Security Awareness among Students in Campus Environment: Case Study

Najihah Osman[1], Haniza N[2], Zulkiflee M.[3]
haniza@utem.edu.my
Faculty of Information Technology and Communication,
Universiti Teknikal Malaysia Melaka, Ayer Keroh, Melaka, Malaysia

Abstract
In this era of globalization without limitation, many security issues occur, especially in a public network. Internet users significantly increased every single day. However, only some users are aware of security issues when they use Internet services. For the campus network environment, both staffs and students are susceptible to security threats such as data theft, unauthorized access and more due to different levels of awareness towards security threats. This paper is to study the level of awareness among students on security issues based on KSA model. As a case study, the survey was distributed among students in the UTeM campus network. A quantitative study was conducted, and a structured questionnaire has been designed and distributed among students. The variables were focused on three (3) aspects, which are Knowledge, Skill and Ability (KSA). The finding shows the relationship between KSA with the level of awareness among students has been revealed. From the result, Knowledge is the most significant aspect that contributes to high awareness. For the future, a study about increasing students' knowledge about security issues should be addressed.

Key words:
Security Issues, Campus Network, Awareness

1. Introduction

Security defined as a quality or condition of being secure that is to be free from danger and protected from enemies that will endanger, deliberate or otherwise. Cybersecurity, computer security or IT security is computer system protection from theft or causing damage to hardware, software, or electronic data. However, various threats have malicious intentions such as phishing threats. Internet users are susceptible to security threats when connected online [1]. This study covers three (3) aspects which are Knowledge, Skills and Abilities (KSA).

Knowledge is a theoretical or practical understanding of subjects such as facts, information, and skills gained through experience or education. Skill refers to the expertise and set of actions acquired through practice. Ability is the ability to perform the physical and mental acts required by the task.

A campus network is a LAN network that relates to corporates, government agencies, universities, or similar organizations. In this context, an ordinary campus includes a set of adjacent buildings. A campus network is referred as a computer network that provides multiple buildings connectivity within a campus area.

In the era of globalization today, various security threats are on an alarming level. Security threats including malware, spyware, and phishing posed a serious problem[2]. The awareness and behavior among consumers are an essential part of organizational security performance. The best solution to improve the security performance is by improving awareness among its users [3].

Most computer users with a lack of security awareness exposed themselves to data loss, data corruption, identity theft, or other malicious activities. These users are now more likely to be victims of social engineering because they lack awareness in computer security and have fewer skills related technology and security policies. Thus, individual awareness of these issues is essential [4][5].

Contribution. In this paper, we investigate the level of security awareness among UTeM students. We conducted a series of experiments with students from different faculties. A structured questionnaire has been distributed and is analyzed to determine the possible factors that influence security issues awareness. As a result, this study may help to raise the level of awareness on security issues among students as well as minimize the risk of threats.

Outline. Section II introduces the literature review on Security Awareness, Model of Study and Operational Definition of Variable. Section III presents the methodology applied in this study. Section IV describes the analysis and results. Section V discusses the findings. Section VI concludes the paper.

2. Related Work

Security defined as a quality or condition of being secure that is to be free from danger and protected from enemies that will endanger, deliberate or otherwise. Cybersecurity, computer security or IT security is computer system protection from theft or causing damage to hardware, software, or electronic data.

Manuscript received October 5, 2023
Manuscript revised October 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.10.23

2.1 Security Awareness

Security Awareness (SA) refers to users understanding of security measures towards the protection of personal data or that of their organization in cyberspace. Meanwhile, Mahamadou Kante (2018) [6] stated that Software Security Awareness (SSA) could be defined as the knowledge that members of an organization possess regarding the protection of the physical and information assets of that organization.

It also reflects the attitude and motivation of the members of an organization towards understanding and addressing various security issues [6]. Being security aware means that there is the potential for some people to steal, damage, or misuse the data stored within a company's computer systems and throughout its organization deliberately or accidentally. Unpreventable incidents could be identified faster, resulting in less business impact. According to a study [7], the Information Security Awareness (ISA) refers to educating the campus community about the inherent risks of the confidentiality, integrity, or availability of systems & data, and how all individuals or students can protect their systems and data.

2.2 Model of Study

Many models have been used in the previous studies to measure dimensions such as Awareness-Knowledge-Attitude (AKA), Attitude-Knowledge-Behavior (AKB) and Knowledge-Skill-Ability (KSA). These models are combined and depict as in Fig. 1.

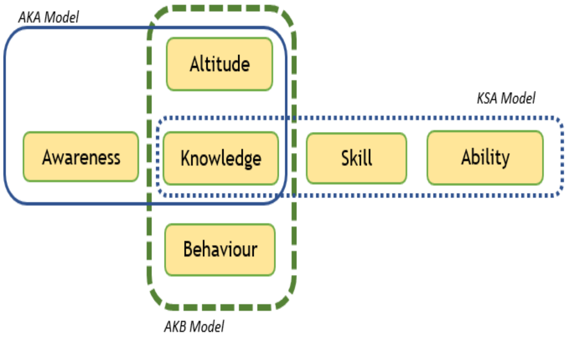


Fig. 1: Common Model of Study

Each model has different purposes. For example, the AKA Model is used to determine *Awareness, Knowledge* and *Altitude* which related to the educational environment. AKB Model is used as a prototype for accessing information security awareness. KSA Model is referred to as a measurement for Cybersecurity competency.

