Security Awareness Issue among Campus Network Environments

Najihah Osman[1], Zulkiflee M[1], Haniza N[1]
[1]Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka,
Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia
Email: zulkiflee@utem.edu.my

Abstract—In this era of globalization, security issues become important especially in a public network and Internet users significantly increased every single day. Most users are unaware of potential security issues such as malware and data exploitation when they use the Internet. Users with IT literate are considered fully aware of these Internet security issues. However, the reality indicates not all IT literate users are fully aware of the security issues. Hence, a study was conducted to prove whether people with IT literacy have higher awareness compared to people with non-IT literacy when it comes to security awareness. This paper is to study the level of awareness among students on security issues based on the Knowledge, Skill and Ability (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 these three (3) aspects. 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.

Index Terms—Security Issues, Campus Network, Awareness, Literacy

I. 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.

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].

In this paper, we investigate the level of security awareness among UTeM students. We conducted a survey 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.

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.

II. 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.

A. 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, [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.

B. 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.

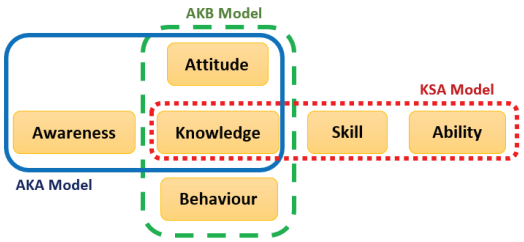

Fig. 1. Common Model of Study.

Each model has different purposes. For example, the AKA Model is used to determine *Awareness, Knowledge* and *Attitude* 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]. Reference [9] stated that these three are reoccurring concepts that are mentioned frequently in the literature, especially *Awareness, Knowledge* and *Attitudes*. According to [10], these three components, AKA play an essential role on the impact of students.

A study 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) [11]. Meanwhile,[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, KSA model is more suitable compared to AKA Model as KSA Model uses factor can assess the *Skill* factor along with *Knowledge* and *Ability* factors to measure the awareness for security issues.

a)*Knowledge*: [13] stated that cognitive psychologists have presented evidence that knowledge is the combination of declarative knowledge and procedural knowledge. Reference [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, [14] defines knowledge is a product of reciprocal and interpretative construction emerges from learners' participation in social practice. 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, [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*: [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.

C. Conceptual Operation Definitions

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 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 organizations. According to [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 I
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 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.

III. 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.

A. 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 emphasizing such as setting passwords is significant. Meanwhile, downloading software from the Internet may have hidden Trojan's virus, backdoors, and other malicious code. Therefore, many systems are invasive and used by the attacker.

[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. Reference [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, reference [27] investigated cybersecurity competency for the organization. There are many aspects of the knowledge, skill, and ability. It 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 proposed general framework as shown in Fig. 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.

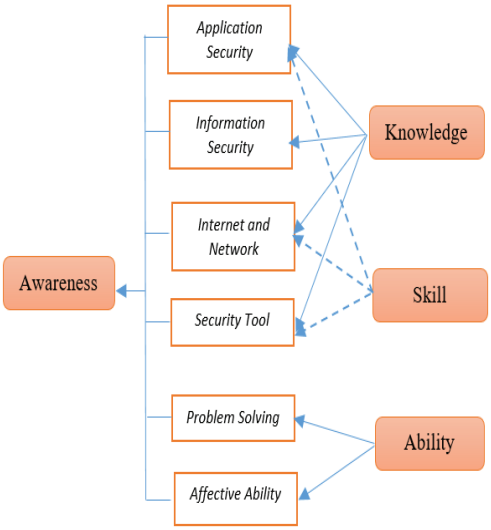

Fig. 2. A proposed framework of Security Awareness.

B. Research Process

For conducting the study, it has seen that Fig. 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.

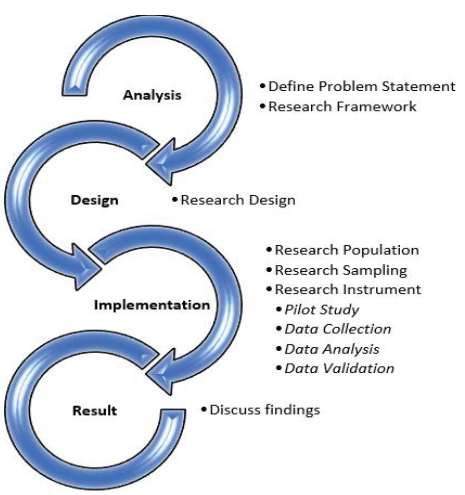

Fig. 3. Research Process.

For the implementation phase, the more significant number of UTeM respondents have undergone this survey. The survey task managed to take to gather 175 students to become respondents. The respondents were from various faculties. These respondents' background was determined based on the faculty of the respondent. These respondents managed to complete the questionnaire survey for further analysis.

