Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 9, Issue. 6, June 2020, pg.141 – 155

Measuring Cyber Security Awareness of Students: A Case Study at Fahad Bin Sultan University

Wejdan Aljohani[1]; Nazar Elfadil[2]

[1]College of Postgraduate Studies and Scientific Research, Fahad Bin Sultan University, KSA
[2]Computer Engineering Department, College of Computing Fahad Bin Sultan University, KSA
[2] nfadel@fbsu.edu.sa

Abstract— In this research paper authors designed questionnaire instrument to measure the current level of cyber security awareness (CSA) among Fahad Bin Sultan University (FBSU) students. The questionnaire is designed to fulfil the goals of this research project aims and objectives. The main goal of this paper aims to evaluate the level of cyber security awareness among FBSU students. Furthermore, cyber security students' awareness level questionnaire is adapted from few other cyber security awareness related questionnaires. A total of 212 students have participated in the survey. The study findings show that the students' awareness is in an average level and there is no difference in cyber security awareness level between male and female students. Furthermore, survey instrument's results indicate that the module has been effective in measuring students' awareness.

Keywords— Cyber Security Awareness (CSA), questionnaire, protection, Awareness behaviour

I. Introduction

Cyber security is defined as an information or data security that considers digital/computing devices as smart phones, computers, servers and Internet. Cyber security includes all elements of computer/network security that secure devices from unauthorized access, changes and destruction of information systems. With the widespread of computer utilization and dependence on Internet, cyber security is an important section of any information system.

Cyber security vulnerabilities are the elements that put a system or network at risk of being infected with malicious software. When one recognizes that a system was influenced by an assault, this illustrated that an assault on the framework occurred and being effective. This can be assumed that the system was powerless against the assault, then the expression vulnerability can be used to refer to the peculiarities of the framework that causes it defenceless against the assault or to refer to the gimmicks of all frameworks that causes them helpless against a comparable assault, or to refer to peculiarities of all frameworks that make them helpless against all assaults [1].

Malwares are utilized all over internet services to influence devices daily and carry out assaults that render devices, networks and data vulnerable. The Osterman research survey discovered that eleven million malware differences were detected by 2008 and ninety percent of these malware derived from concealed downloads from trusted and prominent sites. Network security is a huge referent question yet its political significance emerges from associations with the aggregate referent articles of “The State”, “The Society”, “The Nation” and “The Economy” [2].

A. Problem statement

IT represents all the technology available from hardware, software and all applied techniques such as communication. IT risks can be classified into three main types; namely: operational risks, security risks, and risks from the organization and people within it. With the increase in the spread and use of the Internet, those risks increased. In security risks, the computer infrastructures components may predispose a device at a risk. These components as software, hardware and network. Three elements to secure these components include accountability that is utilized to detect malicious elements, a perimeter defence system that is used for defence against the breach of infrastructure by malicious elements and an access control mechanism, that is used for authorization of incoming/outgoing data.

On the other hand, college students are the most groups that use a network, and they are supposed to be the most aware of cyber security, also cyber security awareness culture should be establishing from an early stage. Students are on this stage which is edge to enter the workforce. There is a great variety in the quality, capacity, importance, and nature of the students’ data, but no one denies the importance of preserving them, not change, falsifying or distorting them, and the importance of preserving even their formats and arrangement. It is a very sensitive nature and any slight change may cause many problems. IT systems, cyber networks need special treatment as they contain numerous data for students to be maintained and confidential, which are exposed to many threats. We need be to secure students data, we need to avoid these risks and their associated effects or at least minimize the effects of these risks. The unawareness of the students about threats and risks that can face them in cyberspace, can cause the successful execution of such threats. Students should establish a culture of awareness before entering the workforce. One of the most important steps in this way is the measuring of cyber security awareness of university students.

B. Research objectives

The end user is seen as a weak link. Therefore if students are not aware enough to recognize a security threat, they cannot be expected to avoid it, report it or remove it. Students are on the edge to enter the workforce, should be prepared and aware of security risks to avoid being a victim of cybercrime. Students need cyber security awareness. The aim of this study is to evaluate the level of information security awareness among university students. Online security, which is important in a society and has become a global village, must be at the front of every educational system so as to secure the safety within cyber environments.

C. The research questions

In this search we will try to focus on the importance of measuring the cyber security awareness of university students by answering the following questions.

Q1: How much do students know about information security?

Q2: What can be done to make sure students remain safe in online communities?

D. Research Hypothesis

Based on these research questions, the research hypotheses of this research can be summarized as follows:

H1: All university Saudi students use multiple digital devices on a daily basis, whether in social or academic tasks.

H2: Even with new systems been formed every day, systems that are supposed to be impenetrable and mainly safe from outside/inside assaults still fall victims of cyber-attacks, systems vulnerabilities are still exploited.

H3: Saudi students have sufficient awareness of cyber security risks.

H4: gender are determinant factors in the information security awareness level of students.

II. Background

Recently, new technologies are increasing and new forms of security compromises are being detected and there are also many ways in which users can maintain safe while traversing through the virtual surroundings. Authors [3] explained the relation between the growing rate of cyber connectivity in the world and increase of the vulnerable and susceptible to hacking activities. They summarized the increase of risks and decrease of cyber secure in five reasons as follows:

1. The progressions of organizations constantly have a confusing effect on the quality of an association's cyber security.
2. Mobile computing brought about the smearing of organizational limits, with IT getting closer to the client and further from the association, the information became more open all over the place.