The awareness term is referring to concern and sensitivity, knowledge is objective and equates awareness with the ability to make forced-choice decisions above a chance level of performance[8]. Palmer (1998) [9] stated that these three are reoccurring concepts that are mentioned frequently in the literature, especially *Awareness, Knowledge* and *Attitudes*. According to Lavega (2004) [10], these three components (AKA) play an essential role on the impact of students.

Kruger and Kearney (2006) [11] concluded that these three AKA Model components used as a basis and the model developed on three equivalent dimensions namely what does a person know (knowledge), how do they feel about the topic (attitude) and what do they do (behavior).

Alavi & Leidner (2001) [12] stated that Knowledge, Skill and Ability (KSA) are defined by as all possibilities of this KSA Model to accomplish a specific job action. As for this study, the most suitable model is the model of combined necessary KSAs for security issues awareness.

a) *Knowledge*: Camerer and Hogarth (1999) [13] stated that cognitive psychologists have presented evidence that knowledge is the combination of declarative knowledge and procedural knowledge. Alavi and Leidner (2001) [12] defined knowledge as a justified understanding that improves an entity's capacity for taking effective action. Without advanced knowledge of computer science, most users could not tell which program a process belongs to. Meanwhile, Baartman 2011 defines knowledge is a product of reciprocal and interpretative construction emerges from learners' participation in social practice [14]. As a summary, knowledge is the capability of a person to understand things from various perspectives.

b) *Skill*: Skill is representing a consistent response, based on components in knowledge to a particular set of situational criteria [15]. Skills are also interwoven with knowledge and pertain to the psychomotor domain in manipulating and constructing. Meanwhile, Prestwich & Ho-Kim [16] determined the skills needed for Minnesota businesses when hiring international business professionals. In summary, the skill can be referred to as a goal-directed, well-organized set of actions that is acquired through practice and performed with an economy of effort, which enables a person to do something well.

c) *Ability*: Rhee, Kim, and Ryu (2009) [17] contended that understanding cybersecurity terminology is an ability. Ability is the foundation for knowledge and skill application [18]. To sum up, the ability is the capacity to carry out the physical and mental acts required by a specific task.

As a summary, in this paper KSA model is used to evaluate the relationship between capabilities of mind, body and soul towards the response to security awareness. Each factor has its function and there are interconnected to each other. However, this paper will define the most significant factor in improving the awareness level among students.

2.3 Conceptual Operation Definition

This section will elaborate on the variables involved in the process of determining the relationship between KSA model. Each variable has its operational definition. Table 1 shows several variables definition based on their operational in security perspective. An understanding of these operations is required.

Physical security is a critical practice that is a fundamental principle to all computer systems [19]. Physical security is a primary cybersecurity concern for OISUs and organizations. According to Newsome & Jarmon, 2016 [20] physical security is defined as physical measures taken to safeguard personnel, to protect unauthorized access to equipment, installations, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft.

Table 1: Conceptual Operation Definitions

Variables	Operation Definition
Physical Security	Physical measures are taken to safeguard personnel, to protect unauthorized access to equipment, installations, material documents and to safeguard them.
Application Security	The use of software, hardware, and methods to protect from threats.
Information Security	Protecting information from unauthorized access and modifications.
Internet & Info Security	The Internet security element is to protect data during online transactions while network security consists of policies and practices adopted.
Security Tool	Security measures are designed to deny unauthorized access and to protect personal and property.
Problem Solving	Finding solutions for difficult or complex issues.

Information Security used to maintain organizational data from unauthorized access or modification to ensure availability, confidentiality, and integrity. Maintaining information security generally focuses on protecting three main aspects of confidentiality, integrity and availability of information [21]. Information security also defines as a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. The term information security (IS) simply implies the act of protecting and preserving information.

Internet Security measures to data protection during online transmission over a collection of interconnected networks. In contrast, network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the safeguarding of an organization’s data networking devices, connections and contents, and the ability to use the network to achieve the organization’s data communication tasks.

Indeed, *problems* and *problem solving* have had multiple and often contradictory meanings through the years-a fact that makes interpretation of the literature difficult [22]. The study revealed categories of goals that were identified by respondents as *problem solving* is to train students to *think creatively* and *develop their problem-solving ability*. The problem solving can be referred to as any specific sequence of cognitive operations. As a summary, problem-solving can be defined as a process that is the extracting part of the more extensive problem process that involves problem finding and problem shaping. Hence, problem solving can be defined as the process of finding solutions to a problem.

3. Methodology

In this section, we describe the methodology that is used to complete the study. Begin with defining the proposed framework, research process and sampling strategies. This process is critical to ensure that the study has been carried out systematically and produces the expected output.

3.1 Proposed Framework

A previous study conducted by [23] stated that knowledge towards application security, information security and Internet and network security is an essential thing in order to avoid threats. For example, password disclosure can result in data leakage and the emphasization such as setting passwords is significant. Meanwhile, downloading software from the Internet may have hidden Trojans virus, backdoors, and other malicious code. Therefore, many systems are invasive and used by the attacker.

