International Journal on Applications in Engineering and Technology
Volume 9 : Issue 2 : April 2023, pp 8 – 13 www.aetsjournal.com ISSN (Online) : 2455 - 0523

CYBER SECURITY AWARENESS IN ONLINE EDUCATION A CASE STUDY ANALYSIS

P. NATARAJAN , MAHENDRAN

***Abstract*—** This study presents to what extent Kyrgyz-Turkish Manas University students are knowledgeable about cybersecurity in the distance education process. The survey was conducted with a sample of 517 students from all faculties of the university at the undergraduate, graduate, and PhD levels. Our research study shows that although huge numbers of cyberattacks are occurring around the world, the students did not have any knowledge about cybersecurity and the effects of cyberattacks overall. An analysis of cybersecurity awareness was undertaken by asking questions focused on malicious software, password security, and social media security. Although we live in an age of technology where our entire lives are indexed to the internet through the distance education process, it has been determined that students have a weak cybersecurity awareness. It has been further concluded that cybersecurity education should be given to prevent the students from becoming a victim of cyberattacks, helping them to use the internet more effectively.

I. INTRODUCTION

With the spread of technology and the penetration of the internet into every aspect of daily life, cyber security has begun to be of great importance for both individuals and states alike [1]. Although these innovations have made our lives easier, the increase in cyber attacks has made it necessary to take measures in this area [2]_[4]. In addition, one of the most basic points is that the types of cyber attack, in other words the malicious use of cyberspace, have changed in the last 20 years. This has led to the use of new ``cyber'' concepts and risks in the literature [5].

A cyber attack is defined by Hathaway *et al.* as follows: ``A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose'' [6]. The most basic question to ask is `Does this definition define cyber attacks today?' Today, saying that cyberattacks are carried out only for political purposes is insufficient when it comes to trying to understand the nature of cyber attacks. This is because new cyber concepts have emerged that have changed the nature of cyber attacks. What remains similar is the use of computers in attacks. In this context, cybercrimes are defined as crimes committed through computers [7]. The Department of Justice of the USA defines a cybercrime as ``any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation or prosecution'' [8].

On the one hand, it is important to explain what cyber security is. Although the concept does not have any common definition, the International Telecommunication Union (ITU) defines cyber security as ``the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment'' [9].

Although there are now more complex structures in cyber attacks and cyber security compared to the past, the ability to perform cyber attacks has developed. The capacity to learn through websites that almost every computer user can access has increased. This is especially so the new generation, called the Z generation. They are often completely involved with computer technologies and can easily perform any activity they want by using it [10]_[13].

P.Natarajan , Assistant Professor , Department of Computer Applications , Erode Sengunthar Engineering College (Autonomous), Perundurai , Erode.
(Email : palanisamynatarajan50@gmail.com)

Mahendran , PG Scholar , Department of Computer Applications, Erode Sengunthar Engineering College (Autonomous), Perundurai , Erode.

On the other hand, this situation has also led to the emergence of new situations regarding computer technologies, or cyber security awareness as it is called in the literature. Although the Z generation has grown up with the internet and with computer technologies, sometimes they do not know what kind of problems they may encounter or they do not know how to deal with the problems arising from the continual development of internet technologies [14], [15].

Cyber security awareness, or information security awareness, has become an important issue today. The number of studies on this subject, which affects every aspect of daily life, is increasing. First of all, defining cyber security awareness is important to better gain a full understanding of the subject. Shaw *et al.* defined the concept as; ``the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks" [16]. As can be understood from the definition, the important points are evaluated in two ways. Firstly, it emphasizes the importance and responsibilities to do with information security. Secondly, it is aimed at knowing and applying information security control practices at an adequate level to protect the information.

Hwang *et al.* defined information security awareness as a phenomenon that aims to enable users to recognize the security vulnerabilities or problems that may arise and to respond in an appropriate way. Naturally, it also intends to keep the security phenomenon on the internet at the forefront of the user's minds [17]. Khan *et al.* made similar points to Hwang. Khan *et al.* defined information security awareness as the fact that users have information about security and act within the framework of the known rules [18]. Zilka, on the other hand, defines cyber security awareness as a phenomenon that aims to increase the level of knowledge about the online applications that users use so then they can stay safe in response to online risks [19]. Within the framework of these definitions, it can be clearly seen that security awareness training should be provided to improve cyber security awareness [20].

Within the framework of this information, it will also be questioned what kind of information the students have about cyber security awareness during the online education period and whether they want to receive training in this direction. The second aim of this study is to obtain data for use by further studies on how students can increase their cyber security awareness based on the theoretical framework findings.