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 as shown in Fig. 4. 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.

STATEMENT
(A) KNOWLEDGE
Security Tool
1. I have knowledge regarding when to physically lock my personal computer 1
2. I have knowledge to protect unauthorized access to equipment and resources and to protect personnel from damage or harm
Information Security
1. I have knowledge of information handling regarding not posting sensitive information to public domain
2. I have knowledge of information privacy regarding the consequences for violating information privacy laws
Internet and Network Security
1. I have knowledge regarding protection against phishing
2. I have knowledge regarding the purpose of spam
Application Security
1. I have knowledge regarding the definition of antivirus software
2. I have knowledge of password reuse regarding creating unique passwords for accounts or logins
(B) SKILL
Security Tools
1. I have skill in disabling wireless capabilities when the information security is using a LAN
2. I have skill in encrypting sensitive information when using a mobile device such as laptop
Internet and Network Security
1. I have skill in identifying and avoiding a malicious popup window
2. I have skill in identifying and avoiding dubious Websites
Application Security
1. I have skill in using an antivirus application to properly update the software when notified that antivirus requires an update
2. I have skill in avoiding downloading malicious code such as trojan horses
(C) ABILITY
Problem Solving
1. I am able to find an alternative solution when problem occur
2. I am able in implement action to solve the problems in a timely fashion
Affective Ability
1. I am able in representation of thoughts, feelings and ideas using symbols of the writer's language system for the purpose of communication or recording

Fig. 4. A sample of Security Awareness questionnaires.

For the content validation, the pilot study has been carried out to determine the validity and reliability of the 60 questions. Based on the results of the content validation, 12 questions have been 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. Finally, the statistical approach was used to analyze the results and propose the findings.

C. Sampling Process

A lot of survey was distributed and eventually 175 respondents who manage to complete the survey were collected. The strategies will be explained as Item Compilation and Scale Construction.

a) *Item Compilation*: The questions created and organized to reflect on the variables. The invalid variables were removed from the instrument while the remaining variables were reorganized.

b) *Scale Construction*: Likert scales has been used to measure the variables from (Strongly Disagree) 1 to (Strongly Agree) 6.

IV. 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 to obtain high-quality research results. The acceptable range is more than 0.65. For each domain, our values are more than 0.90 which means that our questionnaire items are very high reliability. After the validation process, the number of items has been deducted into 42 items as shown in Fig. 5.

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

Fig. 5. Content with Cronbach Alpha Size for Pilot Run

V. 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.

a) 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 TABLE 2. 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. The author has 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 compared to no job experience.

TABLE II
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. This survey is to distinguish between aware and unaware of the security issues among the respondent. The survey has defined that if the respondent able to obtain 7-10 score from the survey, then they will be labeled as an aware respondent. Meanwhile, if the respondent gets score 6 or less then they are labeled as an unaware respondent. Fig. 6 shows the result of the survey. From the survey among the 175 respondents, 109 respondent or 62 percent (%) of the respondents are aware of the security issues while only 38 percent (%) not aware of the issues. Thus, this indicates that majority of the UTeM students are aware of security issues.

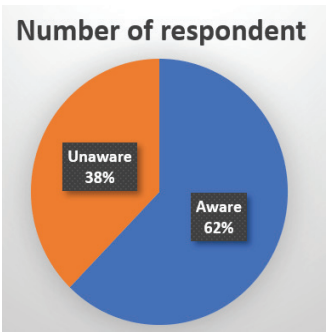

Fig. 6. Security Awareness Level based on the number of respondents.

c) Respondent Awareness by Demographic: Based on Fig. 7, 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 compared to females.

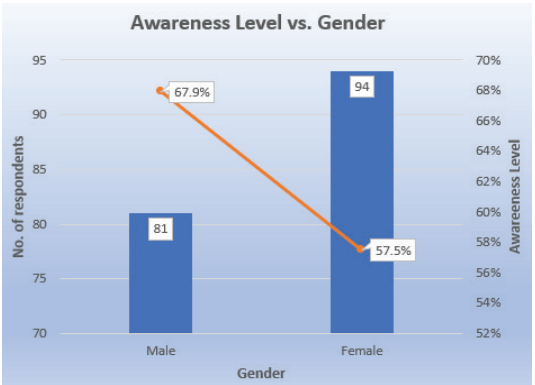

Fig. 7. The relationship between Security Awareness Level vs. Gender

Based on Fig. 8, 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.

