are examples of cybersecurity incidents such as malicious codes, intrusion attempt, intrusion, denial of services, fraud and more. It is interesting to note that fraud incidents showed the crime most reported for every month in 2020. Scams, phishing, and social engineering tactics to deceive victims and obtain sensitive information are examples of online fraud cases. Figure 1 also shows that intrusion incidents are the second leading crime after fraud incidents throughout the year 2020. In contrast, vulnerabilities incidents are the least reported throughout the year 2020. Besides, fraud incidents increased from January to April and started decreasing from May to September before increasing again gradually from October to December.

This study applies to the students in UiTM Negeri Sembilan Branch, Seremban Campus that focuses on all faculties which are Faculty of Computer and Mathematical Sciences (FSKM), Faculty of Administrative Science and Policy Studies (FSPPP) and Faculty of Sports Science and Recreation (FSR). The total students who registered in October 2020 at UiTM Negeri Sembilan Branch, Seremban Campus is 5846 students.

1.2 PROBLEM STATEMENT

According to the report done by Farhana (2020), there were 10,790 general cybersecurity incidents reported in 2020. Additionally, based on the article by (Meikeng, 2020), cybersecurity cases rose to 82.5 percent during movement control order (MCO) due to COVID-19 pandemic compared to 12 percent in April 2019. Nowadays, people do everything online such as business, education, entertainment, socializing or working from home due to MCO.

There are some negative effects due to the lack of awareness about cybersecurity that occurs from the use of technology. First, internet users will be easily influenced by others. This is because they have no experience on the issue of fraud in cyberspace which can lead to the problem of losing large amounts of money. According to an article by Meikeng (2020), most cases during the MCO involved fraud, intrusion and cyber harassment. This is due to the increased usage of technologies during MCO.

If internet users lack the awareness of cybersecurity, they will be easily influenced by hackers, scammers or cyber-criminal. The findings by Fatokun et al. (2019) stated that male students had a higher score in their security awareness compared to female students. This could imply that with regards to this study, male students are surer of their awareness of cybersecurity as compared to their female counterparts. However, this result is not enough to make conclusions on this issue, as it might be that the male students in this study may have answered the survey due to overconfidence. Nevertheless, the researcher can say that differences exist between the female and male students with regards to their awareness of cybersecurity. Therefore, this study try to examine which gender has better awareness of cybersecurity while using social media.

Next, the effect due to the lack of awareness of cybersecurity is the probability to get involved in cybercrime is higher. Based on an article by Farhana (2020), from January to September 2020, there have already been 8,366 reported incidents of cybercrimes. Social media is a significant medium that increases the score of involvement in cybercrime activities rates. Cyber-criminals tend to take advantage of new technologies and remote working platforms due to the COVID-19 pandemic. Therefore, this study attempts to prevent more negative effect from occurring among students especially those in UiTM Negeri Sembilan Branch, Seremban Campus due to the lack of awareness of cybersecurity. This study also aims to helpreduce cybercrime rates in Malaysia.

1.3 RESEARCH OBJECTIVES

Based on the research problems, the objectives of this study are to determine the significance difference of cybersecurity awareness between genders and to investigate the significant predictors of the cybersecurity awareness.

1.4 RESEARCH HYPOTHESES

H_1: There awareness of cybersecurity score is different between male and female students while using social media platforms.

H_2: Social media information gives impact to the awareness of cybersecurity.

H_3: The attitude of internet users gives impact to the awareness of cybersecurity.

H_4: The internet users' experience gives impact to the awareness of cybersecurity.

H_5: The involvement in the social environment of cybersecurity gives impact to the awareness of cybersecurity.

2.0 LITERATURE REVIEW

This section will discuss the previous research that have been conducted on the awareness of cybersecurity. It will discuss the predictors of the study such as demographic profile, social media information, attitude factor, knowledge factor, and environmental factor.

2.1 DEMOGRAPHIC PROFILE

In this research, four criteria of demographic profiles are examined which are gender, age, marital status and faculty. Garba et al. (2020) identified females as more likely to become victims of a cybersecurity attack in Nigeria. A total of 201 respondents participated in the study, and the result indicates that males are more into learning or responding to cybersecurity awareness surveys than female students. From this result, the female students are predicted to become the victims of basic cyber-attacks.