II. OBJECTIVE DEDUCTION AND OVERVIEW

Our research study shows that although huge numbers of cyberattacks are occurring around the world, the students did not have any knowledge about cybersecurity and the effects of cyberattacks overall. An analysis of cybersecurity awareness was undertaken by asking questions focused on malicious software, password security, and social media security. Although we live in an age of technology where our entire lives are indexed to the internet through the distance education process, it has been determined that students have a weak cybersecurity awareness.

Naturally, it also intends to keep the security phenomenon on the internet at the forefront of the user's minds [17]. Khan *et al.* made similar points to Hwang. Khan *et al.* defined information security awareness as the fact that users have information about security and act within the framework of the known rules [18].

III. LITRETURE SURVEY:

Technology has developed rapidly in the last three decades. With the beginning of the millennium, the rate of the use of the internet has also increased and is now more than 50 % [21]. Although people use the internet and technology in their routine, they do not know how to protect themselves from the possible risks associated with technology and the internet. Especially today, given the Covid-19 pandemic, the education process has started to be carried out through the online system of distance education. This situation has also led to the beginning of a new era for students and the creation

of activities on cyber awareness. Although the students' use of online education platforms is through programs determined by the universities themselves, students may also be the target of cyber attackers due to services such as the unconscious use of the internet, downloading software from illegal sites, or not updating their software, social media accounts, and internet banking. Today, cyber-attackers send more spam emails, try to manage network traffic, and even access user information by hijacking personal computers with files that they send to individual email accounts [22]. For this reason, it is necessary to engage in cybersecurity awareness studies focused on students [23], [24]. Several studies have been conducted to measure the level of cybersecurity awareness among students and academics. For example, Ismailova and Muhametjanova [23] studied the cybercrime risk awareness in the Kyrgyz Republic with 172 participants. The results show that the students were not familiar with cybercrime. Another survey was done in New Zealand in 2016 to measure cybersecurity awareness among individuals between the ages of 8-21. This was conducted by Trimula, Sarrafzadeh, and Pang. According to the authors, most of the students were not aware of the presence of cyber threats and they did not know the term cybersecurity [25]. Ahmed et al. examined the cybersecurity awareness of the people of Bangladesh [26]. Their research states that the sample did not have enough information about cybersecurity. The authors made a recommendation that a guide should be prepared so then people can become consciously aware of cybersecurity [26]. The Department of Computer Science at Yobe State University conducted a survey that showed that although the students were aware of cybersecurity, they did not know how to protect the data that they have [27]. Today, social media accounts are very popular among students. Sometimes people can be defrauded and their information stolen through their social media accounts. Kirwan et al. conducted a study on this subject involving Malaysian students. They investigated whether the sample of students knew about this subject and whether they had been the victim of this type of fraud [28]. The results of their survey showed that more than 30% of students had been a victim of a social networking site scam [28]. Senthilkumar and Sathiskumar surveyed cybersecurity awareness among college students in Tamil Nadu. They found that the students were able to protect themselves from cyber threats [29]. Zwilling et al. conducted a survey among undergraduate and graduate students. The survey was conducted on students from various countries [1]. The results revealed that internet users are aware of cyber risks and simple precautions are taken by them. The authors claimed that there is a link between cyber awareness and cyber knowledge [1].

IV. EXISTING SYSTEM

Several studies have been conducted to measure the level of cybersecurity awareness among students and academics. For example, Ismailova and Muhametjanova [23] studied the cybercrime risk awareness in the Kyrgyz Republic with 172 participants. The results show that the students were not familiar with cybercrime.

Another survey was done in New Zealand in 2016 to measure cybersecurity awareness among individuals between the ages of 8-21. This was conducted by Trimula, Sarrafzadeh, and Pang. According to the authors, most of the students were not aware of the presence of cyber threats and they did not know the term cybersecurity [25].

Ahmed *et al.* examined the cybersecurity awareness of the people of Bangladesh [26]. Their research states that the sample did not have enough information about cybersecurity. The authors made a recommendation that a guide should be prepared so then people can become consciously aware of cybersecurity [26]. The Department of Computer Science at Yobe State University conducted a survey that showed that although the students were aware of cybersecurity, they did not know how to protect the data that they have [27].

Today, social media accounts are very popular among students. Sometimes people can be defrauded and their information stolen through their social media accounts. Kirwan *et al.* conducted a study on this subject involving Malaysian students. They investigated whether the sample of students knew about this subject and whether they had been

the victim of this type of fraud [28]. The results of their survey showed that more than 30% of students had been a victim of a social networking site scam [28].

Senthilkumar and Sathiskumar surveyed cybersecurity awareness among college students in Tamil Nadu. They found that the students were able to protect themselves from cyber threats [29]. Zwilling *et al.* conducted a survey among undergraduate and graduate students. The survey was conducted on students from various countries [1]. The results revealed that internet users are aware of cyber risks and simple precautions are taken by them. The authors claimed that there is a link between cyber awareness and cyber knowledge [1].