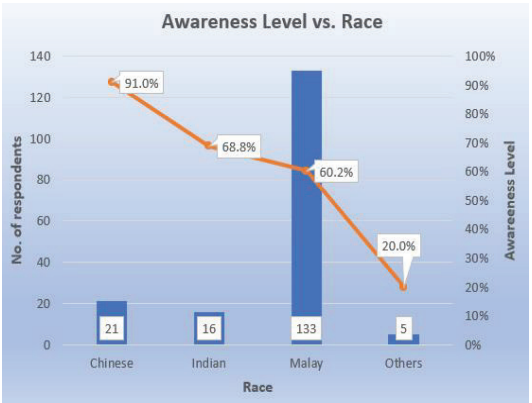

Fig. 8. The relationship between Security Awareness Level vs. Race

Based on Fig. 99, 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.

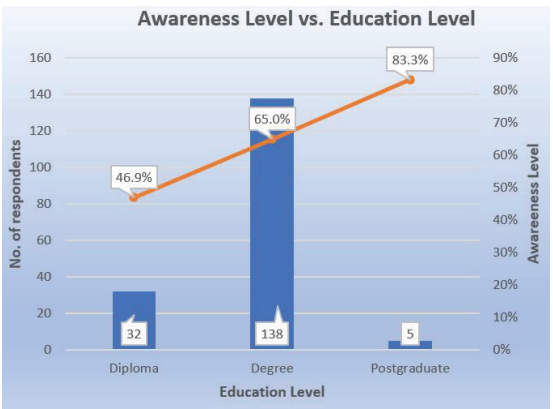

Fig. 9. The relationship between Security Awareness Level vs. Education Level

Based on Fig. 10, 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 histogram shows that students from FTKEE have higher awareness levels compare to students from FTMK. 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. This low level awareness does not mean the student is lack of IT technical competency but it rather indicates the awareness about security issues need to be emphasized although they have high IT technical competencies.

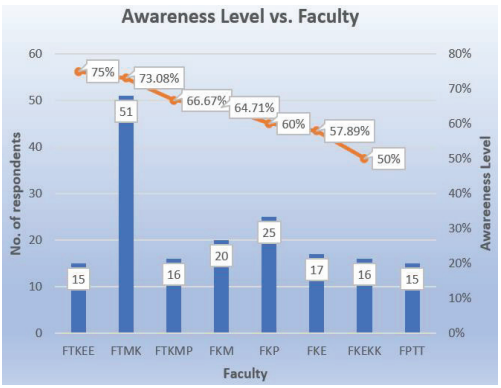

Fig. 10. The relationship between Security Awareness Level vs. Faculty

Based on 1, 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 compared 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.

Fig. 11. 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 Fig. 2. 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.

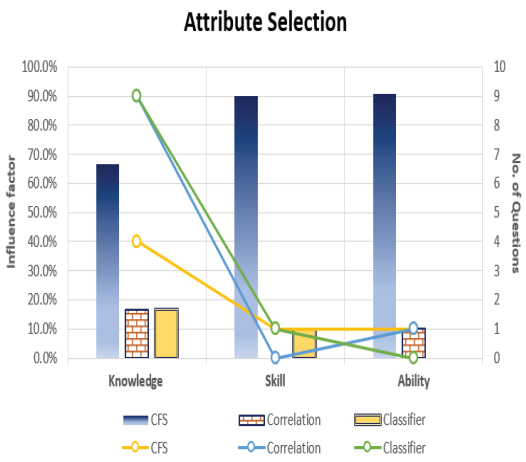

Fig. 12: The summary of Attributes Selection

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.

VI. Conclusion

From the conducted study, the result from the case study shows approximately 62 percentages (%) of UTeM students aware of Security issues. From the survey, the result shows that FKEKK students (non-IT literate) have higher awareness level compared to FTMK students (IT-literate). Even though FTMK students can be considered as IT-literate, but the awareness about security among FTMK students is still low. However, the result proves that the awareness level of security issues is regardless of the program they have enrolled in the university. Hence, the result indicates the necessary training is required to increase security awareness to all Internet users regardless their training background. For the future, a study about the most effective way to increase the awareness among the Internet users about security awareness should be addressed.

Acknowledgment

We would like to thank Research Group of Information Security Forensics and Computer Networking and Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Universiti Teknikal Malaysia Melaka and to all research members for their expertise and assistance throughout all aspects of our study.

References

[1] M. Gurunathan and M. A. Mahmoud, "A Review and Development Methodology of a LightWeight Security Model for IoT-based Smart Devices," International Journal Advanced Computing Science Application, 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," International Journal of Information Management, 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," Computer. Fraud & Security, 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," Computer Security, 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," Journal of 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," Computer Security, 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," Computer Security, 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," Journal Network Computing Application, 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," European Journal Information System, 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," Education Psychology Measure, vol. 30, no. 3, pp. 607–610, 1970.

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.

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***.

Najihah Osman received the Degree in Computer Science from Faculty of Information and Communication Technology (FTMK), Universiti Teknikal Malaysia Melaka (UTeM).