A study done by Anwar et al. (2017) with the objective to explore the function of gender in perspective and faith in cybersecurity showed that there are significant differences between genders. This research showed that women are more likely to be victims of cybersecurity because men tend to report about their own cybersecurity experience more than women. Apart from that, the self-efficacy of women is lower than men. Next, in another study conducted by Fatokun et al. (2019), the impact of age was also studied. The results reveal that cybersecurity habits differ from age to age based on many factors. The results also show that senior students are less vulnerable to cyber threats than junior students. This also can be supported by Ogutcu et al. (2016) who found that students in lower age groups are more susceptible to cyber-attacks in higher institutions.

Furthermore, a study by Shaari et al. (2019) said that scammers usually look for unguarded, gullible and lonely people who are looking for companions or relationships as their victims. They take advantage from gathering information about the victims such as her status as a single mother on her social media platform. In addition, they continue their fraud until it results in instant relationship, psychological or emotional acceptance and trust, especially among lonely or single victims. Marital or relationship status can also be identified as one of the factors someone can become a potential victim of cybersecurity or cybercrime.

2.2 SOCIAL MEDIA INFORMATION

Muniandy et al. (2017) conducted a study aimed at examining whether higher education students in Malaysia use the internet regularly. Based on the results, they are convinced that higher education students are undoubtedly hardcore Internet users. This can be proven when an email has at least been used as a medium communication by almost all students who participated in the study. In addition, these students are also dedicated social site users such as online banking which has been used by almost half of the respondents. Furthermore, more than half of the respondents who were involved in the study shop online and download online games. The study has also expressed the opinion that higher education students use the Internet for a variety of reasons.

2.3 ATTITUDE FACTOR

In this era of globalization, there are many social media users from various walks of life and age. For sure there are many attitudes that can be seen from day to day. The internet users must be responsible users. They should be knowledgeable and careful with anything that comes to them because not all of the information can be believed. Besides, Zhang and Gupta (2018) mentioned that security and trustworthiness issues have become increasingly serious, which need to be addressed urgently. A negative attitude towards cybersecurity in business is positively related to dangerous cybersecurity practices as mentioned in a study by Hadlington (2017).

Smitherson (2012) said that the willingness to share personal information with others should only be for someone who can be trusted and to check and ensure that any information that has been shared by others is verified. People nowadays hide their identity by creating fake accounts so that they can get others' attention towards their contents as mentioned by Bhatnagar and Pry (2020).

To achieve effective growth, the information security awareness should be as prioritized, which was also mentioned by other researchers such as Marks and Rezgui (2009) and Talib et al. (2010). Some challenges might involve human attitude, which is hard to measure because other aspects like culture, motivation, values and mentality can influence it. Kruger and Kearney (2006) also mentioned that the attitudes of staff and students have been acknowledged as a key factor in protecting organizational information.

The result of a previous study by Hadlington (2018) found a correlation between attitudes towards cyber security and risky cyber security behaviours as significantly negative, with more negative attitudes being connected to higher levels of risky behaviours. Furthermore, a study from Saizan and Singh (2018) indicated that most of the respondents still have a moderate level of awareness of cybersecurity.

2.4 KNOWLEDGE FACTOR

As social media users, it is important to have the knowledge and ability to control their social media as stated by Saizan and Singh (2018). Based on the previous study from Bada et al. (2019), they suggested that interventions based on major theoretical knowledge is required to change the behaviour of the social media users. In order to change one's behaviour, knowledge and awareness are very important but not necessarily enough. Due to the lack of knowledge, many users are more vulnerable to cyber-attacks and are unaware of the risks when sharing their personal information (Das & Patel, 2017).

Based on the results of the previous study from Cain et al. (2018), differences in cyber knowledge do not exist among different age groups but men have more knowledge about cyber than women. In addition, the older age group, usually perceived as those who do not understand technology is in fact not weak, but they are the group that is most vulnerable to cyber-attacks. Researchers have also mentioned that someone who describes themselves as a cybersecurity expert will be safer and have more knowledge about cybersecurity hygiene than other users but instead their assumptions are wrong because they are reported to be less secure and less aware of cybersecurity hygiene than other respondents.

Moreover, Kovacevic et al. (2020) found that knowledge proves to be a dominant factor for cyber security awareness. This is because, even though students are digital natives, they do not feel safe in the cyber world and do not have enough knowledge to protect themselves in cyberspace. The study from Kovacevic et al. (2020) showed that this finding can be a signal to educational institutions to take a more active approach to improve cyber security knowledge in a structural way and to teach students to protect themselves against cyber-attacks.

