Cybersecurity and Multidisciplinary Students: A Survey

Hina Irfan, Kashmala Jamshaid Akhter, Ramsha Shakeel

Abstract— The exponential growth of the Internet interconnections has led to a significant growth of cyber-attack incidents often with disastrous and grievous consequences. As more and more people are connected over the Internet, understanding all levels of users including both experts and non-experts in computing system and devising security mechanisms corresponding to their confidence levels is a biggest challenge as new attack patterns in emerging technologies such as social media, cloud computing, smartphone technologies are used to exploit personal security but there's also a lack in awareness in people specially in students which led them being **exploited by others. In our survey, we intended to identify the awareness in cyber security among university students which belongs to different domains. We collected data from 203 students from different areas of Pakistan. After data collection, results** were analyzed and discussed. It's concluded that cy**bersecurity awareness programs should be organized as cyber-attacks are increasing day by day and students should properly be educated.**

Index Terms cybersecurity, cyber awareness, cyber awareness assessment, security risks, University students.

1 Introduction

The term 'Cybersecurity' is not bound to a specific definition, it has been addressed differently by many researchers. By studying different literature reviews some researchers think that it's protection of end-users and their assets from online threats whereas some think that it's lack of security[1]. Cybersecurity is a practice of defending electronic systems, servers, data and networks from malicious attacks. There are multiple layers of protection spread across the systems to keep data secure from harmful attacks. Attackers are becoming innovative day by day so implementing cybersecurity has become more challenging.

Cyber-attacks flourish because they are more convenient, cheaper than physical attacks. Cyber criminals do not have to use a lot of money for their cyber-attacks. They are difficult to track as they know how to escape from being tracked or identified due to anonymous nature of internet. Cyber-attacks are increasing rapidly. Youth is an easy target to cybersecurity threats as they surf many social and gaming sites. They unknowingly download files which contain malicious data and viruses that affect their systems. Many gaming websites offer games which contain viruses and malicious functions (BBC, 2012). Once the malicious files are downloaded, they can cause severe damage to the system and data. Important files can get corrupted or may get into dangerous hands. To deal with these threats, colleges and universities should organize cybersecurity awareness programs.

- *Hina Irfan currently pursuing Master's degree in Computer Science at Bahria University, Karachi, Pakistan. E-mail: hinairfanbutt1992@gmail.com*
- *Kashmala Jamshaid Akhter currently pursuing Master's degree in Computer Science at Bahria University, Karachi, Pakistan. E-mail: kashmala_jamshaid@yahoo.com*
- *Ramsha Shakeel is currently pursuing Master's degree in Computer Science at Bahria University, Karachi, Pakistan. E-mail: ramsha.shakeel@hotmail.com*

Colleges and Universities are lacking in cybersecurity awareness and education among students of different domains. Students should be continually educated of cyber-attacks and online risks as practices and interest of users change with time. This survey intends to identify the cyber security knowledge and its awareness in higher education students in Pakistan and the behavior of patterns represented by students in different domains (such as Computer Science and BBA students). The survey is based on both qualitative and quantitative questions and it will seek to answer the following research question by comparing different researches done by the researchers i.e. What is the current state of cyber security behavior in the aspects of malware, password usage, phishing, social engineering and online scam among higher education students in Pakistan?[2].

Further, our research will be divided in two major characteristics:

1. Role of University in providing courses in rising of cybersecurity awareness.
2. Source of knowledge used as for cybersecurity for best practices such as People tend to search on their own information related to cybersecurity area on the Internet or asking other users.

Why Youth a Prime Target?

Hackers may pick anyone or any company as their target but many of them pick youth as their target. The following are the reasons why youth are prime targets:[3]

1. They've low motivation to follow security guidelines
2. Children and youth have high level of trust for others
3. Lack of knowledge may push them to act spontaneously while browsing the web.