3. Expanding of using the digital systems in our live is increasing the probability of the cybercrime in both the work and home environment
4. Cloud-based administrations, and outsider information management and storage, generate new channels of risks on the information.
5. New closed Infrastructure of operational technology systems pushed cybercrime to advance into these infrastructures such as systems of power generation, transportation frameworks, and other computerized closed systems.

There are several common methods of compromising known as hacking a system, they can be listed as [4]:

1. Malware: Is the most common threat to Cyberspace either by exploitation of vulnerable spaces or utilization of new technologies. There are bot executable, Trojans, viruses, worms rogue ware etc. All of these malwares may be loaded into systems through opening of tainted files or through accessing of infected websites. These will get the malwares downloaded into a system hence giving access to hackers. Victims of malware attacks are end-user systems, servers, network devices and process control system such as Supervisory Data Acquisition.
2. Denial-of-Service: Distributed Denial of Service (DDoS) has additionally developed over the long haul. DDoS assaults utilize multitudes of computers send multiple data packets at the same time to a target server to overwhelm and render it useless. They take advantage of the lack of security that the average computer user at home has, attackers have figured out how to plant dirty programming to surrender the remote control of home PCs programs.
3. Internet Protocol Spoofing (IP spoofing): is a technique used to make a PC system components communicate by adjusting the IP locations of the source component in the information parcels by supplanting them with false addresses. IP-spoofing makes a circumstance that breaks the ordinary relationship of trust that must exist between two components that communicate.
4. Spyware: Spyware is a type of malware that lodges onto computers. These soft wares have the ability to send information gathered from gaining access to a victims system from the host computer to other computers or take control of the victims' computer without their knowledge.
5. Bots: Bots are little programming that run robotized goals over the Internet. They run basic assignments that the individual would some way or another not need to perform. Botnets are intended to work so that the command centre has to come to PC and shared rapidly between different computers botted in the network. There are bots that harvest email addresses (spam bots), viruses and worms, file name comparisons, automated purchase of concert tickets, and bots that work with botnets, or coordinated attacks on networked computers [5].
6. Network Intrusion: A network intrusion is an unapproved entrance into a company's system, or an individual machine address in an appointed area. Intrusions can originate externally from a systems structure or internally such as a representative or client. A few intrusions are basically intended to tell the damaging your website with different sorts of messages or unrefined pictures. Others are more vindictive, looking to concentrate basic data like relationship that keeps on siphoning off information until it has found what it is looking for.

III.RELATED WORKS

The author [6] focused on studying student awareness at a higher academic institutionو when reveal that they engage with social media platforms. Their framework based on the most popular social media platforms which are Facebook, Twitter, LinkedIn and YouTube, they are widely used by users regularly. The author employed that University of Technology has accounts on these social media platforms to measure the awareness behaviour of students on cyber security. This study found that there is a lack among students to engage with cyber security awareness initiatives that are available. They suggested that academic institutions can make use of social media platforms to the awareness of students by providing cyber security awareness material on a regular basis to them.

A log analysts need good cyber situation awareness to perceive malicious activity, comprehend the impact and type of threat, and predict future consequences. The paper of [7] describes the development and validation technique to measure log analysts' situation awareness, especially when it comes to practical examples. The validation was conducted in a realistic setting by forming of two questionnaires designed for the two different roles in log analysis and during an exercise involving five professionals. The results suggest that the technique can be used to evaluate cyber situation awareness for log analysts to keep track of incidents. To address the same issue, a framework is proposed [8] to help network analysts to evaluate the security situation of the network and increase their awareness from three dimensions: threat, vulnerability and stability, and merge the results at decision level to measure the security situation of the overall network.

In Research [9], the security awareness of data in the Middle East area, especially in educational environments such as undergraduate students, researchers, academic staff and employee has been studied to analyse and understand the awareness level of IS in this environment. The results appeared that there is a clear lack of knowledge of IS principles, the participants do their daily work and practical application without the requisite knowledge and understanding of the importance of IS basics. The authors were interested with impacts associated security risks and lack of its awareness on the institutions. The paper set several recommendations to reduce the harmful of this situation, the important one of these recommendations was through supporting of training and awareness programs as well as adopting all the necessary safety measures at academic and employees of the institution to enhance security of their data. Other studies [10, 11, and 12] focus on the analysing and raising the awareness of cyber security on university students. Authors [13] attempted to measure the level of cyber security parental awareness to protect their children. A quantitative data analysis was performed using statistical software.

In research [14, and 15], employees are seen as the most vulnerable links, they need cyber security awareness and training to protect themselves and the company against new evolving cyber-attacks. An (Analyse -Predict-Aware-Test) APAT based Model along with Algebraic Equation has been adopted in developing a proactive approach towards enhancing the cyber security by making employees aware of new forms of security threats and what measures to follow when a suspicious activity is identified. Other researches [16, and 17] developed and validated a model which assists in reducing big data security and privacy risk caused by employee weakness.

In paper [18] the authors investigated the cyber security awareness of the public people in Saudi Arabia. The investigation was based on various aspects and contexts including demographics, cybercrime awareness, cyber security practices, and incident reporting as well as, a quantitative online, survey was conducted to collect information related to cyber security awareness in Saudi nationals. The results cleared that the Saudi citizens had a good knowledge of IT, but they have limited awareness of the threats associated with cyber as security practices, cybercrime, and the organizations and government roles in guarantee information safety across the Internet. Additionally, that Internet skills have an effect on cyber security practices from the users' end. The study recommended to develop a model to create cyber security awareness in the region in order to reduce cybercrime. In the same field, area (Middle East) and people culture but in a different country, Fadi [19] reviewed the need for security education, training, and awareness programs in United Arab Emirates. The study, involved and focused on the chances of the fall victims to phishing, a comprehensive wireless security survey of access points in Dubai and Sharjah and the Radio-frequency identification (RFID) security awareness. These determinants and aspects have been studied and discussed in Emirati the schools, universities, private and government organizations. Many countermeasures to rise the security awareness among students and professionals in UAE were reported. Recently, a study [20] includes and across four countries Palestine, Slovenia, Poland and Turkey in particular. To investigate of cyber security awareness, beyond the differences in respondent country or gender.