2.5 ENVIRONMENTAL FACTOR

Environmental factors can include the influence of parents, peers and colleagues. These three elements are important for the formation of high environmental values. A study from Pitchan (n.d.), found that most of parents of respondents play a role in educating their children on cyber security practices.

Parents should monitor their child's social media accounts no matter where they are. Monitoring and advising children on the advantages and disadvantages of social media will indirectly affect the value of children's awareness of how to use social media safely. In addition, colleagues and peers can also help by reminding each other and sharing accurate information about threats or how to handle social media safely (Saizan & Singh, 2018).

Further evidence on the importance of a cyber-literate environment is also available from the Cyber Parenting Model and the Cyber Bullying Study at Universiti Malaysia Terengganu. Ahmad et al. (2018) also agreed that including environmental values in his study model as a cyber-literate environment is very important. Noh and Ibrahim (2014) stated that the existence of a cyber-literate environment can prevent the occurrence of cyber bullying and other cybercrimes.

Zulkipli et al. (2021) studied about the importance of awareness among the elderly. In the study they mentioned about the ways in which attackers deceive the elderly by sending messages that may cause these people to be easily misled by them. It will therefore cause these elderly people to provide personal data information such as financial and health to the attacker. To save the elderly from being deceived by attackers, the researchers have listed several suggestions. Among the suggestions is that the researchers hope that this group has a support system on their side so that if anything happens to them, at least they have someone to depend on.

A recent study done by Tan et al. (2020) on the elderly showed the importance of environmental factors on cybersecurity awareness. Through the method of face-to-face interview research, this study concluded that many seniors are aware of cybersecurity problems and they are also conscious of the lack of current cyber laws. This study has proven that older people in Malaysia are interested in learning about cyber security. Therefore, given that we are now amid COVID-19, the Malaysian government and society must play a very important role in further raising cybersecurity awareness to all senior citizens in Malaysia

2.6 AWARENESS OF CYBERSECURITY

A study in Saudi Arabia done by Alotaibi et al. (2016) stated that awareness is one of the effective approaches in developing applications for creating cybersecurity awareness. This research reviews gaming as a tool for this purpose. Based on a study done by Saizan and Singh (2018), most of social media users from German-Malaysian Institute showed moderate awareness of cybersecurity. Social media consumer awareness is measured based on several factors which are attitude, knowledge factors and the environment. This measurement is very important because social crime also occurs when using social media.

Likewise, the study done by Bhatnagar and Pry (2020) indicated that even though university students demonstrated a high level of awareness on certain elements in cybersecurity such as cyberbullying, personal information, and internet banking but they are still lacking appropriate knowledge on other aspects. For example, they lack proper knowledge on cybersex and self-protection. Therefore, various stake holders need to do their jobs and responsibilities in order to disseminate the knowledge to all the level of community,

Next, the overall result from a study done by Al-Janabi and Al-Shourbaji (2016) suggested that their target group which include academic staff, researchers, undergraduate students and employees within the educational sector in the Middle East lack awareness on most cybersecurity incidents and their consequences. Based on the weaknesses identified in this study, a few recommendations are proposed and the awareness framework is required for other substantive safety measures to protect important data from being exposed. The required awareness frameworks include identity management, audit, digital forensics, and information-system management security to safeguard personal information data now and in the future.

As a conclusion, this study used demographic profile, social media information, attitude factor, knowledge factor and environmental factor as the main factors since most of the journals proved that these factors affected the awareness of cybersecurity. The researchers also used the gender factor to achieve the objective of this study.

3.0 METHODOLOGY

3.1 INSTRUMENT

The questionnaire for this study was adapted from Saizan and Singh (2018) and Hammarstrand and Fu (2015). Based on the questionnaire adapted from Saizan and Singh (2018), there are five sections that consist of Section A until Section E. Section A was the information on demographic profile to know the background of the respondents. Then, for Section B the respondents were asked about their social media information such as what type of social media account that they have and also the estimated time that they spent to use their social media in a day. Section C was the information pertaining to the attitude of the respondents when using social media. Subsequently, Section D was the knowledge of the respondents against cyber threats, cyber laws, and ongoing cybercrime. The last section was Section E where the environmental situation of the respondents is identified.