International Journal of Scientific & Engineering Research, Volume 11, Issue 4, April 2020
ISSN 2229-5518

2 LITERATURE REVIEW

Cyber security is an important issue which is affecting Internet users throughout the world and is main issue in Pakistan as well, this study aims to explore the cyber security behavior among Youth especially students. Because, Higher education students are usually aged between 18-25 years. Previous literature indicates that basic security requirements are CIA triad Figure 1. According to Adams, Serb & Weippl, Confidentiality refers to the protection of user's sensitive information from being recovered by unauthorized persons. To protect this information, techniques are used such as encryption and authentication. Integrity refers to the protection of data from unauthorized changes, where access control is the main feature to maintain integrity in the e-learning environment. Availability means the readiness for correct service [4-6]. Bada & Sasse in 2014 highlighted that if security practices are too inefficient or tough, users will try to avoid the controls in place, which can also reduce the efficiency of previous and current awareness drives. Influencing strategies are required to the knowledge transfer and awareness in order to positively alter behaviors and attitudes [7]. For training purpose, Peltier found that a baseline of the cybersecurity perception levels, behaviors are required to guide the training [8]. An exploratory study of college students by Mensch and Wilkie in 2011 found that a false sense of security, in relation to personal information protection, is created by the installation of security applications and tools [9].

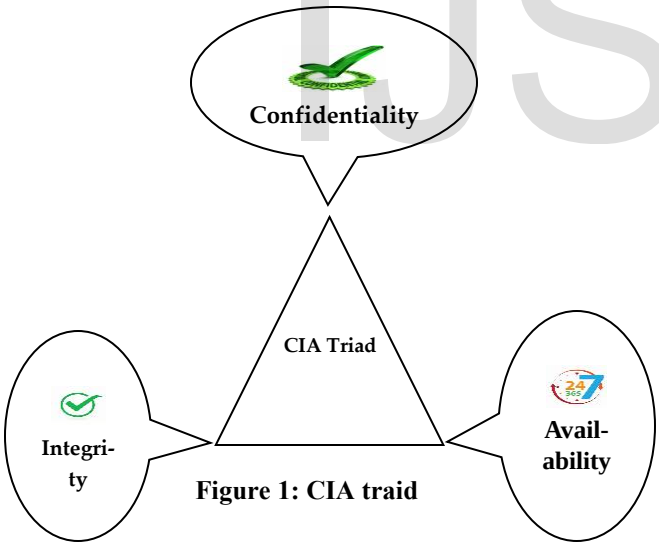

Figure 1: CIA traid

Aliyu et al. found that university students in Malaysia were major violators of computer beliefs and security, as students are irresponsible sometimes while posting content or browsing any data and sometimes involve in illegal usage via sharing and downloading software's, movies and funny clips. Due to a variety of factors including idleness and economic standing, the students were found that they are not practicing safe computing[10]. In 2015 a Malaysian Communications and Multimedia Commission conducted a survey which concluded that among respondents 62.5% were in universities or colleges, 34.90% in secondary school, while 2.40% of them were in primary schools and 0.20% in others. Although cyber security awareness is an important topic to discuss, especially for students involved in higher education. College students and those students who are taking online classes or enrolled in programs are the main target for phishing attacks as they spent most of their time on the internet to do research work or communicate with their fellow students for queries and performing different activities. This supports the fact that higher education students are heavy Internet users as compared to students at the primary or secondary level[11]. Nowadays academic institutions are preparing their students about their careers but are not focusing on the fact that they should start campaigns supporting the information security awareness due their assumptions that employers will train their employees about cybersecurity issues and their solutions. Sekyere highlighted that students from their intermediate level may have some basic knowledge about information security, as they are not associated with an organizations' security practices. So, educational institutions should provide proper training to students in order to create a continuous secure behavior in the future[12]. In 2015 Pretorius and Van Niekerk recommended awareness training and campaigns after observing weaknesses in industrial control systems due to doubtful password management of user's, remaining software patches, and out-of-date or uninstalled anti-virus. These studies further illustrate how there can be misalignment among cybersecurity attitudes, knowledge, and behavior[13].