Many researches [21, and 22] set models to measure accurately and raising the awareness level according to the measurements as a key to be able to talk about effective information security against all types of attacks. These models defined awareness as a problem, not a solution, to solve this problem we must able to measure it and raising the awareness level according to the measurements. Dynamic model is superior to other models [23, and 24] because of it is designed in a stepped structure with levelling standardization, applicable to all groups/levels and capability based approach used. After displaying most of our research-related ideas, we see that there is a lack of addressing some of the concepts that we must deal with to measure, analysis the cyber security awareness of university students in Kingdom of Saudi Arabia.

IV. RESEARCH METHOD

As there is few IS (Information Security) awareness programs available for students globally, this research will discover the existing IS awareness programs available to students. It will also apply an in-depth survey for university students answer a questionnaire that includes questions about their basic online behaviors. This will be utilized to evaluate the awareness level of IS and factors affecting this among students. In this research, a number of hypotheses as age, gender might be determinant factors in evaluating the students' awareness level and apply an analysis to confirm these hypotheses.

1. Research Step One: To evaluate the students' awareness level depend on the results of the answered questions in the questionnaire and the hazards students face.
2. Research Step Two: To detect the factors influence the students' awareness level. The aim of research step one is to evaluate the students' awareness level and realize what it means. In the post-survey analysis, there will be a hierarchy grouping that will be utilized to investigate the analysis proceedings. The aim of research step two is to confirm the hypotheses in this research. The analysis tool will record the results of the survey which will investigate factors affect students and determines types of students' knowledge of IS.

For the purpose of this research, a survey will be carried out to evaluate cyber security threats. The survey targets University students, it is clear that students need to be educated about security issues early, the earlier they are aware of Information Security vulnerabilities, the safer they will be in the future as they will be able to pay more attention to security matters and also avoid engaging in illegal behaviour. The location, gender, age and department are all factors that may affect the security awareness level of the students, wherefore the questionnaire should be cover the students from different departments across different areas in KSA and age groups. The data from the questionnaire answered by the students will be used to determine how aware students are of Information security threats. In order to reach this goal, this study make use of a research methodology. This section discusses several methods that will be utilized in collecting information. This will be focusing on research designing, the population and sampling plan, questionnaire designing, data analysing. Fig. 1 shows the research flowchart.

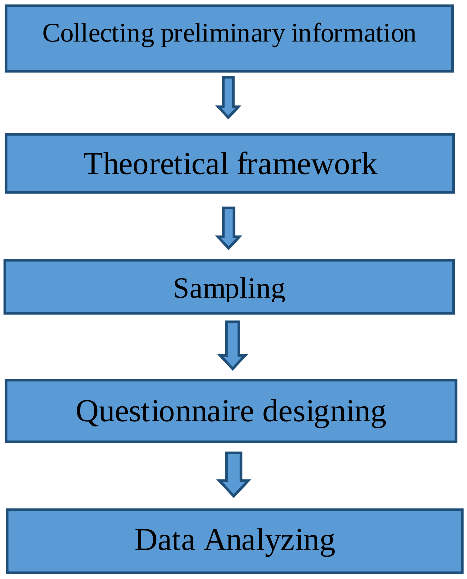

Fig. 1: Shows the research flowchart.

E. Research Design

Research design aims to fulfil the objectives of the research and find the solutions for research questions. This research used the quantitative design to offer a clear view of the security awareness level of the university students and it guarantees the validity and reliability of the research. In the quantitative design, the descriptive statistics are used to indicate the scores' distribution using a few indices. Structured questionnaire is conducted for data collection through online distribution. This method is preferred because it is fast and economic. The main steps can be listed as follows:

1. Students from different Universities and departments will be asked to take part in this survey.
2. Students will be evaluated based on what they have answered from the survey.
3. Survey will be carried out voluntarily.
4. Survey will be published on a web site page for a wider reach of students.
5. The questionnaire will require approximately 3 to 4 minutes to complete.
6. Survey was deployed 2 months.
7. Results will be discussed at the end of the Survey after online survey has being closed.

F. Data Sources

There are two sources of data collection were used in this study as the followings:

1. Secondary Data: the data was collected from websites, scientific researches, books, journals, articles and research. The main objective of collecting these data is to design a suitable, structured questionnaire that accommodates all aspects of the university students' awareness of cyber security.
2. Primary Data: the data was collected by developing a structured questionnaire to study, analyse and discuss Saudi university students' awareness of cyber security.
3. Information Security awareness of students is measured by Security Awareness survey. This survey will be used to ask students how they would respond to specific security related questions and situations. The results of this survey can be used to assess how vulnerable students are in terms of Information Security and what needs to be improved this done by computation of a risk score.
4. 212 questionnaires only were submitted, incomplete questionnaires containing ambiguous, chaotic answers or repeated responses from the same participant were excluded, so the valid response rate achieved was 89% (189) of the total sample.

G. *Data Analyses*

The research depended on the structured questionnaire as the main instrument for data collection, which was distributed on the research's sample to fill the required information. There are 56 questions in the Survey. The questionnaire comprised three sections.