Gabriel & Joshua (2018) [24] identified that knowledge and behavior of general security awareness, information security and physical security are crucial amongst students joining higher academic institutions in developing countries. Meanwhile, a previous project [25] studied knowledge and skill in physical security, application security, information security, and Internet and network security in a survey on security issues in service delivery models of cloud computing. Aggeliki et al. (2015) [26] identified that the problem-solving activities are used to confirm or disconfirm the applicability of the theoretical knowledge related to the practical problems analyzed.

In addition, Richard (2017) [27] investigated cybersecurity competency for the organization. There are many aspects of the knowledge, skill, and ability. Richard focused on four aspects of knowledge and skill which is application security, information security, physical security and Internet and network security. Ability to focus on the natural capacity that enables an individual to perform a particular job or task successfully developed a framework related to cybersecurity competency.

These findings synthesized into a general framework as shown in Figure 2. It presents the component of dimensions of security issues elements are recognized. There are six (6) components in the security issues and there are components categorized according to security issues dimensions which is knowledge, skill, and ability. All the security issues components and elements are included in this present study for further inquiry or examination.

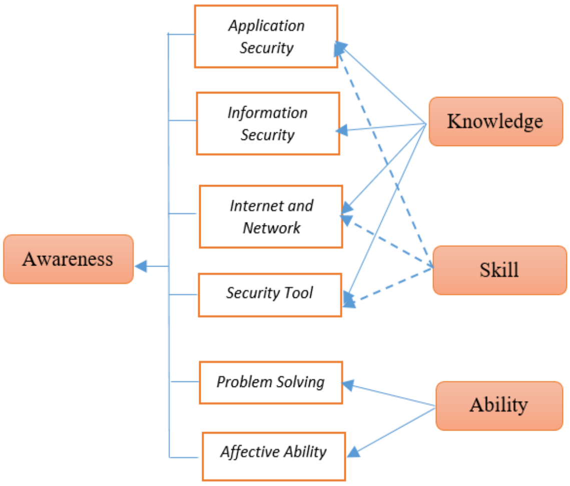


Figure 2: A proposed framework of Security Awareness

3.2 Research Process

For conducting the study, it has seen that Figure 3 summarizes the phases and their activities involved. This research process can be divided into four (4) stages: 1) Analysis, 2) Design, 3) Implementation and 4) Result & Discussion.

In the first stage, the problem has been formulated. We need to identify the research model to be used and choose the best model from a previous study. Secondly, the quantitative methodology requires a structured questionnaire to be developed based on the framework given. It is vital to obtain valid and accurate information in conducting studies on the sample. As a result, the data has been collected by distributing questionnaires to the respondents.

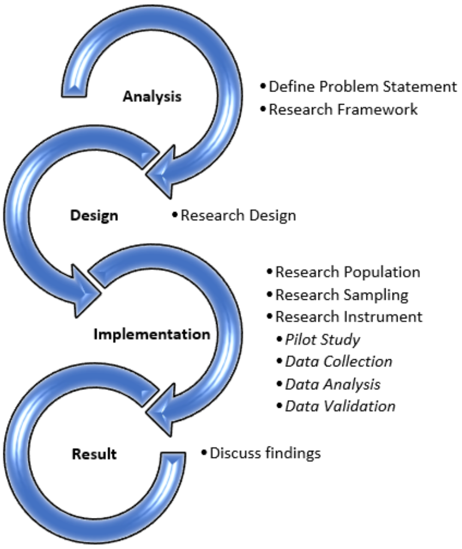


Figure 3: Research Process

For the implementation phase, the more significant number of UTeM respondents have undergone this survey. Universiti Teknikal Malaysia Melaka (UTeM) was established on 1st December 2000 as the 1st Technical Public University in Malaysia. There are eight (8) faculties with a total of 12,490 students enrolled with a majority at the undergraduate level. Based on the determination of sampling size stated by Krejcie and Morgan (1970) as shown in Table 2, we manage to take a sample of 175 students to becomes respondents.

Table 2: Sample size determination sample

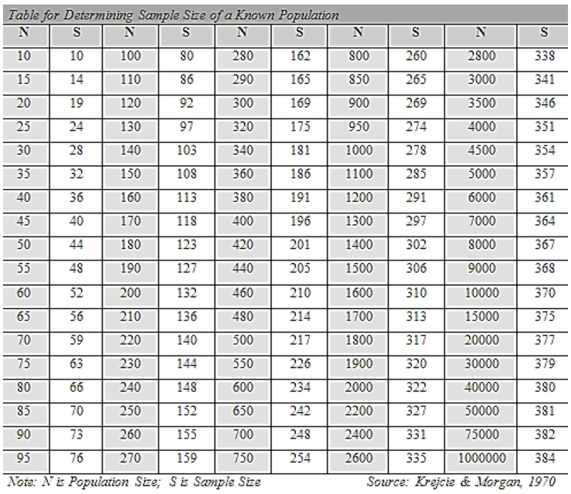


Table for Determining Sample Size of a Known Population

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

Note: N is Population Size; S is Sample Size *Source: Krejcie & Morgan, 1970*

The questionnaire is the most effective way to get information from respondents. The use of the instrument in the form of a questionnaire is beneficial if it is well prepared and has consistent and reliable items [28]. In a situation of limited time and cost, it is the most suitable. The use of closed-ended questionnaires is good because it does not require the respondent to think or to produce new ideas on a question. The data obtained will also be arranged in an orderly, clearly, and subsequently analyzed findings from answers given to interpret more effectively.