Butler and Butler in 2014 conducted their survey in South Africa and concluded that they consider suitability a priority element over security as only 23% of users change their passwords on daily basis whereas 70% of users representing that it is good practice[14]. In 2014 Pramod and Raman conducted their study which concludes that higher education students are not unaware of security concerning smartphones, but they are not fully aware of the security risks and its practices[15]. A study that was conducted by the National Cyber Security Alliance (NCSA) and sponsored by the Microsoft Corporation found in today's digital times where technology is advancing schools are not well prepared to create awareness among students regarding online information sharing, security (U.S. Schools Not Preparing Kids for Digital Age, 2013). In 2014 Kim found that college students in the US did not participate in training programs started to support information security. Another finding of this study was that the students' needed to participate more in these types of programs to be well aware of information security issues[16].

3 METHODOLOGY

We performed a survey analysis to provide a deeper insight into the user's behaviors and expectations specially students from different age groups about cybersecurity. The form of survey is the online questionnaire. It is a collection of questions that are being prepared and circulated to a large number of chosen participants. Below Figure 2 illustrates the process of online survey.

International Journal of Scientific & Engineering Research, Volume 11, Issue 4, April 2020
ISSN 2229-5518

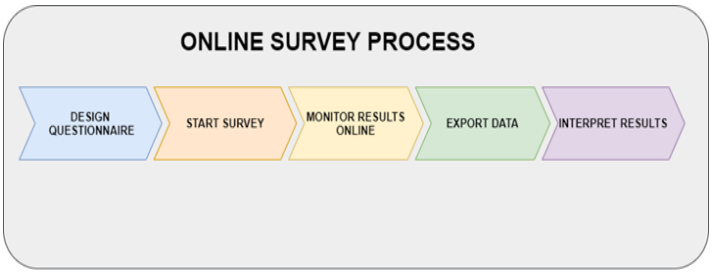

Figure 2: Online survey process

The population is the whole category of people we're involved in digging at. The survey is a demographic sub-set, which is the real number of exams. In our survey we tried to do the overall student survey belongs to various universities as a population and we set a sample size of 203 students who are taken randomly from two major provinces of Pakistan such as Sindh as major focus is institutes all over Karachi having students belonging different fields of education. As far as sample taken from Punjab is based on random cities to somehow check the awareness pattern in other cities as well. But the main objectives of the research is to identify: (1) University position in offering awareness-raising courses on cybersecurity and (2) Base of expertise used as cybersecurity for best practices including users continue to check on the Web for their own information relevant to the cybersecurity field or question other people is our main focus of study.

4 SURVEY METHODS AND TOOLS

This research approach is focused on survey questions called "Survey on Cybersecurity Awareness among multidisciplinary students" to investigate and find out the extent of understanding of cybersecurity among the citizens of Pakistan belonging different domains of education. These survey questions are sent to the students through Google online survey forms. This study would aim to address the following research question by comparing multiple work that the respondents have done which is: What is the current state of cyber security activity among students in Pakistan especially higher education students in the areas of malware, password use, phishing, social engineering and online scam? The survey questions cover four sections A. Participant educational backgrounds B. Cybersecurity Practices C. Cybercrime Awareness and D. Incident Reporting. The questionnaire was spread to individuals of different educational backgrounds. Support was taken from individuals and social networking sites to meet the public. A nonprobability sampling technique for snowball (also known as chain sampling, chain-referral sampling, referral sampling) was often used for entering the public. Audiences were told cordially to spread the survey. A nonprobability sampling technique snowball (also known as chain sampling, chain-referral sampling, referral sampling) has also been used to meet the population. Audiences were asked to share the survey cordially[17]. The of using snowball sampling technique is that it helps experiments to take place where otherwise, due to a lack of participants, it would be difficult to perform. Audiences were cordially invited to spread the survey link (google forms) to members of their families, acquaintances and colleagues. To maximize test participants, the Snowball sampling methodology was acquired in this way. In order to find out results, a total of 203 questionnaires were compiled and analyzed. The study was targeted at people who are under 18 to 50 years of age and have limited computer literacy schooling as this work centered on the extent of consumer understanding in cybersecurity.