1. **Section** 1: Personnel information: which contained the name which was optional, gender, department of the research's sample. Also, contained non optional questions to collect data on student behaviour and response to the most important sources of threats and common gaps in the cyber cloud.
2. **Section** 2: included several YES/NO Toggle questions which were used to clear and measure the cyber security awareness.
3. **Section** 3: The survey questionnaire included on the close-ended questions designed on a 3 scores Likert Scale as shown in Table 1. The positive Likert scale has been replaced by the negative, neutral or positive. This section targeted the student cyber security behaviour on online.

TABLE.1

THE SCORES OF LIKERT SCALE.

Disagree	Don’t know	Agree
-1	0	+1

Data analysis techniques intend to attain the objectives of the study and answer its questions. According to the appropriateness of analysis procedures to the study objectives and scale the variables, so the data analysis techniques are an essential section of the study. Descriptive statistics were used in this study to analyse the collected data. After the collection of questionnaires from respondents, the data was entered into the computer and processed by using the EXCEL.

V. FINDINGS DISCUSSION

For the purpose of this research, a survey will be carried out to evaluate cyber security threats. The survey targets University students, the data from the questionnaire answered by the students will be used to determine how aware students are of Information security threats. This section presents the statistical results which were collected from the questionnaire administered to sampled respondents at students to achieve the objectives of the study. Data was analysed by use of Excel Application to compute various statistics. The responses were collected and recorded to compute the frequencies and percentages of each question; as shown in Table 2. We selected descriptive statistic as analytical approach for analysing the collected data from the questionnaire.

TABLE 2

GENDER OF RESPONDENTS

Gender	Frequency	Percentage
Male	69	36.5 %
Female	117	62%
Prefer not to say	3	1.6
Total	189	100%

A. *Response Rate*

Information Security awareness of students is measured by Security Awareness survey. This survey will be used to ask students how they would respond to specific security related questions and situations. The researcher published this questionnaires by online. They requested from the respondents to fill the questionnaires and submit them immediately. Worth to mention that 212 questionnaires only were submitted, so the valid response rate achieved was 89% (189) of the total sample; as shown in Table 2.

B. *Statistical results*

The survey was posted on Google drive for duration of two months and students were asked to volunteer. There are 56 questions in the Survey. Each student answered all 56 questions of the survey. Each of these questions has a list of values, which indicates strong awareness and good security practice or weak awareness and bad security practice. Three groups have been set in our questions

1. Some questions have been assigned with true or false to analyse the concepts and awareness of cyber security.
2. Another questions group has been assigned a risk 3 values between -1, 0 and +1 (Agree, Don’t know and Disagree) based on Lekart scale but instead of positive scale the negative, neutral or positive, is used to trend to awareness, the results of these type questions can be used to calculate the overall sensitivity of risk level, vulnerability score of students [25] and they targeted to measure the cyber security behaviour on online. The cyber security behaviour on online can be calculated by, each questions’ risk value will be

multiplied by the number of times it was chosen by subjects. Each question express a cyber security behaviour on online. To determine the awareness of the risk level of each question, the cumulative response will be divided by the number of survey takers to calculate the students' awareness score of each question. The score is determine as given in Table 3.

3. Others had answers in closed list answers.

TABLE 3

AWARENESS SCORE ANALYSIS.

Students awareness score of risk level	**Description**
Low (10-25)	Students are aware of Security threats and how to mitigate them. They have knowledge of security standards and policies and also apply them.
Below Average (25-50)	Students are aware of security threats, have knowledge of security policies and standards but do not apply them.
Average (51-75)	Students are aware of security threats; they have no knowledge of security standards and policies but also do not take any measures against them or take part in activities that put them at risk.
High (76-100)	Students are not aware of security threats and policies. The take part in activities that can easily be used to exploit them.

The data gotten from the survey were downloaded into a excel file. The statistical output data was downloaded and converted into a word file. Below are the results from the analysis, frequency tables, statistics and charts. These results will be used to prove the awareness levels of students and what factors affect their awareness levels. Pie Charts depict the survey variables and the answers that the students chose. Table 4, which is a numerical representation shows the results of all 189 students, percent and our analysis/comments of their answer.

TABLE 4

CYBER SECURITY CONCEPTS AND AWARENESS PART.

Questions	**No%**	**Yes%**	**Analysis**
Do you have prior knowledge about cybercrimes?	40.74	59.26	There is general awareness and knowledge of cybercrime, but it is few and insufficient to develop an accurate visualization of the details of the types, outcomes and causes of each type.
Do you have sufficient information about cybersecurity and its roles?	57.14	42.86	
Do governments supervise the Internet?	11.64	88.36	It is clear that the government promoted well, in short time and through more than one track and method, the fact that it controls and supervises the information over the cloud, and that its supervision for the protection and maintenance of the law. As a result, a large sector believed in the importance of learning and understanding the concepts of cybersecurity
In your view, does a strict law reduce cybercrime?	13.76	86.24	
Does focusing on awareness and education reduce cybercrime?	23.28	76.72	
Do you have prior knowledge about Information Security?	30.16	69.84	It is clear that government interest, the industrial sector, work, as well as community culture have contributed to the use and exploitation of information technology and have become part of every student's daily life
Is your home computer connected to the Internet?	13.76	86.24	
Is the firewall on your computer enabled?	23.81	76.19	The results indicate suspicion and a high sense of fear of external threats, and on the other hand, lack of awareness and indifference to nearby or internal risks (surrounding people) represented by fraudulent reassurance of not using passwords and also lack of conviction of using two-factor authentication. This vulnerability needs a lot of effort to raise awareness about it because it stems from the culture of a society which is the most difficult factor in terms of the possibility of change.
Does anyone have your computer password?	30.69	39.31	
Is anti-virus currently installed into your computer are updated and enabled regularly?	35.98	64.02	
Do you use two-factor authentication, when possible?	46.03	53.97	
Are you backing up your files regularly?	41.80	58.20	There is awareness of the two most important vulnerabilities for data loss and penetration, but it is never sufficient, given that these vulnerabilities represent the largest percentage of causes of data loss and theft.
Do you connect your mobile device with public networks?	73.02	26.98	
You have been cyberbullied?	87.30	12.70	Religious and moral imperative interfered in limiting the cyberbullied phenomenon
Have you cyberbullied someone else?	93.65	6.35	
Someone else has pretended to be me online.	88.89	11.11	The result of answering the two interconnected questions shows the reality of the result, though this point needs to be measured continuously and continuously as a result of the development of cybercrime. This point needs to be studied more, the result may be due to ignorance of ways to know impersonation and may be realistic and true.
Have you pretended to be someone else online?	91.53	8.47	
Have you use the same password for everything that needs a password?	52.38	47.62	Insufficient awareness, and the concept of Human–Computer Interaction must be enhanced in terms of ease, flexibility and increased safety of password using and files management.