For this study, the questionnaire covers three (3) sections which are Demographic Background, Awareness Assessment, and Influence Factors for Security Issues Awareness. For a demographic background that involves gender, race, current education, faculty, and job experience. After analyzing the level of awareness and the possible factors that influence the awareness of security issues.

For the content validation, the pilot study has been carried out to determine the validity and reliability of the question. Based on the results of the content validation, some questions of the instrument are modified during the process occurs. The relevant items are maintained while the unnecessary items will be deleted. We used the platform Google Form and distributed to students through a link in WhatsApp and Instagram application. All responses data are collected and exported to excel file before data analysis procedures.

In the last stage, we use Statistical Package for the Social Science (SPSS) 25 and Waikato Environment for Knowledge Analysis (Weka) 3.8. Weka is a data mining software that uses a collection of machine learning algorithms and these algorithms can be applied directly to the data or called from the Java code. It contains tools for data pre-processing, classification, regression, clustering, association rules, and visualization. It is also well-suited for developing new machine learning schemes. It can be used to detect the various hidden patterns in the used dataset and find the most determining factors out of many. The use of SPSS can avoid errors during data analysis and calculations made are accurate. The expected outcome from this study is to determine the factor that influences security issues awareness.

3.3 Sampling Strategies

Sampling is part of the respondent selected from the larger population for the study. In the sample size determination Krejci and Morgan, the researcher selected a sample of 175 students. The strategies will be explained as Item Compilation and Scale Construction.

a) *Item Compilation*: The questions created and phrases by the target of UTeM students. The items are to be well-formed to avoid uncertainty for people. All items organized to reflect on the variables and. Next, the questionnaire also has been sorted in the proper flow. Later, invalid variables were removed from the instrument while the remaining variables were reorganized.

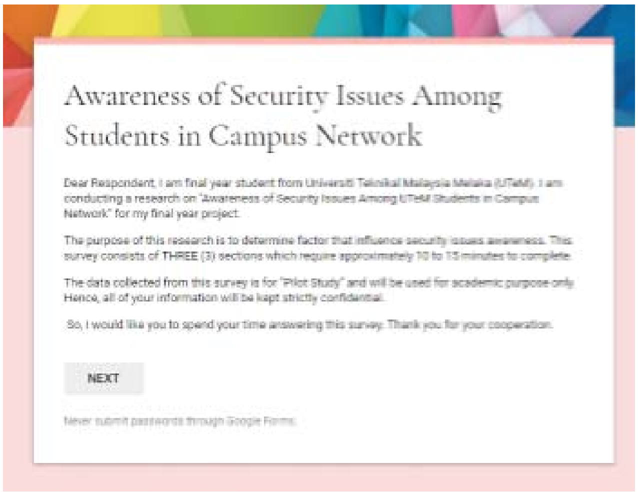
b) *Scale Construction*: Statements for the items on the variables used are positive and negative statements. Likert scales ranges from (Strongly Disagree) 1 to (Strongly Agree) 6 will be used as a scale range to measure the variables.

4. Analysis and Results

At the beginning of developing a structured questionnaire, we propose approximately 60 items, including positive and negative statements to avoid respondents' dishonesty and one-way statements. There are two sets of questions, namely *Awareness Assessment* and *Factor* that influence security issues awareness. All these domains were undergoing a reliability test using the Cronbach Alpha size. The acceptable range is more than 0.65. After the validation process, the number of items has been deducted into 42 items as shown in *Table 3*. Meanwhile, the following Figure 4 represents the questionnaire that has been distributed among UTeM students.

Table 3: Content with Cronbach Alpha size for Pilot run

Domain	Sub Domain	No of Item	Cronbach Alpha
Knowledge	Security Tool	19	0.980
	Information Security		
	Internet and Network Security		
	Application Security		
Skill	Security Tool	13	0.980
	Internet and Network Security		
	Application Security		
Ability	Problem Solving	10	0.976
	Affective Ability		
Total	42 Items		


Awareness of Security Issues Among Students in Campus Network

Dear Respondent, I am final year student from Universiti Teknikal Malaysia Melaka (UTeM). I am conducting a research on "Awareness of Security Issues Among UTeM Students in Campus Network" for my final year project.

The purpose of this research is to determine factor that influence security issues awareness. This survey consists of THREE (3) sections which require approximately 10 to 15 minutes to complete.

The data collected from this survey is for "Pilot Study" and will be used for academic purpose only. Hence, all of your information will be kept strictly confidential.

So, I would like you to spend your time answering this survey. Thank you for your cooperation.

Never submit passwords through Google Forms.

Figure 4: The distributed questionnaire

5. Discussion

This section discusses more detail about several results from different perspectives such as Descriptive Results, Awareness Assessment Result, Respondent Awareness based on Demographic and Attributes Selection Results.