5 DISCUSSION

A. PARTICIPANT EDUCATIONAL BACKGROUNDS

Figure 4 Figure 3illustrates the total number of percentage of participants involved in the research having 44.8% males and 55.2% females. The majority of the participants, i.e., 63.1%, were 18-24 years old. 28.6% belongs to 25-34 years of age group, 7.9% of age group 35-50 and rest were under 18 as shown in Figure 3

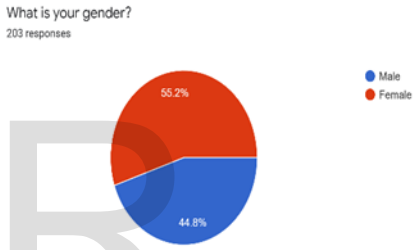

Figure 3: Gender wise percentage of participants involved in the survey

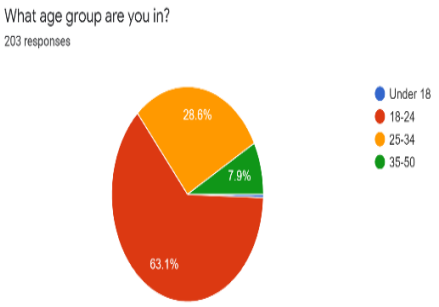

Figure 4: Participants age group

The participants belong to different knowledge areas in order to identify its awareness in multidisciplinary students. 30% of the participants belongs to Computer Science/IT, 28% of the participants belongs to Finance/Marketing/HR/Accounting/Supply Chain, 7% of the participants belongs Software engineering, 7% of the participants belongs to Psychology, 4% belongs to electrical engineering, 2% belongs to Math's, and 1% belongs to Media sciences, 5% participants didn't chosen any majors and rest of 16% participants belong to different domains including Biomedical

International Journal of Scientific & Engineering Research, Volume 11, Issue 4, April 2020
ISSN 2229-5518

engineering, Civil Engineering, Maritime, Graphic designing, Microbiology, Chemistry, Zoology, Social Sciences, Engineering, Networking and Fashion Designing. Below Figure 5 demonstrates the knowledge area of participants obtained by asking open-ended question regarding there majors.

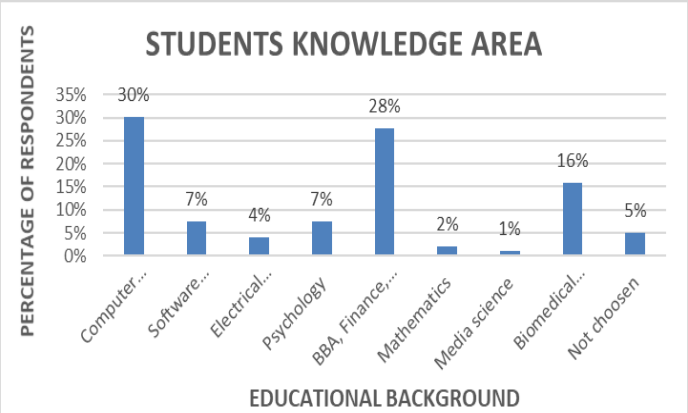

Figure 5: Participants knowledge area

B. Cybersecurity Practices

The main purpose of this section is to know how much students are aware of cybersecurity, from where they learn about cybersecurity and whether university is providing enough knowledge about cybersecurity or not. Figure 6 shows awareness of cybersecurity among students concluded that 51.7% participants responded that they know about cybersecurity whereas, 46.3% knows a little bit and remaining 2% are still not aware of cybersecurity. Figure 7 illustrates the fact that if participants are aware of cybersecurity so from which source, they get this information out 203 participants 58.1% responded that they got cybersecurity information from Internet, 18.7% participants heard it from their friends and 18.7% heard it from their respective universities.

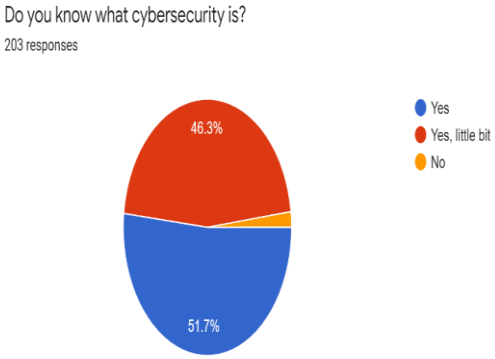

Figure 6: Cybersecurity practices

In this section the main question arise is whether universities are providing enough knowledge about cybersecurity to their students irrespective of their departments or not. So, according to the participants 34.5% responded that they are neither agree nor disagree with the question, 30% responded that universities are providing enough knowledge, and according to 30% participants universities are not providing knowledge about cybersecurity. As shown in Figure 8.