Furthermore, Section F was the section where a dependent variable was examined which is the awareness of cybersecurity. For this section, the question was adapted from Hammarstrand and Fu (2015). In this section, the respondents were asked on the awareness of the risk that may occur and what they had done to protect themselves from these threats.

Further investigation has been made by conducting a pilot study in order to test the questionnaire. This pilot study involved 30 students of UiTM Cawangan Negeri Sembilan Kampus Seremban 3. Furthermore, the researcher tested the reliability of their pilot study by using Cronbach’s Alpha. The validity and reliability of the questionnaire are satisfied where each item in the questionaires indicate more than 0.6 of Cronbach’s Alpha values.

The theoretical framework of the study is explained in Figure 2. The independent variables involved are demographic profile, social media information, attitude, knowledge and environmental factors.

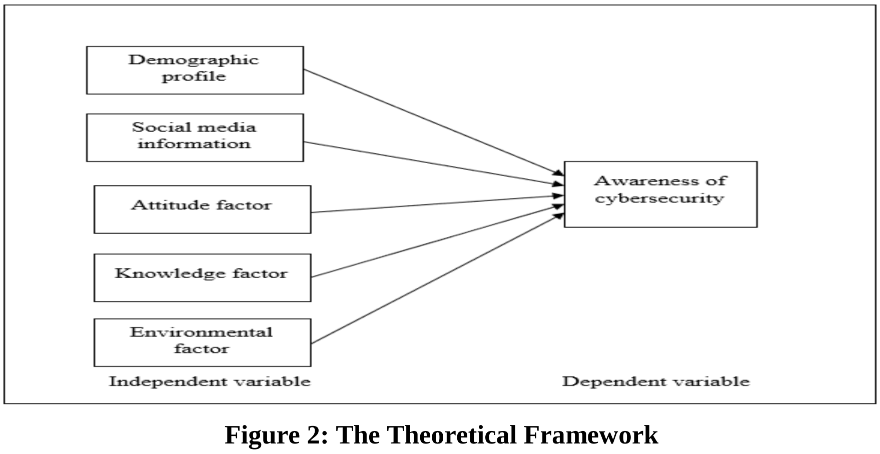

Figure 2: The Theoretical Framework

3.2 MULTIPLE LINEAR REGRESSION

In this study, the researchers used Multiple Linear Regression (MLR) by running the data in IBM SPSS software to achieve the objectives for this research. Multiple linear regression extends simple linear regression to include more than one explanatory variable (Tranmer & Elliot, 2008). Awareness of cybersecurity is the dependent variable that will be used in this research. Meanwhile factors that lead to cybersecurity will be the independent variables which are age, gender, marital status, faculty (FSKM, FSPPP and FSR), social media type (messaging, video sharing, microblogging and social networking) , approximate duration of using social media, attitude factor, knowledge factor and environmental factor.

The MLR model for this research is:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + ... + \beta_{14} X_{14}$$

Where,

Y = Total Score of Cybersecurity Awareness

$\beta_1, \beta_2, ..., \beta_{14}$ = Parameters of regression equation

$X_1, X_2, ..., X_{14}$ = Predictor/Independent Variables

MLR has been done to check the significance of the whole model. In MLR, the significance of the relationship between the independent variables and the total score of cybersecurity awareness can be examined by using the p-value in the t-test analysis. To examine this method, there are a few assumptions that need to be fulfilled before conducting MLR. The important assumptions are the relationship between the dependent variable and each independent variable must be linear, the errors terms should be normally distributed, there is no multicollinearity that exist in the data, the error variance must be constant, the error terms must be independent and no outlying that denote as influential cases in the data.

3.3 SAMPLING TECHNIQUES

Overall, the total students who registered at UiTM Negeri Sembilan Branch, Seremban Campus in October 2020 is 5846 students. There are three faculties which are FSKM, FSPPP and FSR. However, the total number of students in each faculty is different. There are 1695 students in FSKM, 3187 students in FSPPP and lastly 964 students in FSR. The sampling technique that the researchers use to conduct this study is stratified sampling. The sample size that was collected is 201 respondents. Table 1 shows the number of sample size for each faculty that was taken for this study.