Descriptive Result*: In general, the detailed result explains the information about gender, race, education level, faculty, and job experience. The detail has been summarized in*

a) *Table 4*. Based on the demographic distribution of respondents by gender, the researcher took a sample of 175 respondents from the University Technical Malaysia Melaka (UTeM), Melaka. Based on the determination of sample size [29], researchers have selected a sample of 81 male respondents which is equal to 46.3 percent (%). In contrast, 94 of the female respondents show a percentage of 53.7 (%). Thus, the total percentage of respondents is equal to 100 percent (%). Meanwhile, the difference in the number of both genders is 13 respondents which is about 7.4 percent (%).

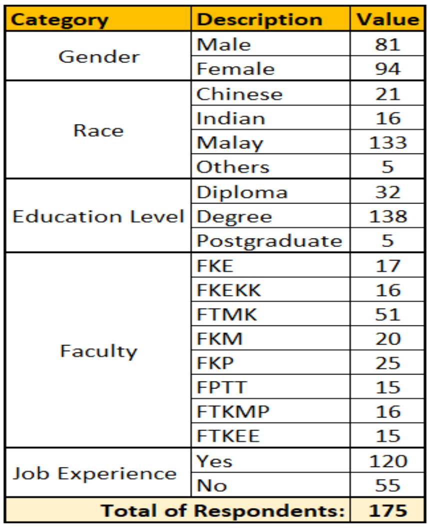
The results data based on the percentage of respondents by *race*, it shows that 76.0 percent (%) respondents involved in this study are Malay student with a frequency of 133. While respondents for Chinese and Indian shows the percentage of 12.0 and 9.1 percent (%) with a frequency of 21 and 16. The least response with a percentage of 2.9 percent (%) and frequency of 5 is another race. Based on the findings, the percentage of Malay respondents is higher than in others.

From the demographic for current Education level, there are three (3) levels, namely Diploma, Degree and Postgraduate. 78.9 percent (%) respondents involved in this study is in Degree education student with a frequency of 138. While respondents for Diploma and Postgraduate shows the percentage of 18.3 and 2.9 percent (%) with a frequency of 32 and 5. Based on the findings, students in Degree education has the most responses.

The demographic for the Faculty distribution is divided into eight (8) categories, namely FKE, FKEKK, FTMK, FKM, FKP, FPTT, FTKMP and FTKEE. FTMK shows the highest number of respondents involved in this study which is 29.1 percent (%) with a frequency of 51. The second and third highest was from FKP and FKM with a percentage of 14.3 percent (%) and 11.4 percent (%). The frequency of FKP and FKM was 25 and 20, respectively. Moreover, 9.7 percent (%) respondents were from FKE with a frequency of 17. FKEKK and FTKMP show the same percentage which is 9.1 percent (%) with a frequency of 16 respondents. FPTT and FTKEE also shows the same percentage which is 8.6 percent (%) with frequency of 15 respondents and was the lowest percentage, among others.

Finally, based on the distribution of the job experience of the subject studied show that 68.6 percent (%) respondents involved in this study have job experience with a frequency of 120. While 31.4 percent (%) respondents with a frequency of 55 have no job experience. Based on the findings, respondents with job experience have a higher percentage compare to no job experience.

Table 4: The detail of demographic information



Category	Description	Value
Gender	Male	81
	Female	94
Race	Chinese	21
	Indian	16
	Malay	133
	Others	5
Education Level	Diploma	32
	Degree	138
	Postgraduate	5
Faculty	FKE	17
	FKEKK	16
	FTMK	51
	FKM	20
	FKP	25
	FPTT	15
	FTKMP	16
	FTKEE	15
Job Experience	Yes	120
	No	55
Total of Respondents:		175

b) *Awareness Assessment Result*: The objective is to determine the level of awareness among UTeM students on security issues, whether students are aware or not of the issue. Students were required to answer the survey on awareness assessment from AA1 to AA10 in the structured questionnaire. Based on Figure 5, it shows that about 62 percent (%) of the respondents are aware of the security issues. Only 38 percent (%) not aware of the issues. Thus, this indicates that majority of the UTeM students are aware of security issues.

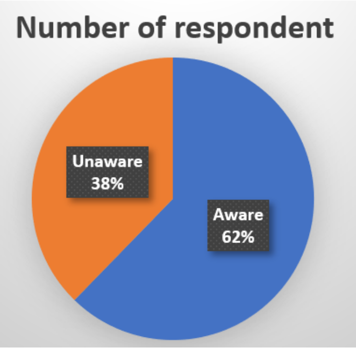


Figure 5: Security Awareness Level based on the number of respondents

c) *Respondent Awareness by Demographic*: Based on Figure 6, the percentage level of Security Issues Awareness among UTeM students by gender had been given. It shows that about 67.9 percent (%) of the respondents with high awareness about this issue were male. Only 57.5 percent (%) with awareness was female. Thus, this indicates that males have a higher awareness level compare to females.