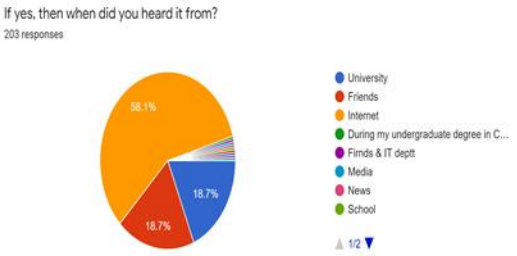

Figure 7: Source of information

Figure 8: University providing awareness

C. Cybersecurity Awareness

This section comprises of the questions about cybercrime awareness how well students are aware of cybercrime which windows they are using, and do they use firewall or any other software to overcome security issue. We asked the participants which windows they are using among 203 participants, 66.5% responded that they use windows 10, 12.8% are using windows 8 and 16.3% are using windows 7 shown in Figure 9.

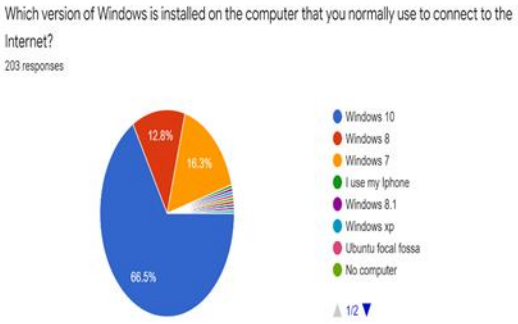

Figure 9: Windows version installed

According to Figure 10, 56.7% participants responded that their antivirus software updated automatically, 18.2% said they never updated the antivirus software installed in their PC's, Laptops. 16.7% occasionally, when they remember to update their antivirus software. When asked about VPN usage 40.9% Responded that they do not use VPN, whereas 34% uses VPN and according to 9.4 they don't know whether they are using VPN or not in Figure 11.

International Journal of Scientific & Engineering Research, Volume 11, Issue 4, April 2020
ISSN 2229-5518

Figure 10: Updating antivirus software

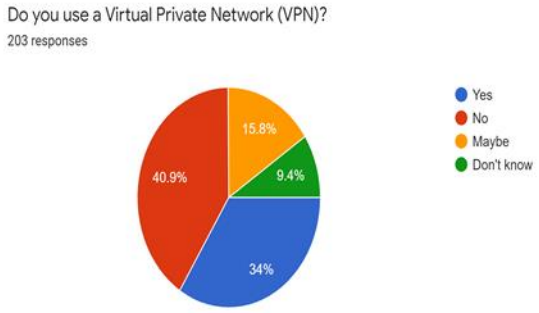

Figure 11: VPN Usage

When asked about their information and how they think information sharing is secure online or not? Figure 12 shows that 47.8% participants out of 203 responded it is not safe to share information online whereas 41.9% responded it is safe and 7.9% do not know about it.

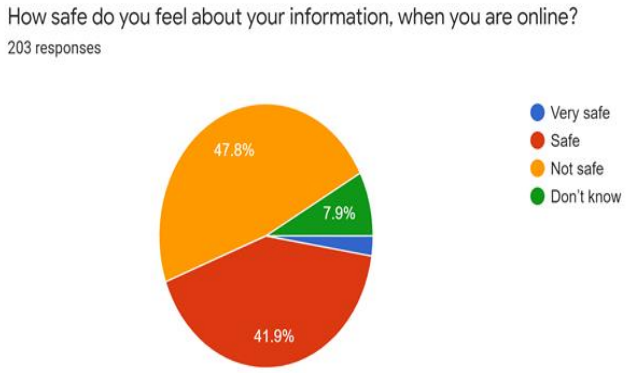

Figure 12: Information Security

D. Incident Reporting

In incident reporting section we ask from the participants how many times they face issues regarding cybersecurity and what could be the major security risks. Figure 13 Shows the situations which a user might face when using their system i.e. effecting by trojan or malware, inappropriate email generation, social media profiles misuse, files hacking. So, 48.8% responded they never experienced these situations, 27.6% experienced trojan or malware attack their system, 26.6% said mails generated automatically in their mailbox and 7.9% their profiles being hacked.