Table 1: Number of Sample Size for each Faculty

FACULTY	POPULATION	SAMPLE SIZE
FSPPP	3187	72
FSKM	1695	111
FSR	964	18
TOTAL	5846	302

4.0 RESULT AND DISCUSSION

4.1 DESCRIPTIVE ANALYSIS

The demographic profile was analysed by presenting the frequency and percentage of the respondents that were involved in this study. Basically, this analysis was to describe the demographic profile, type of social media used and score of hours spent on social media. The collection of the data for 201 respondents is used for descriptive analysis.

Table 2 shows the summary of demographics profile analysis. Based on this table, mostly the gender involved in the study is female students with the percentage of 77.61 percent while there are some male students with the percentage of 22.39. In conclusion, the percentage of the female students involved in this study is more than half compared to the male students. Next, the range of the age of the students involved in this study is between 19 to 26 years old. Majority of them with 82 students recorded are 22 years old. The least students recorded based on their age are 25 and 26 years old with both ages have one respondent respectively. Lastly, the largest number of respondents was from FSKM with 111 students followed by 72 students from FSPPP. Students from FSR recorded the lowest number of respondents at 18 students.

Table 2: Summary of Demographics Profile Analysis

Criteria		Total Students	Percentage
Gender	Female	156	77.61
	Male	45	22.39
Age	19 years old	2	1.00
	20 years old	31	15.42
	21 years old	51	25.37
	22 years old	82	40.80
	23 years old	26	12.94
	24 years old	7	3.48
	25 years old	1	0.50
	26 years old	1	0.50
Faculty	FSKM	111	55.22
	FSPPP	72	35.82
	FSR	18	8.96

Next, the respondents were asked about the category of social media that they used. Table 3 shows the results of the descriptive statistics for each category in the social media. Messaging is the category that is mostly used with the total respondents of 157. This is followed by video sharing, micro blogging and social networking. Social networking gets the least number of users in this study with 36 respondents only.

Table 3: Type of Social Media

Type of Social Media	Total Users	Percentage
Messaging	157	48.5
Video Sharing	81	25.0
Microblogging	50	15.4
Social Networking	36	11.1

Table 4 shows the mean score and variance for hours spent on social media. The results indicate that the average hours spent on social media is 7.51 hours per day with variance 19.031.

Table 4: Mean Score and Variance for Hours Spent On Social Media

Variable	Mean	Variance
Hours Spent On Social Media	7.51	19.031

4.2 THE AWARENESS OF CYBERSECURITY BETWEEN GENDERS

Table 5 shows that the total score of cybersecurity awareness between female and male. There are more female respondents than male respondents.

Table 5: Total Score of Cybersecurity Awareness between Gender

Gender	N	Mean	Standard Deviation	Standard Error Mean
Female	156	28.42	4.072	0.326
Male	45	28.76	4.978	0.742

In Table 6, the Levene's Tests for Equality of Variances reveals insufficient evidence of unequal variances since the F value is equal to 1.139 with p-value equal to 0.287 which is larger than α=0.10. The t-test for Equality of Means shows that there is no significant difference in the total score of cybersecurity awareness between male and female with t value equal to -0.458 and p-value equal to 0.647 which is larger than α=0.10.

Table 6: Independent t-Test of the Cybersecurity Awareness between Genders

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
TEST MARK	Equal variances assumed	1.139	0.287	0.458	199	0.647	0.332	0.726	-1.099	1.764
	Equal variances not assumed			0.410	61.970	0.683	0.332	0.811	-1.288	1.953

4.3 THE DETERMINANTS OF AWARENESS OF CYBERSECURITY

Firstly, the original model of MLR was analysed. Since MLR was used, the assumptions of MLR have been checked in order to fulfil all the assumptions. Based on the original model, there are 14 predictor variables and 1 dependent variable which is the total score of cybersecurity awareness. The output of the variable significant values are shown in Table 7.

Table 7: The Results of Original Model

Predictor	Variable Significant Value
Gender	0.538
Age	0.075
Single	0.216
Married	0.098
FSKM	0.786
FSPPP	0.692
Messaging	0.837
Video Sharing	0.490
Microblogging	0.265
Social Networking	0.522
Hours Spent	0.991
Total Score of Attitude Factor	0.040
Total Score of Knowledge Factor	0.000
Total Score of Environmental Factor	0.866

Based on Table 7, the predictors' variables that are chosen for the final model are the variables that have significant value less than 0.10. According to the significant value for each variable, the predictors that will be chosen for the final model are age, marital status, total score attitude factor and total score knowledge factor. Since the significant variable for each predictor variable is less than 0.10, hence only four out of 14 predictor variables were chosen to be included in the final model. The researchers then used a stepwise method which is one of the technique in MLR to find the best factors that affect cybersecurity awareness.