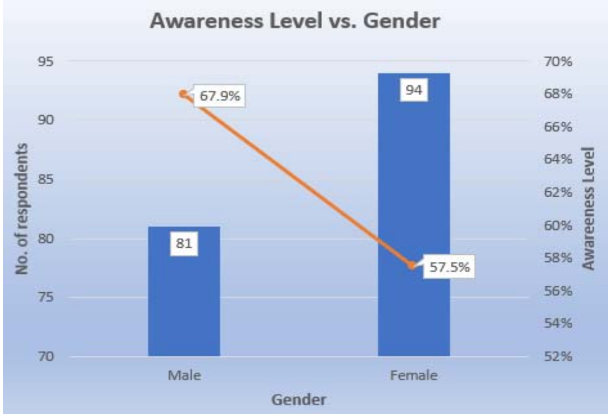


Figure 6: The relationship between Security Awareness Level vs. Gender

Based on Figure 7, the percentage level of Security Issues Awareness among UTeM students by race had been given. It shows that Chinese students have the highest awareness level with 91.0 percent (%) of the respondents. The second and third were Indian and Malay with a percentage of 68.8 percent (%) and 60.2 percent (%). In contrast, other has the lowest awareness level with a percentage of 20 percent (%). Thus, this indicates that Chinese students have a higher awareness level.

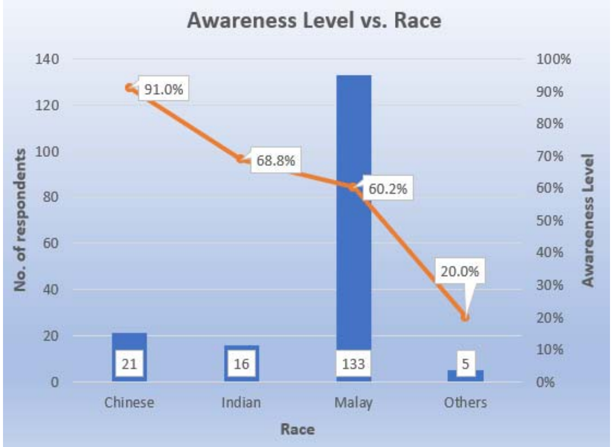


Figure 7: The relationship between Security Awareness Level vs. Race

Based on Figure 8, the percentage level of Security Issues Awareness among UTeM students by current education had been given. It shows that Postgraduate students have the highest awareness level with 83.3

percent (%) of the respondents. The second and third was Degree and Diploma with a percentage of 64.96 percent (%) and 46.88 percent (%). In summary, the result indicates that the higher the education level of a student, the better the awareness level about the issues.

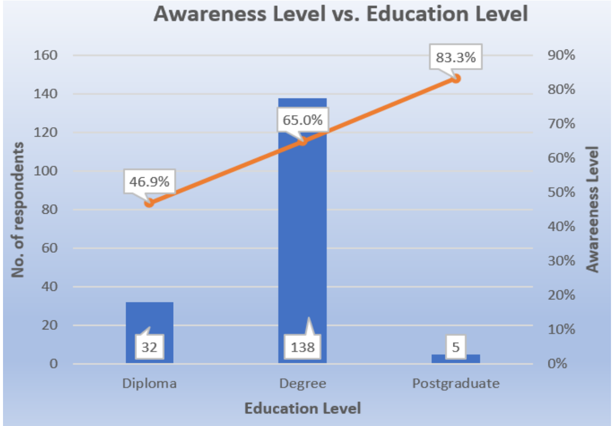


Figure 8: The relationship between Security Awareness Level vs. Education Level

Based on Figure 9, the percentage level of Security Awareness among UTeM students based on the faculty. The result shows that students form FTKEE have the highest awareness compares with other faculty with 75 percent (%) of the respondents. The second and third were belong to students from FTMK and FTKMP with a percentage of 73.08 percent (%) and 66.67 percent (%), respectively. Meanwhile, the fourth and fifth was from FKM and FKP with a percentage of 64.71 percent (%) and 60 percent (%). On the other hand, FKE and FKEKK have a percentage of 57.89 percent (%) and 50 percent (%). Finally, the lowest was FPTT with a percentage of 26.67 percent (%). The result indicates that even students from FTMK were the IT student, it does not confirm that they have a better awareness level, or they have higher security solution. The histogram shows that students from FTKEE have higher awareness levels compare to students from FTMK.

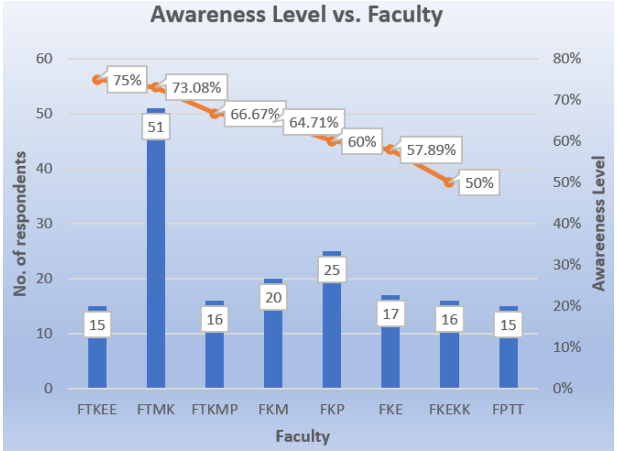


Figure 9: The relationship between Security Awareness Level vs. Faculty

Based on Figure 10, the percentage level of Security Issues Awareness among UTeM students by job experience had been given. It shows that about 65.6 percent (%) of the respondents with high awareness about this issue had job experience. Only 55.4 percent (%) of them have no job experience. Thus, this indicates that students with job experience have a higher awareness level compare to students with no job experience. Students with job experience tend to have a high awareness level towards security issues because they have experience and have the knowledge gained from the working environment.