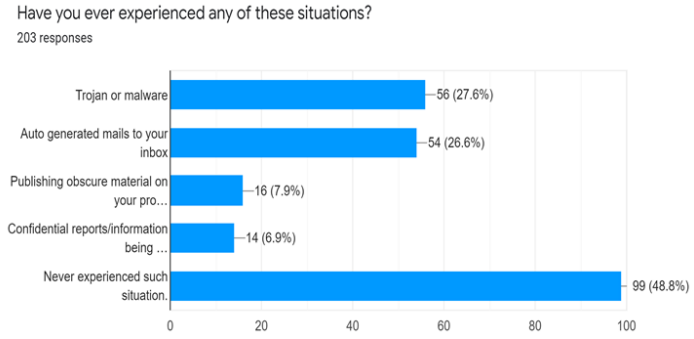

Figure 13: Security Issues

When asked from the participants how many times they have been victim of any cybercrime activity and have they reported them as well, as shown in Figure 14, 75.9% responded that they never face such problem whereas 14.3% claim that they became victim 1-time, and few said 2-5 times, and out of 203 82.3% said they never reported cybercrime incident, approx. 11 % claim that they have reported cybercrime incidents. Figure 15.

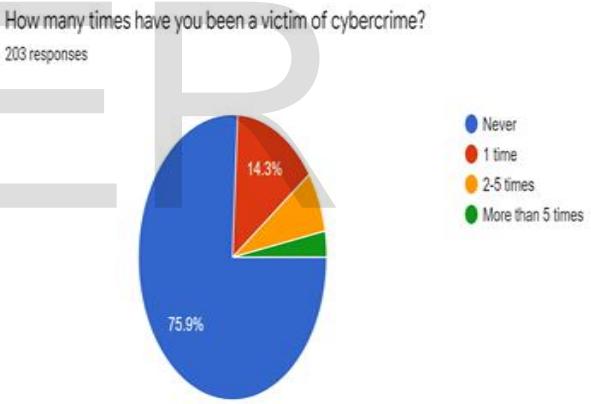

Figure 14: Cybercrime Victim

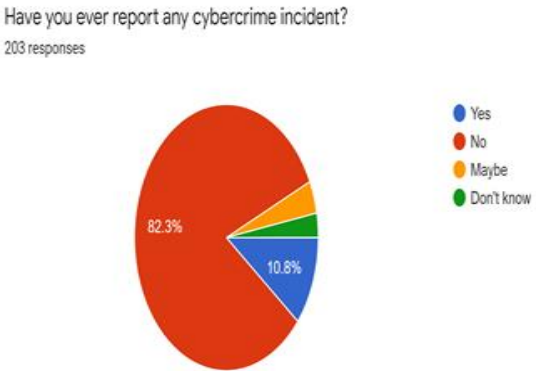

Figure 15: Reported Cybercrime incident

According to the participants in Figure 16 with 40.9% the greatest security risks are the files which we download from internet because few files are harmful for our system, 31.5%

International Journal of Scientific & Engineering Research, Volume 11, Issue 4, April 2020
ISSN 2229-5518

hacking attempts caused by hackers, 7.9% said it would be malware or any other virus and 10.8% have no idea about the security risk.