Again, for the final model, the assumptions of the final model need to be examined one by one. There is a linear relationship that exists between the total score of cybersecurity awareness and the total score of knowledge factor and the errors are normally distributed. The error variances are also constant and there is no serial correlation problem and multicollinearity presence in this model. So, it can be concluded that all the assumptions of multiple linear regression have been fulfilled.

Based on the analysis done, the results of the final model is shown in Table 8. The total score of knowledge factor is the only factor influencing cybersecurity with the significance less than alpha 0.10.

Table 8: The Results of the Final Model

Predictor Variable	Significant Value
Age	0.991
Married	0.996
Total Score of Knowledge Factor	**0.000**
Total Score of Attitude Factor	0.804

5.0 CONCLUSION AND DISCUSSION

The t-test results indicate that there is no significant difference in the total score of cybersecurity awareness between male and female. This suggests that there is no evidence to show that cybersecurity awareness differs by gender i.e. men and women have the same level of awareness of cybersecurity. A research done by Anwar et al. (2017) stated that there are significant differences in cybersecurity awareness between genders. However, the results of this study are contrary to the results of previous studies which say that there is no difference in cybersecurity awareness between men and women.

In this study, all the respondents have at least two types of social media. Based on the finding of this study, messaging social media platforms such as whatsapp, telegram and messenger had the highest number of users. Kemp (2019) referred to the global statistics that illustrate messaging apps is in the top 5 of having active user in the world as of April 2019.

The next finding is the significant relationship that exist between the knowledge factor and cybersecurity awareness. This was supported by Kovacevi ˇ c et al. (2020) that stated knowledge proved to be a dominant factor for cyber security awareness. The knowledge to control their social media is also important among social media users as mentioned by Saizan and Singh (2018). Due to the the lack of knowledge, a large number of users are more vulnerable to cyber attacks and are unaware of the risks when sharing their personal information as discovered by Das and Patel, 2017. It is proven that the knowledge factor plays an crucial role in cybersecurity awareness.

The finding also points out that people who have more knowledge of the various types of cybersecurity threats have a low probability of falling victim to cybersecurity crimes. Meanwhile, demographic profile, type of social media used, time spent on social media, attitude factors as well as environmental factors do not affect the level of cybersecurity awareness among individuals.

As a conclusion, this research is to determine the relationship between demographic profile, social media information, attitude factor, knowledge factor, and environmental factor as significant predictors of the awareness of cybersecurity. It can be seen from this study that male and female have the same level of cybersecurity awareness. Hence, male and female students do not differ on cybersecurity awareness. Furthermore, both genders have equal risk of falling victim to cybersecurity cases. Ultimately, both genders have the same right to express an opinion on cybersecurity matters. The finding also points out that people who have more knowledge of the various types of cybersecurity threats have a low probability of falling victim to cybersecurity cases. Meanwhile, demographic profile, type of social media used, time spent on social media, attitude factors as well as environmental factors do not affect the level of cybersecurity awareness among individuals.

Future recommendations can be made in the future to further improve the results of this study. Improvements can be done by increasing the number of respondents since the researchers cannot reach a lot of respondents due to their lack of interest. In fact, in order whether which gender is related to awareness about cybersecurity, further study needs to balance the number of respondents between male and female. Lastly, the recommendation is to conduct this study using a different group of respondents in order to discover whether many people are conscious about their security while using the social media platform.

ACKNOWLEDGEMENTS

A special thanks to all staff and students of UiTM Negeri Sembilan, Seremban Campus for their contributions directly and indirectly towards this study.

REFERENCES

Ahmad, N., Mokhtar, U. A., Fariza Paizi Fauzi, W., Othman, Z. A., Hakim Yeop, Y., & Huda Sheikh Abdullah, S. N. (2018). Cyber security situational awareness among parents. In *2018 cyber resilience conference (crc) (p. 1-3).* doi: 10.1109/CR.2018 .8626830

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness. *Int. J. Inf. Secur. Res.(IJISR)*, 6(2), 660– 666.