Disadvantages

- ❖ The system is not implemented SECURITY VULNERABILITIES AND CYBER THREATS.
- ❖ The system is not implemented AWARENESS OF CYBERCRIMES AND LAWS.

V. PROPOSED SYSTEM

Cybersecurity awareness, or information security awareness, has become an important issue today. The number of studies on this subject, which affects every aspect of daily life, is increasing. First of all, defining cybersecurity awareness is important to better gain a full understanding of the subject. Shaw *et al.* defined the concept as; ``the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks" [16]. As can be understood from the definition, the important points are evaluated in two ways. Firstly, it emphasizes the importance and responsibilities to do with information security. Secondly, it is aimed at knowing and applying information security control practices at an adequate level to protect the information.

Hwang *et al.* defined information security awareness as a phenomenon that aims to enable users to recognize the security vulnerabilities or problems that may arise and to respond in an appropriate way. Naturally, it also intends to keep the security phenomenon on the internet at the forefront of the user's minds [17]. Khan *et al.* made similar points to Hwang. Khan *et al.* defined information security awareness as the fact that users have information about security and act within the framework of the known rules [18].

Zilka, on the other hand, defines cybersecurity awareness as a phenomenon that aims to increase the level of knowledge about the online applications that users use so then they can stay safe in response to online risks [19]. Within the framework of these definitions, it can be clearly seen that security awareness training should be provided to improve cybersecurity awareness [20].

Advantages

- ➢ Before measuring the level of awareness of an ordinary computer user about the risks of cyberattacks, it is important to determine whether they have basic security knowledge. For this reason, while creating the framework of this survey study, an attempt was made to understand whether the basis of possible unawareness in relation to the field of cybersecurity is a lack of knowledge.
- ➢ Since it is predicted that most of the participants are a population that uses passwords, has social media accounts, and installs various software on their computers, the questions were chosen in this direction

VI. SYSTEM IMPLEMENTATION:

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Login, View All Users, Add Category, View Attack Type Hash code, View All Datasets, View All Attacks By Chain, View Attacks Size Results, View Education Level Size Results, View Institution Size Results

A. View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user’s details such as, user name, email, address and admin authorizes the users.

B. End User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like Register and Login, View Your Profile, Upload Datasets, View All Datasets, Find Attack Type.

VII. CONCLUSION

When the results of the survey conducted involving Kyrgyz Turkish Manas University students were examined, it could be seen that the majority of the students did not have sufficient knowledge about internet use and cyber threats. At the same time, they were found to lack technical knowledge of many issues including whether the websites they visit have security certificates or whether their information can be stolen by a hacker through deception. Since cyber threats affect people from all educational backgrounds, it would not be appropriate to provide this information only in the departments that provide technical education. The results of this study also show that the students who received cyber security education were more competent in terms of computer use and basic network security subjects. Almost all of the students who did not receive the education were eager for the same education. The study revealed that taking this education would be beneficial to the students to help them use the internet more securely. Cyber security awareness training can not only teach the students to be prepared for possible cyber threats but also inform them about the legal dimension of cybercrime.

The awareness levels can be re-measured after basic cyber security training is given to the students as a pilot application in future studies. Cyber skills can be tested through hands-on activities where the effects of the training can be explored. The same study can also be repeated with different demographics, for example, with students from a different country. In this way, it can be understood whether the lack of cyber security awareness is a regional or local problem. Apart from this, future studies may offer possible solutions by measuring the proficiency of the students or a different demographics in specific areas such as social media, password security, and malware.

This study, in its current form, has some limitations as it only measures the cyber security awareness of the students from a certain university based on a questionnaire. This study can be re-evaluated by adding other methods such as interviews and assessment/evaluation exams. More qualitative and quantitative results will be useful to increase the reliability of the study. After adding new methods, the framework of the study can also be visualized to increase its readability and coherence.

Ethical Statement: This study was approved by the Faculty of Economics and Management of Kyrgyz Turkish Manas University document number R.30.2021/IBF-1745. (03/02/2021).

Conflict of Interest: The authors declared there to be no conflict of interest.

VIII. REFERENCES

[1] M. Zwilling, G. Klien, D. Lesjak, .. Wiechetek, F. Cetin, and H. N. Basim, ``Cyber security awareness, knowledge and behavior: A comparative study," *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 82_97, Jan. 2022.

[2] A. A. Karim, P. M. Shah, F. Khalid, M. Ahmad, and R. Din, ``The role of personal learning orientations and goals in Students' application of information skills in Malaysia," *Creative Educ.*, vol. 6, no. 18, pp. 2002_2012, 2015.

[3] N. Kaloudi and J. Li, ``The AI-based cyber threat landscape: A survey," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1_34, Jan. 2021.