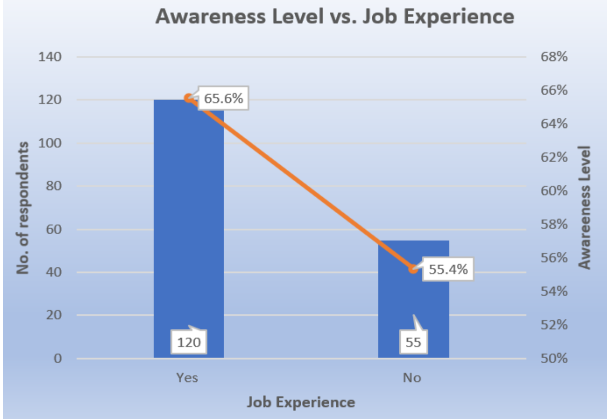


Figure 10: The relationship between Security Awareness Level vs. Job Experience

d) Attributes Selection Result: In this section, there are three (3) different types of tests obtained from Waikato Environment for Knowledge Analysis (Weka) 3.8 use to determine the factor that influences security issues awareness among UTeM students. These are referring to Correlation-based Features Selection (CFS) Subset Evaluation, Correlation Attribute Evaluation and Classifier Attribute Evaluation.

The result for Attributes Selection is represented in Figure 11. These attributes were selected based on their percentage. The bar chart shows the attributes selected based on the percentage given. Meanwhile, the line graph represents the total average questions that take place from different domains namely Knowledge, Skill and Ability. It has been labelled from KST1 to AAA4. Overall, the questionnaire is consisting of 42 questions.

By using the Correlation-based Features Selection (CFS) Subset Evaluation, it shows that only 6 items were selected which is 66.67 percent (%) of selected attributes is an item for domain knowledge with a frequency of 4. Meanwhile, the other two is from domain skill and ability both 16.67 percent (%) with a frequency of 1. Thus, this test shows that all the domains become the factor that influences security issues awareness.

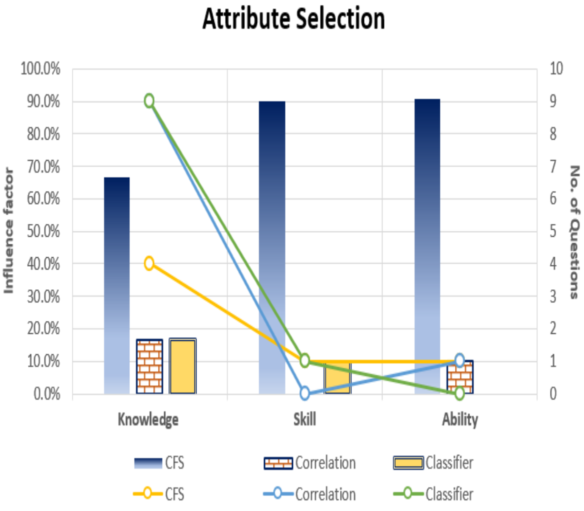


Figure 11: The summary of Attributes Selection

For the Correlation Attribute Evaluation, the top 10 items from the questions have been chosen for this study. After the analysis, the result found that there were items from domain knowledge and ability with a percentage of 90.00 percent (%) and 10.00 percent (%) involved in the top 10 items. Thus, this test shows that all domains are the factor that influences security issues awareness but only two domains were selected from the rank given which is knowledge and ability.

The Classifier Attribute Evaluation also using the top 10 items from the questions that have been chosen for this study. After the analysis, the result shows that there were items from domain knowledge and skill with a percentage of 90.00 percent (%) and 10.00 percent (%) involved in top 10 items. Thus, this test shows that all domains are the factor that influences security issues awareness but only two domains were selected from the rank given which is knowledge and skill.

In summary of the findings, it proves that *Knowledge*, *Skill* and *Ability* (KSA) are the core attributes that influence security issues awareness among UTeM students. However, the most important factor is knowledge.

6. Conclusion

From the conducted study, the result can be concluded that approximately 62 percentages (%) of UTeM students aware of Security issues while they are in the campus environment. Based on the distributed questionnaire, the result proves that the Security Awareness highly depends on Knowledge and followed by Skill and Ability. What is more, the result also shown that is not necessarily if a person is IT literate, he has higher awareness level. Meanwhile, if students know computer security, then they have a higher awareness of security issues regardless of the program they have enrolled in the university.

For the future, the study about the most effective way to increase knowledge among students about security awareness should be addressed.

Acknowledgments

The authors would like to thank INSFORNET, Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Universiti Teknikal Malaysia Melaka for giving opportunity and equipment to conduct this study.

References

[1] M. Gurunathan and M. A. Mahmoud, “A Review and Development Methodology of a LightWeight Security Model for IoT-based Smart Devices,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 2, pp. 125–134, 2020.

[2] H. Naderi, P. Vinod, M. Conti, S. Parsa, and M. H. Alaeiyan, “Malware signature generation using locality sensitive hashing,” in *International Conference on Security & Privacy*, 2019, pp. 115–124.

[3] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, “Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior,” *Int. J. Inf. Manage.*, vol. 45, pp. 13–24, 2019.

[4] M. Bada, A. M. Sasse, and J. R. C. Nurse, “Cyber security awareness campaigns: Why do they fail to change behaviour?,” *arXiv Prepr. arXiv1901.02672*, 2019.