Do you check for viruses when you download a file or open an email attachment?	41.27	58.73	
Do you use instant messaging programs (for example: AOL, MSN, Yahoo, ICQ, etc.)?	64.02	35.98	I think that the result is not expressive and inaccurate. There are other applications that are very prevalent in the Saudi society, such as WhatsApp, Twitter and others. If it is correct, it is not required to move away from the modern applications of the cloud. The required is to increase awareness of security to use it

The next section explains the results of the cyber security behaviour on online. Table 5 lists the awareness score of each question based Table 3. Each question has risk weight value, to simplify, we set all question have the same weight so, we can calculate the all over awareness of student as the average of all awareness questions, it equals 56.40 %. The all over awareness score of Saudi student of the cyber security behaviour on online is a low rank (50-60) in "Average" level".

TABLE 5

AWARENESS SCORE OF THE CYBER SECURITY BEHAVIOUR ON ONLINE.

Questions	**The answer that tends awareness**		**awareness Score**
	answer	**%**	
Password doesn't follow keyboard pattern	Agree	56.08	Average
Password consists of lowercase, uppercase, numbers, special characters	Agree	88.36	High
Passwords longer than 8 characters	Agree	75.13	Average
Passwords based on personal information	Disagree	50.79	Below Average
Never change password	Disagree	63.49	Average
Usage of "Remember my password" option	Disagree	35.98	Below Average
Used to write down the password	Disagree	39.68	Below Average
Never use "hint" to recover forgotten password	Agree	33.86	Below Average
Established trusted online relationship with strangers	Disagree	62.96	Average
Ignored emails from well-known organizations announcement On something unusual or too good	Agree	52.91	Average
Respond to SMS announcing contests involving huge sums of money	Disagree	81.48	High
Never trust strangers information given on the Internet	Agree	70.90	Average
Never consider any amount of money for services offered by an online site	Disagree	21.16	Low
Willing to deposit money requested by online friends	Disagree	65.08	Average
Aware of and able to identify the latest online scams	Agree	48.15	Below Average
Trust strangers' pictures posted on the Internet	Disagree	71.96	Average
Never receive parcels and gifts from Internet friend	Agree	55.03	Average
Wouldn't hesitate to face-to-face with Internet friends	Disagree	42.33	Below Average
mean		56.40	Average

The next section will present the results of the questions of the closed list answer, as follows:

1. 98 of the students which is 51.85 percent of response total of the first question of this group "*When you receive a file that you are not expecting, you typically*" answered, "Delete the file immediately without opening it.", 41 of the students, 21.69 percent, answered "Open the file to see what it is." and 26 of the students, 13.76 percent answered "None of Above." as seen in Fig 2. Although the higher percent answer was in favour of students' awareness of the risk of cybersecurity, the opposite answer scored the second rate.

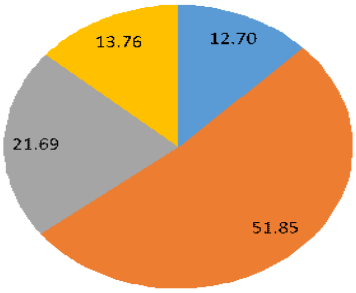

Fig. 2: When you receive a file that you are not expecting, you typically

2. Fig 3 depicts the graphical representation of variable 4 and the responses of the students. Out of the 189 students of the survey, 32 of them, as seen in table 2.6 answered "*No, I cannot do anything about it*" which is a 64.55 percent of the response total of the variable 4. 25.58 percent answered, "*Yes, I know what to do if my computer is hacked*". The result is good and reflects a high sense of being careful not to use passwords that are easy to expect.

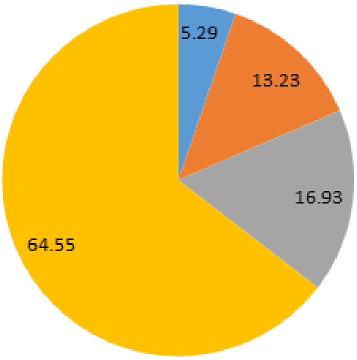

Fig. 3: An example of a good password

3. In Fig 4, 50.26 percent of the students answered "*Application*" that is, 95 out of the 189 students as seen in Fig while 24.34 percent of them answered "*Movies or songs*". These are realistic answers for a group of participants who are student and young adults.

