# Cybersecurity Awareness in Online Education: A Case Study Analysis

**MEHMET EMIN ERENDOR**[1] **AND MERVE YILDIRIM**[2]
[1]Faculty of Economics and Administrative Sciences, Kyrgyz-Turkish Manas University, Bishkek 720044, Kyrgyzstan
[2]Faculty of Engineering and Architecture, Erzurum Technical University, 25050 Erzurum, Turkey

Corresponding author: Mehmet Emin Erendor (mehmet.erendor@manas.edu.kg)

This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by the Faculty Of Economics And Administrative Sciences, Kyrgyz-Turk Manas University, under Application No. R.30.2021/İBF-1745.

**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.

**INDEX TERMS** Awareness, cyberattacks, cybersecurity, Manas University, students.

## I. INTRODUCTION

With the spread of technology and the penetration of the internet into every aspect of daily life, cybersecurity 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 cyberattacks 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 cyberattack, 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 cyberattack 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 cyberattacks today?' Today, saying that cyberattacks are carried out only for political purposes is insufficient when it comes to trying to understand the nature of cyberattacks. This is because new cyber concepts have emerged that have changed the nature of cyberattacks. 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 cybersecurity 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. Cybersecurity 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 cyberattacks and cybersecurity compared to the past, the ability to perform cyberattacks 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

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamed Elhoseny.

computer technologies and can easily perform any activity they want by using it [10]–[13].

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].

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].

Within the framework of this information, it will also be questioned what kind of information the students have about cybersecurity 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 cybersecurity awareness based on the theoretical framework findings.

## II. LITERATURE REVIEW

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].

**TABLE 1.** The methods and results of similar studies.

| Authors | Title | Publication Source | Method | Results | Year |
|---|---|---|---|---|---|
| Ismailova and Muhametjanova | Cyber crime risk awareness in Kyrgyz Republic | Information Security Journal: A Global Perspective | Questionnaire | Despite the widespread use of information technology, students must be taught about information security to avoid being the victims of cybercrime. | 2016 |
| Moallem | Cybersecurity Awareness Among Students and Faculty | CRC Press | Survey | - | 2018 |
| Tirumala | A Survey on Internet Usage and Cybersecurity Awareness in Students | 14th Annual Conference on Privacy, Security and Trust (PST) | Survey | The findings also revealed that the majority of students were unaware of cybersecurity measures for tablets and smartphones, both of which are often used gadgets. | 2016 |
| Ahmed et.al. | Cybersecurity Awareness Survey: An Analysis from Bangladesh Perspective | 2017 IEEE Region 10 Humanitarian Technology Conference | Survey | According to the survey, there is a patchy level of awareness that is not sufficient. The general public is uninformed of cybersecurity best practices. Concerns about cybercrime are not well-received by the government and its agencies. | 2017 |
| Garba et.al. | A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach | International Journal on Emerging Technologies | Quantitative Approach | The findings were evaluated, revealing that the university students' cybersecurity knowledge is at a satisfactory level, with more than half of them unaware of how to secure their data. | 2020 |
| Kirwan et.al. | Risk Factors for Social Networking Site Scam Victimization Among Malaysian Students | Cyberpsychology, Behavior, and Social Networking | Online Survey | Having higher scores in impulsivity (particularly cognitive complexity), using fewer devices for Social Network Sites, and being on a Social Network Site for a longer period of time were all found to be victimization risk factors according to the logistic regression analysis. | 2018 |
| Senthilkumar and Sathishkumar | A Survey on Cyber Security Awareness Among College Students in Tamil Nadu | IOP Conference Series: Materials Science and Engineering | Questionnaire | According to the results of the survey, Tamil Nadu college students have an above-average degree of awareness about cyber-related hazard issues, which can help them protect them from cyberattacks. | 2017 |
| Zwilling et.al. | Cyber Security Awareness, Knowledge and Behavior: A Comparative Study | Journal of Computer Information Systems | Paper-Based Survey | The findings demonstrate that while internet users are aware of cyber threats, they only take modest precautions that are typically common and straightforward. Beyond the differences in respondent nation or gender, the study findings suggest that stronger cyber knowledge is linked to a higher level of cyber awareness. | 2022 |
| Shamsi | Effectiveness of Cyber Security Awareness Program for Young Children: A Case Study in UAE | International Journal of Information Technology and Language Studies | Qualitative Methods | Children can be exposed to different cyber risks and they should learn the precautions for this in the cybersecurity awareness program they can take | 2019 |
| Abd Rahim et.al. | Enhancement of Cybersecurity Awareness Program on Personal Data Protection Among Youngsters in Malaysia: An Assessment | Malaysian Journal of Computer Science | Mixed Method Research Methodology | The young people had a positive reaction to the content of the program. It was reported that there were changes in their knowledge and skills on the protection of personal data and in the implementation of the desired behaviors | 2019 |
| Moallem | Cybersecurity Awareness Among College Students | Advances in Human Factors in Cybersecurity, AHFE 2018 Advances in Intelligent Systems and Computing | Quantitative Method | It has been revealed that although the students do not trust the university system, they do not know how they will protect their data. It is also claimed that universities do not provide cyber awareness studies for their students. | 2019 |
| Ismailova et.al. | Cybercrime risk awareness rate among students in Central Asia: A comparative study in Kyrgyzstan and Kazakhstan | Information Security Journal: A Global Perspective | Quantitative Research | According to the results of the research, it has been revealed that the gender and age of the participants in Kazakhstan affected the cybercrime awareness rate. No factors affected the situation in Kyrgyzstan. | 2019 |