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. *Journal of Information & Knowledge Management, 15*(01), 1650007.

Al-Mohannadi, H., Awan, I., Al Hamar, J., Al Hamar, Y., Shah, M., & Musa, A. (2018). Understanding awareness of cyber security threat among it employees. In *2018 6th international conference on future internet of things and cloud workshops (ficloudw) (pp. 188–192).*

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437–443.

Bhatnagar, N., & Pry, M. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. *Information Systems Education Journal, 18*(1), 48–58.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?* arXiv preprint arXiv:1901.02672.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of information security and applications*, *42*, 36– 45.

Das, R., & Patel, M. (2017, 04). Cyber security for social networking sites: Issues, challenges and solutions. *International Journal for Research in Applied Science and Engineering Technology, V*, 833-838. doi: 10.22214/ijraset.2017.4153

Dollarhide, M. E. (2021, Mar). *Social media definition. Investopedia*. Retrieved from https://www.investopedia.com/terms/s/social-media.asp

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

Fatokun, F., Hamid, S., Norman, A., & Fatokun, J. (2019). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: An empirical investigation on malaysian universities. *In Journal of physics: Conference series*, *1339*, 012098.

Fumudoh, S., & Viswanathan, U. (2014). *Exploring the relationship between online privacy on cyber security*.

Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. (2020). *A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach*.

Hammarstrand, J., & Fu, T. (2015). *Information security awareness and behaviour: of trained and untrained home users in Sweden.*

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), 00346.

Kemp, S. (2019, Apr). *Digital 2019: Q2 global digital statshot - datareportal – global digital insights. DataReportal – Global Digital Insights*. Retrieved from https://datareportal.com/reports/digital-2019-q2-global-digital-statshot

Kovacevi ˇ c, A., Putnik, N., & To ´ skovi ˇ c, O. (2020). *Factors related to cyber security ´ behavior.* IEEE Access, 8, 125140–125148.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & security, 25(4), 289–296.

Malaysia Computer Emergency Response Team (MyCERT). (2021, Jan). Retrieved from MyCERT : Incident Statistics - Reported Incidents based on General Incident Classification Statistics 2020

Marks, A., & Rezgui, Y. (2009). A comparative study of information security awareness in higher education based on the concept of design theorizing. In *2009 international conference on management and service science (pp. 1–7).*

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

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber security behaviour among higher education students in malaysia. *J. Inf. Assur. Cyber Secur, 2017*, 1–13.

Noh, C. H. C., & Ibrahim, M. Y. (2014). Kajian penerokaan buli siber dalam kalangan pelajar umt. *Procedia-Social and Behavioral Sciences*, *134*, 323–329.

Ogutcu, G., Testik, O. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83–93.

Pitchan, M. A. b. (n.d.). *Kesedaran dan amalan keselamatan siber dalam kalangan pengguna internet di malaysia.*

Saizan, Z., & Singh, D. (2018). Cyber security awareness among social media users: Case study in german-malaysian institute (gmi). *Asia-Pacific J. Inform. Technol. Multimedia*, *7*, 111–127.

Shaari, A. H., Kamaluddin, M. R., Paizi, W. F., Mohd, M., et al. (2019). Online-dating romance scam in malaysia: An analysis of online conversations between scammers and victims. GEMA Online. *Journal of Language Studies*, *19*(1).

Smitherson, D. (2012, Nov). *Impact of cybercrime and security on social media.* Retrieved from https://www.socialmediatoday.com/content/impact-cyber -crime-and-security-social media

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. In *2010 international conference on availability, reliability and security (pp. 196–203).*

Tan, S. L., Vergara, R. G., Khan, N., & Khan, S. (2020). Cybersecurity and privacy impact on older persons amid covid-19: A socio-legal study in malaysia. *Asian Journal of Research in Education and Social Sciences*, *2*(2), 72–76.

Tranmer, M., & Elliot, M. (2008). Multiple linear regression. *The Cathie Marsh Centre for Census and Survey Research (CCSR), 5*, 30–35.

Zhang, Z., & Gupta, B. B. (2018). Social media security and trustworthiness: overview and new direction. *Future Generation Computer Systems, 86*, 914–925.

Zulkipli, N. H. N., et al. (2021). Synthesizing cybersecurity issues and challenges for the elderly. *Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12*(5), 1775–1781.