[4] J. Jang-Jaccard and S. Nepal, ``A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973_993, Aug. 2014.

[5] G. Pogrebna and M. Skilton, *Navigating New Cyber Risks: How Businesses Can Plan, Build and Manage Safe Spaces in the Digital Age*, London, U.K.: Palgrave Macmillan, 25, Jun. 2019.

[6] O. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, and J. Spiegel, ``The law of cyber-attack," *California Law Rev.*, vol. 100, no. 4,817-885, 2012.

[7] F. Forester and P. Morrison, *Computer Ethics*. Cambridge, MA, USA: MIT Press, 2001.

[8] D. Parker. (1989). *Computer Crime: Criminal Justice Resource Manual*. Accessed: Jan. 2, 2022. [Online]. Available: https://www.ncjrs.gov/ pdf_les1/Digitization /118214NCJRS.pdf

[9] *De_nition of Cybersecurity*. Accessed: Mar. 2, 2022. [Online]. Available: https://www.itu.int/en/ITU-T/study groups / com17/Pages/cyber security.aspx

[10] G. Pons-Salvador, X. Zubieta-Méndez, and D. Frias-Navarro, ``Internet use by children aged six to nine: Parents' beliefs and knowledge about risk prevention," *Child Indicators Res.*, vol. 11, no. 6, pp. 1983_2000,Dec. 2018.

[11] T. Correa, J. D. Straubhaar, W. Chen, and J. Spence, ``Brokering new technologies: The role of children in their parents' usage of the internet," *New Media Soc.*, vol. 17, no. 4, pp. 483_500, Apr. 2015.

[12] M. Micheli, ``What is new in the digital divide? Understanding internet use by teenagers from different social backgrounds," in *Communication and Information Technologies Annual*. Bingley, U.K.: Emerald Group Publishing, 2015, pp. 55_87.

[13] N. H. Abd Rahim, S. Hamid, and M. L. Mat Kiah, ``Enhancement of cybersecurity awareness program on personal data protection among youngsters in Malaysia: An assessment," *Malaysian J. Comput. Sci.*, vol. 32, no. 3, pp. 221_245, Jul. 2019.

[14] F. Quayyum, D. S. Cruzes, and L. Jaccheri, ``Cybersecurity awareness for children: A systematic literature review," *Int. J. Child-Computer Interact.*, vol. 30, Dec. 2021, Art. no. 100343.

[15] J. P. Hourcade, *Child-Computer Interaction*. Scotts Valley, CA, USA: CreateSpace Independent Publishing Platform, 2015.

[16] R. S. Shaw, C. C. Chen, A. L. Harris, and H.-J. Huang, ``The impact of information richness on information security awareness training effectiveness," *Comput. Educ.*, vol. 52, no. 1, pp. 92_100, Jan. 2009.

[17] I. Hwang, R. Wake_eld, S. Kim, and T. Kim, ``Security awareness: The _rst step in information security compliance behavior," *J. Comput. Inf. Syst.*, vol. 61, no. 4, pp. 345_356, Jul. 2021.

[18] B. Khan, ``Effectiveness of information security awareness methods based on psychological theories," *Afr. J. Bus. Manage.*, vol. 5, no. 26, pp. 10862_10868, Oct. 2011.

[19] G. Cohen Zilka, ``Awareness of eSafety and potential online dangers among children and teenagers," *J. Inf. Technol. Education: Res.*, vol. 16, pp. 319_338, 2017.

[20] M. Adams and M. Makramalla, ``Cybersecurity skills training: An attacker-centric gami_ed approach," *Technol. Innov. Manage. Rev.*, vol. 5, no. 1, pp. 5_14, Jan. 2015.

[21] *Statista*. Accessed: Feb. 5, 2022. [Online]. Available: https://www.statista.com/topics/1145/internet-usage-worldwide/

[22] A. Cuthbertson. (Jan. 5, 2022). *Ransomware Attacks Rise 250 Percent in 2017, Hitting U.S. Hardest*. Newsweek. [Online]. Available: https://www. newsweek.com/ ransomware- attacks-rise-250-2017-us-wannacry-614034

[23] R. Ismailova and G. Muhametjanova, ``Cyber crime risk awareness in Kyrgyz republic," *Inf. Secur. J., A Global Perspective*, vol. 25, nos. 1_3, pp. 32_38, Apr. 2016.

[24] A. Moallem, *Cybersecurity Awareness Among Students and Faculty*. Boca Raton, FL, USA: CRC Press, 2018.

[25] S. S. Tirumala, A. Sarrafzadeh, and P. Pang, ``A survey on internet usage and cybersecurity awareness in students," in *Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST)*, Auckland, NewZealand, Dec. 2016, pp. 223_228.