**TABLE 2.** Demographic variables.

| | | n | % |
|---|---|---|---|
| Age | 17-20 | 299 | 57,8 |
| | 21-25 | 196 | 37,9 |
| | 26-29 | 9 | 1,7 |
| | 30+ | 13 | 2,5 |
| Sex | Female | 344 | 66,5 |
| | Male | 173 | 33,5 |
| Education Level | Undergraduate | 463 | 89,6 |
| | Master's Degree | 54 | 10,4 |
| | Ph.D. | 0 | 0,0 |
| Faculty | Humanities | 129 | 25,0 |
| | Sciences | 39 | 7,5 |
| | Fine Arts | 24 | 4,6 |
| | Economics and Management | 116 | 22,4 |
| | Communication | 32 | 6,2 |
| | Theology | 23 | 4,4 |
| | Engineering | 109 | 21,1 |
| | Veterinary Medicine | 21 | 4,1 |
| | Agriculture | 24 | 4,6 |
| Personal Computer | Yes | 307 | 59,4 |
| | No | 210 | 40,6 |
| How to Connect to the Internet | Mobile Phone | 408 | 78,9 |
| | Notebook | 103 | 19,9 |
| | Internet Cafe | 1 | ,2 |
| | University Facilities | 5 | 1,0 |

**TABLE 3.** Cybersecurity awareness.

| | | n | % |
|---|---|---|---|
| How competent do you feel about the use of the computer? | Very Good | 84 | 16,2 |
| | Good | 205 | 39,7 |
| | Average | 164 | 31,7 |
| | Few | 47 | 9,1 |
| | Very Few | 17 | 3,3 |
| The knowledge of computer hardware, operating systems, network systems. | Very Good | 36 | 7,0 |
| | Good | 150 | 29,0 |
| | Average | 207 | 40,0 |
| | Few | 92 | 17,8 |
| | Very Few | 32 | 6,2 |
| Attacks over network systems | Very Good | 26 | 5,0 |
| | Good | 104 | 20,1 |
| | Average | 174 | 33,7 |
| | Few | 152 | 29,4 |
| | Very Few | 61 | 11,8 |
| "Social engineering" and "phishing" attacks | Yes I heard | 159 | 30,8 |
| | No, I didn't hear | 358 | 69,2 |
| The knowledge of the concepts of HTTPS, secure connection, SSH, TSL | Very Good | 12 | 2,3 |
| | Good | 55 | 10,6 |
| | Average | 107 | 20,7 |
| | Few | 146 | 28,2 |
| | Very Few | 197 | 38,1 |
| How much do you know about cyber-attacks? | Very Good | 26 | 5,0 |
| | Good | 76 | 14,7 |
| | Average | 152 | 29,4 |
| | Few | 138 | 26,7 |
| | Very Few | 125 | 24,2 |
| Do you follow the cyber-attacks in the world and your country? | Yes | 153 | 29,6 |
| | No | 364 | 70,4 |

Shamsi conducted a study on children. The author, who used a qualitative method in his study, stated that children can be exposed to different cyber risks and that they should learn the associated precautions through cybersecurity awareness programs [30].