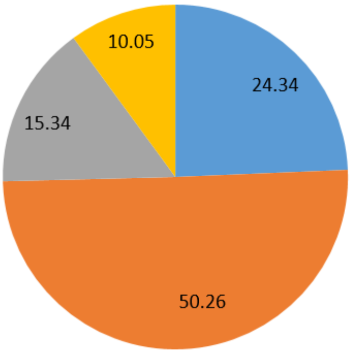

Fig. 4: Do you download from internet?

4. Students were asked in Fig 5 how regularly you update your antivirus. 61.38 percent answered "*Automatic update*" that is ideal answer but, it should have achieved more than this percentage. Also, the "*Never*" answer scored a large percentage against security cyber.

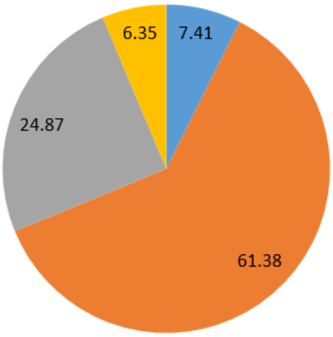

Fig. 5: How regularly you update your antivirus?

5. Fig 6 shows that 117 students, which is 61.90 percent of the students answered, "*I know very well what to share*" when asked what kind of information do you share on social media while 28 students, 14.81 percent answered, "*Everything*". The last percentage is very large because it represents the percentage of students who are easy to fall victim to multiple cybercrimes.

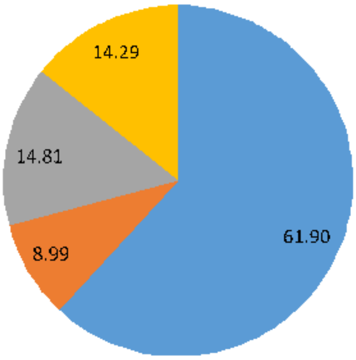

Fig. 6: What kind of information do you share on social media?

6. Fig 7 gives 49.74 percent, which is 23 of students answered "*Use the same password you used on other websites to make it easier remember*" to the question; When you open an account for a website? While 56 students, which is 29.63 percent answered, "*I create a strong password and keep it in the password management program*". In short, we must work hard to exchange these percentages.

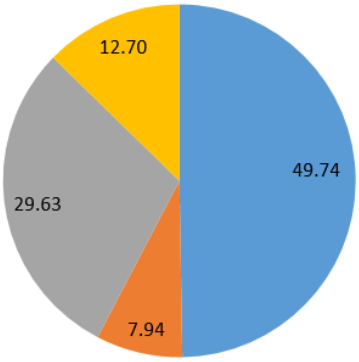

Fig. 7: When you open an account for a website

7. In Fig 8, Out of 189 students whom took part in the survey, 57 (30.16%) of the students gave an valid response which was "Check the site or link information before clicking on it with the mouse button". 75 (39.68%) They were too careful.

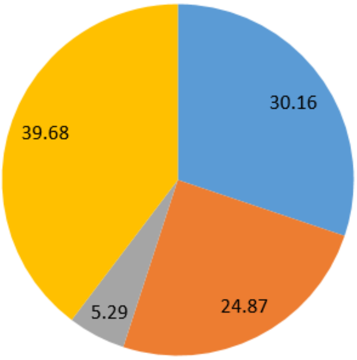

Fig. 8: When you receive an email containing links to external websites

8. As seen in Fig 9, students were asked to when you browse a bank or credit card purchase site. Fig shows that 111 of them, which is 58.73 percent of them answered, "*You check the link and the desired bank website*". With the continuous increase in electronic theft, this percentage should be increased, 39 students, 20.63 percent answered, "*You do not use banks over the Internet or other websites for financial transactions*", in the era of information technology, this rate should decrease to near zero.

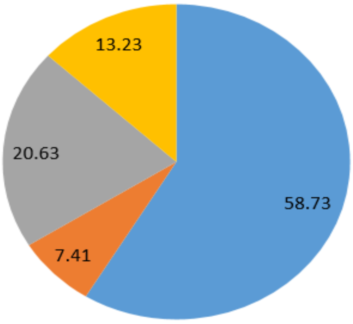

Fig. 9: When you browse a bank or credit card purchase site

9. Fig 10 depicts the response of students to the question; "*When you heard about a program and want to try it, and I have searched through the internet browsing sites and found a trial version of the program on the unknown website* ", 46.03 percent of the students answered, "*You never download or install the program*". 30.16 percent answered "*You search for program information before downloading it*". The two percentages indicate that there is sufficient awareness among students.

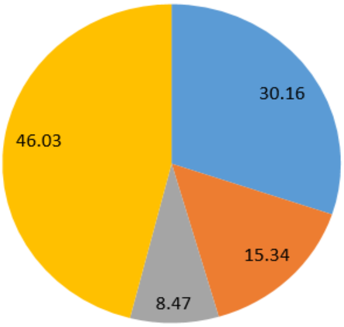

Fig. 10: When you heard about a program and want to try it, and I have searched through the internet browsing sites and found a trial version of the program on the unknown website.

10. As seen in Fig 11, students were asked You found a USB flash drive while going to work, 52.91 percent did not know hence answered "*None of above*", all previous answers were against information security, so this result is very good.

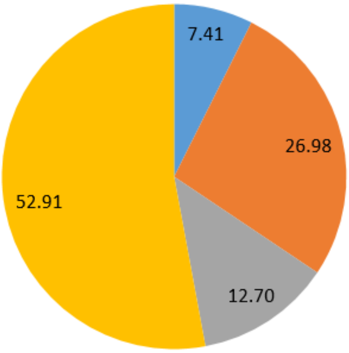

Fig. 11: You found a USB flash drive while going to work

11. Fig 12 asked the students in the survey, "*You were in desperate need of an internet and found a free Wi-Fi hotspot without a password*", unfortunately, the worst and most dangerous answer "*Connect to it and browse the internet*" was the highest percent (47.62%).