[5] G. Kemper, “Improving employees’ cyber security awareness,” *Comput. Fraud Secur.*, vol. 2019, no. 8, pp. 11–14, 2019.

[6] M. Kante, “Software Security Awareness: A forgotten tactical and strategic weapon,” 2018.

[7] H. Hamid and A. M. Zeki, “Users’ Awareness of and Perception on Information Security Issues: A Case Study of Kulliyyah of ICT Postgraduate Students,” in *2014 3rd International Conference on Advanced Computer Science Applications and Technologies*, 2014, pp. 139–144.

[8] P. M. Merikle, “Toward a definition of awareness,” *Bull. Psychon. Soc.*, vol. 22, no. 5, pp. 449–450, 1984.

[9] J. A. Palmer, “History and development of Environmental Education,” *Environ. Educ. 21st century*, 1998.

[10] E. L. de la Vega, “Awareness, knowledge, and attitude about environmental education: responses from environmental specialists, high school instructors, students, and parents.” University of Central Florida, 2004.

[11] H. A. Kruger and W. D. Kearney, “A prototype for assessing information security awareness,” *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006.

[12] M. Alavi and D. E. Leidner, “Knowledge management and knowledge management systems: Conceptual foundations and research issues,” *MIS Q.*, pp. 107–136, 2001.

[13] C. F. Camerer and R. M. Hogarth, “The effects of financial incentives in experiments: A review and capital-labor-production framework,” *J. Risk Uncertain.*, vol. 19, no. 1–3, pp. 7–42, 1999.

[14] L. K. J. Baartman and E. De Bruijn, “Integrating knowledge, skills and attitudes: Conceptualising learning processes towards vocational competence,” *Educ. Res. Rev.*, vol. 6, no. 2, pp. 125–134, 2011.

[15] W. A. Conklin, R. E. Cline, and T. Roosa, “Re-engineering cybersecurity education in the US: an analysis of the critical factors,” in *2014 47th Hawaii International Conference on System Sciences*, 2014, pp. 2006–2014.

[16] R. Prestwich and T.-M. Ho-Kim, “Knowledge, skills and abilities of international business majors: What we teach them versus what companies need them to know,” *J. Teach. Int. Bus.*, vol. 19, no. 1, pp. 29–55, 2007.

[17] H.-S. Rhee, C. Kim, and Y. U. Ryu, “Self-efficacy in information security: Its influence on end users’ information security practice behavior,” *Comput. Secur.*, vol. 28, no. 8, pp. 816–826, 2009.

[18] D. H. Tobey, “A vignette-based method for improving cybersecurity talent management through cyber defense competition design,” in *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, 2015, pp. 31–39.

[19] M. T. Dlamini, J. H. P. Eloff, and M. M. Eloff, “Information security: The moving target,” *Comput. Secur.*, vol. 28, no. 3–4, pp. 189–198, 2009.

[20] B. O. Newsome and J. A. Jarmon, *A practical introduction to homeland security and emergency management: From home to abroad*. SAGE Publications, 2015.

[21] J. Kaur and N. Mustafa, “Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME,” in *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 2013, pp. 286–290.

[22] A. H. Schoenfeld, *Problem solving in the mathematics curriculum: A report, recommendations, and an annotated bibliography*, no. 1. Mathematical Association of America, Committee on the Teaching of …, 1983.

[23] C. Wu, “The problems in campus network information security and its solutions,” in *2010 2nd International Conference on Industrial and Information Systems*, 2010, vol. 1, pp. 261–264.

[24] J. R. Ndiege and G. Okello, “Information security awareness amongst students joining higher academic institutions in developing countries: Evidence from Kenya,” 2018.

[25] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.

[26] A. Tsohou, M. Karyda, S. Kokolakis, and E. Kiountouzis, “Managing the introduction of information security awareness programmes in organisations,” *Eur. J. Inf. Syst.*, vol. 24, no. 1, pp. 38–58, 2015.

[27] R. Nilsen, “Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knowledge, Skills, and Abilities Necessary for Organizational Network Access Privileges,” 2017.

[28] T. Velki, K. Solic, and H. Ocevcic, “Development of Users’ Information Security Awareness Questionnaire (UISAQ)—Ongoing work,” in *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2014, pp. 1417–1421.

[29] R. V Krejcie and D. W. Morgan, “Determining sample size for research activities,” *Educ. Psychol. Meas.*, vol. 30, no. 3, pp. 607–610, 1970.

Ts. Haniza Nahar , a Senior Lecturer at University of Technical Malaysia Melaka (UTeM). She earned MSc. in ICT for Engineers (Distinction) from Coventry University, UK, and BEng. in Telecommunication from University Malaya. She used to be an Engineer and has been qualified for CFOT and IPv6 Software Engineer. Her postgraduate dissertation has been awarded as the ***Best Project Prize***.

Ts. Dr. Zulkiflee Muslim, a Senior Lecturer at University of Technical Malaysia Melaka (UTeM). He earned MSc. in Data Communication and Software from University of Birmingham City, UK and BSc. in Computer Science from University of Technology Malaysia. He has professional certifications: CCNA, CCAI, CFOT and IPv6 Network Engineer Certified.