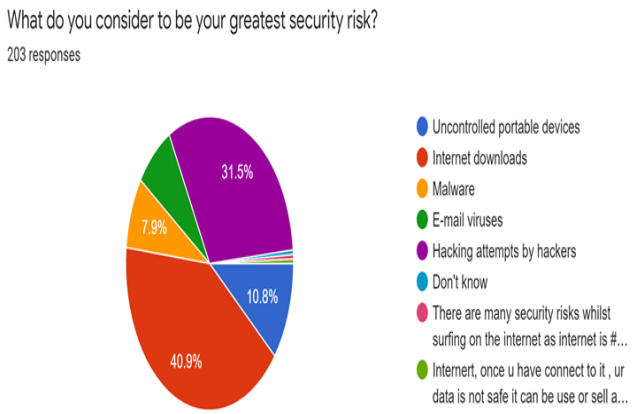

Figure 16: Security Risk

6 Conclusion

Therefore, after conducting the survey we concluded that students are well aware through internet instead of universities providing sufficient knowledge. From incident reporting section it is concluded that students are aware of the possible issues which will occur while using internet and publications on magazines, websites create awareness among students. Moreover, about cybersecurity awareness programs majority of the Participants said, there should be session where experts could talk about the generic risks every individual can counter if they are not well aware of these situations and these programs should definitely be taught in universities, as this issue has now become common so one should know how to deal with it. So, universities need to arrange seminars, short courses for students to become fully aware of cybersecurity.

Acknowledgements

We would like to thank our Instructor, Sir Muhammad Iqbal, Assistant Professor, Department of Computer Science, Bahria University Karachi, Pakistan. For his support in our Research Writing. This research would not have been possible without his guidance. We would also like to appreciate the support and great love of my family and all those who have taken part in this work.

References

[1] A. A. Al Shamsi, "Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE," *International Journal of Information Technology and Language Studies,* vol. 3, 2019.

[2] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences,* vol. 80, pp. 973-993, 2014.

[3] D. T. Smith and A. I. Ali, "YOU'VE BEEN HACKED: A TECHNIQUE FOR RAISING CYBER SECURITY AWARENESS," *Issues in Information Systems,* vol. 20, 2019.

[4] A. Adams and A. Blanford, "Security and Online Learning: To Protect and Prohibit," in *Usability evaluation of online learning programs*, ed: IGI Global, 2003, pp. 331-359.

[5] J. L. N. M. IACOB, "Information security management in e-learning," *Knowledge horizons,* vol. 5, 2013.

[6] E. R. Weippl and M. Ebner, "Security privacy challenges in e-learning 2.0," in *E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education*, 2008, pp. 4001-4007.

[7] M. Bada, A. M. Sasse, and J. R. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?," *arXiv preprint arXiv:1901.02672,* 2019.

[8] T. R. Peltier, "Implementing an Information Security Awareness Program," *Information Systems Security,* vol. 14, pp. 37-49, 2005.

[9] S. Mensch and L. Wilkie, "Information security activities of college students: An exploratory study," *Journal of Management Information and Decision Sciences,* vol. 14, p. 91, 2011.

[10] M. Aliyu, N. A. Abdallah, N. A. Lasisi, D. Diyar, and A. M. Zeki, "Computer security and ethics awareness among IIUM students: An empirical study," in *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010*, 2010, pp. A52-A56.

[11] L. Muniandy, B. Muniandy, and Z. Samsudin, "Cyber Security Behaviour among Higher Education Students in Malaysia," *J. Inf. Assur. Cyber Secur,* vol. 2017, pp. 1-13, 2017.

[12] B. O. Sekyere, "Studying Information Security Behaviour among Students in Tertiary Institutions," ed, 2015.

[13] B. Pretorius and B. Van Niekerk, "Cyber-security and governance for ICS/SCADA in South Africa," in *Proceedings of the 10th International Conference on Cyber Warfare and Security*, 2015, pp. 241-251.

[14] R. Butler and M. Butler, "An assessment of the human factors affecting the password performance of South African online consumers," in *HAISA*, 2014, pp. 150-161.

[15] D. Pramod and R. Raman, "A study on the user perception and awareness of smartphone security," *International Journal of Applied Engineering Research, ISSN,* pp. 0973-4562, 2014.

[16] E. B. Kim, "Recommendations for information security awareness training for college students," *Information Management & Computer Security,* 2014.

[17] N. Ahmed, U. Kulsum, M. I. B. Azad, A. Z. Momtaz, M. E. Haque, and M. S. Rahman, "Cybersecurity awareness survey: An analysis from Bangladesh perspective," in *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, 2017, pp. 788-791.