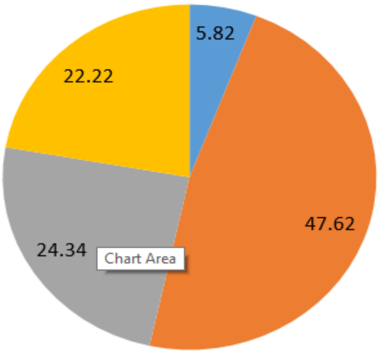

Fig. 12: You were in desperate need of an internet and found a free Wi-Fi hotspot without a password

12. As seen in Fig 13, answered, "*I ignore the message, and download an antivirus program from a trusted site*" scored 118 (62.43%) students, 11.11 percent answered, "*You directly download the advisable program to protect your device*" that is, the sum totalled 73.54 percent, and 4 students, This means good awareness of students of the risks the message of "*appearance a window appeared on your personal computer announcing that there is a group of viruses need to be removed*".

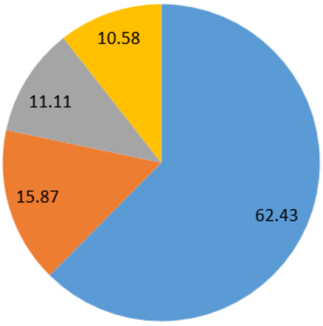

Fig. 13: anti-virus program and remove it from your computer.

13. Figs 14, 15, and 16 represent questions that allow students to choose more than one answer, authors can consider them in the same direction, and Table 5 listed the higher percentage answers for these 3 questions. Nevertheless, Table 6 listed the higher percentage answers of closed list answer questions. All of them indicate a significant awareness among Saudi students regarding to:

Q1- Which of the following actions have you ever taken to keep yourself safe online?
Q2- Where would you get helpful advice about staying safe online?
Q3- What are top the three things that you do most often while online at home?

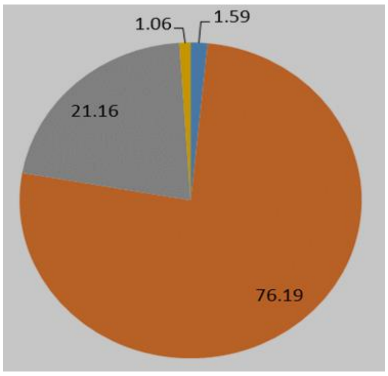

Fig. 14: How regularly change the computer/ mail password

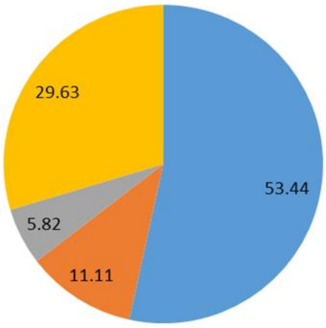

Fig. 15: How can your society being protect against cybercrime?

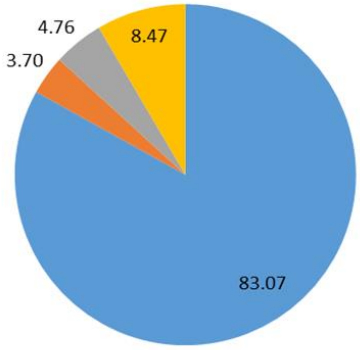

Fig. 16: Which of the following cause's people fall victim to cybercrime?

TABLE 5

LISTED THE HIGHER PERCENTAGE ANSWERS OF OPEN QUESTIONS.

Answer	Related question	percentage
Updated my passwords	Q1	70.37
Only visited websites if I know and trust them	Q1	19.58
Friends, social worker / support worker	Q2	33.86
Websites or apps	Q2	21.16
Browsing website	Q3	52.38
Chatting with friends	Q3	32.80

TABLE 6

LISTED THE HIGHER PERCENTAGE ANSWERS OF CLOSED LIST ANSWER QUESTIONS

Questions	The answer that tends awareness %	awareness Score
When you receive a file that you are not expecting, you typically	51.85	Average
When you receive a file that you are not expecting, you typically	64.55	High
Do you download from internet?	50.26	Average
How regularly you update your antivirus?	61.38	Average
What kind of information do you share on social media?	61.90	Average
When you open an account for a website	49.74	Below Average
When you receive an email containing links to external websites	39.68	Below Average
When you browse a bank or credit card purchase site	58.73	Below Average
When you heard about a program and want to try it, and I have searched through the internet browsing sites and found a trial version of the program on the unknown website.	46.03	Below Average
You found a USB flash drive while going to work	52.91	Average
You were in desperate need of an internet and found a free Wi-Fi hotspot without a password	47.62	Below Average
Anti-virus program and remove it from your computer.	62.43	Average
How regularly change the computer/ mail password	76.19	High
How can your society being protect against cybercrime?	53.44	Average
Which of the following cause's people fall victim to cybercrime?	83.07	High
Mean	**57.31**	Average

VI. CONCLUSION

The objective of this research study was to measure students' cybersecurity awareness level. The study elaborates on the literature related to cyber security awareness among university students. For this purpose a questionnaire instrument was developed. The developed questionnaire focussed on students' awareness as part of the information security concepts. Yet, developed questionnaire intend to measure cyber security awareness level.

Nevertheless, paper findings indicate that students had average levels of awareness with regard to cybersecurity concepts. Worth to mention that students' awareness levels did not differed significantly in terms of gender, and student's class level. This study recommends necessary policy measures to be taken by FBSU to ensure that students from all batches have same level of cyber security awareness.

Cyber security awareness (CSA) is normally neglected by educational institutes. University students should be aware of the possible threats that can face them while using the internet. Therefore, a culture has to be established for students in order to be able to identify possible threats. This culture should be establishing from an early stage. Furthermore, students should be well prepared and aware of security measures that users can apply to avoid being a victim of cybercrime.

REFERENCES

[1] Campara, N. M. (2010). System Assurance: Beyond Detecting Vulnerabilities . Morgan Kaufmann.

[2] Singer, P. F. (2013). Cybersecurity and Cyberwar: What Everyone Needs To Know. Oxford university Press.

[3] Kessel, P.v. and K. Allan, "Get ahead of cybercrime", EY's Global Information Security Survey, 2014.

[4] David Willson, "Cyber Security Awareness for CEOs and Management", Elsevier, 2016.

[5] Rouse M., 2005, http://searchsoa.techtarget.com/definition/bot, [accessed 6 May 2020].

[6] Pieter Potgieter, "The Awareness Behaviour of Students On Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology, " Kalpa Publications in Computing Volume 12, 2019, Pages 272-280 Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019.

[7] Patrik Lif, Magdalena Granåsen, Teodor Sommestad, " Development and validation of technique to measure cyber situation awareness, " 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 19-20 June 2017.

[8] Xi Rongrong, Yun Xiaochun, Hao Zhiyu, " Framework for risk assessment in cyber situational awareness, " IET Information Security, Volume: 13, Issue: 2, 3 2019. https://doi.org/10.1049/iet-ifs.2018.5189

[9] Samaher Al-Janabi, Ibrahim AlShourbaji, "A Study of Cyber Security Awareness in Educational Environment in the Middle East, " Journal of Information & Knowledge Management, Vol. 15, No. 1, 2016. https://doi.org/10.1142/S0219649216500076

[10] Eyong B. Kim, "Information Security Awareness Status of Business College: Undergraduate Students, " Information Security Journal: A Global Perspective, Volume 22, Issue 4, 2013. https://doi.org/10.1080/19393555.2013.828803

[11] Yesem Kurt Peker, Lydia Ray, Stephanie Da Silva, Nathaniel Gibson, Christopher Lamberson, "Raising Cybersecurity Awareness among College Students, " Journal of The Colloquium for Information System Security Education (CISSE) September 2016.

[12] Senthilkumar .K. and Sathishkumar Easwaramoorthy, "A Survey on Cyber Security awareness among college students in Tamil Nadu, " IOP Conf. Series: Materials Science and Engineering 263, 2017. https://doi.org/10.1088/1757-899X/263/4/042043

[13] Nazilah Ahmad, Umi Asma' Mokhtar, Wan Fariza Paizi Fauzi, Zulaiha Ali Othman, Yusri Hakim Yeop, Siti Noru, "Cyber Security Situational Awareness among Parents, " 2018 Cyber Resilience Conference (CRC), Nov. 2018. https://doi.org/10.1109/CR.2018.8626830

[14] Aamir Hussain Khan, Parul Bahl Sawhney, Sangeeta Das, Darshana Pandey, "SartCyber Security Awareness Measurement Model (APAT)". 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), Feb. 2020.

[15] Grayson Kemper, "Improving employees' cyber security awareness, " Computer Fraud & Security, Volume 2019, Issue 8, Pages 11-14, August 2019. https://doi.org/10.1016/S1361-3723(19)30085-5

[16] Gundu, T. (2019). Big Data Big Security and Privacy Risks: Bridging Employee Knowledge and Actions Gap. International Journal of Cyber Warfare and Terrorism (IJCWT), 1-16.

[17] Lee Hadlington, "Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom, "International Journal of Cyber Criminology, Vol 12 Issue 1, June 2018.

[18] Faisal Alotaibi, Steven Furnell, Ingo Stengel, Maria Papadaki, "A survey of cyber-security awareness in Saudi Arabia, " 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Dec. 2016. https://doi.org/10.1109/ICITST.2016.7856687

[19] Fadi A. Aloul, "Information security awareness in UAE: A survey paper, " 2010 International Conference for Internet Technology and Secured Transactions, Nov. 2010.

[20] Moti Zwilling, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetin, and Hamdullah Nejat Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, " Journal Of Computer Information Systems, Vol. 60, 2020. https://doi.org/10.1080/08874417.2020.1712269

[21] Ashish Malviya, Glenn A. Fink, Landon Sego, Barbara Endicott-Popovsky, "Situational Awareness as a Measure of Performance in Cyber Security Collaborative Work, " 2011 Eighth International Conference on Information Technology: New Generations, April 2011. https://doi.org/10.1109/ITNG.2011.161

[22] Maria Evangelopoulou, Christopher W. Johnson, "Empirical framework for situation awareness measurement techniques in network defense, " 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), June 2015. https://doi.org/10.1109/CyberSA.2015.7166132

[23] Salih Erdem Erol, Seref Sagiroglu, "Awareness Qualification Level Measurement Model, " 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Dec. 2018.

[24] S S Tirumala, Maheswara Rao Valluri, GA Babu, "A survey on cybersecurity awareness concerns, practices and conceptual measures, " 2019 International Conference on Computer Communication and Informatics (ICCCI), Jan. 2019. https://doi.org/10.1109/ICCCI.2019.8821951

[25] Human, s. t. (2012). *Security Awareness Survey*. Retrieved from SANS: https://www.sans.org/sites/default/files/2018-01/security-awareness-survey.pdf