Abd Rahim *et al.* worked on a cyber security awareness program. In this study, the authors used the mixed method research methodology through four main steps: analysis, design, development, and evaluation. Within the framework of the data obtained, it was revealed that the young people had positive reactions to the content of the program. They reported that there were changes in their knowledge and skills regarding the protection of personal data and in the implementation of the desired behaviors [13].

Moallem conducted a quantitative data-based study on students in Silicon Valley, California. This study analyzed the cybersecurity awareness of students in Silicon Valley. As a result, the risks in the cutting-edge technology environment were also analyzed [31]. Within the framework of the data obtained, it was revealed that although the students do not trust the university system, they also do not know how they will protect their data. It is also claimed that universities do not carry out cyber awareness programs for their students.

Ismailova *et al.* conducted quantitative research on students at two state universities in Kyrgyzstan and Kazakhstan. The main purpose of this study was to compare the student's cybercrime risk awareness. According to the results of the research, the gender and age of the participants in Kazakhstan affected the cybercrime awareness rate. No factors affected the situation in Kyrgyzstan [32].

Most of the studies in the literature have revealed the fact that there is a lack of knowledge about cybersecurity awareness in the younger generation. Some studies have also stated that even if the participants have the knowledge, this is not enough to protect them from cyberattacks. Our study used the online survey method to determine the cyber awareness levels of university students and they asked the questions in a hierarchy from general to specific to measure the knowledge level of students in the field of cybersecurity. First, the students' general computer usage tendencies were revealed, then their knowledge levels on more technical issues specific to cybersecurity were measured. It was aimed to determine how many of the students had a more detailed background in network and computer security issues since more than superficial knowledge is needed to deal with cyber threats. In addition, our study differs from many other studies in that it is carried out as part of an ongoing online education process.

Table 1 lists the methods used in similar studies and the results obtained. Detailed information about our research methodology is presented in the next section.

**TABLE 4.** The relationship between cybersecurity knowledge and gender.

| | | Sex | | | | Chi-Square | p |
|---|---|---|---|---|---|---|---|
| | | Female | | Male | | | |
| | | n | % | n | % | | |
| How competent do you feel about the use of the computer? | Very Good | 37 | 10,8 | 47 | 27,2 | 25,491[a] | ,000* |
| | Good | 143 | 41,6 | 62 | 35,8 | | |
| | Average | 123 | 35,8 | 41 | 23,7 | | |
| | Few | 30 | 8,7 | 17 | 9,8 | | |
| | Very Few | 11 | 3,2 | 6 | 3,5 | | |
| The knowledge of computer hardware, operating systems, network systems. | Very Good | 14 | 4,1 | 22 | 12,7 | 19,134[a] | ,001* |
| | Good | 92 | 26,7 | 58 | 33,5 | | |
| | Average | 151 | 43,9 | 56 | 32,4 | | |
| | Few | 66 | 19,2 | 26 | 15,0 | | |
| | Very Few | 21 | 6,1 | 11 | 6,4 | | |
| Attacks over network systems | Very Good | 11 | 3,2 | 15 | 8,7 | 21,133[a] | ,000* |
| | Good | 57 | 16,6 | 47 | 27,2 | | |
| | Average | 115 | 33,4 | 59 | 34,1 | | |
| | Few | 115 | 33,4 | 37 | 21,4 | | |
| | Very Few | 46 | 13,4 | 15 | 8,7 | | |
| "Social engineering" and "phishing" attacks | Yes I heard | 96 | 27,9 | 63 | 36,4 | 3,914[a] | ,048* |
| | No, I didn't hear | 248 | 72,1 | 110 | 63,6 | | |
| The knowledge of the concepts of HTTPS, secure connection, SSH, TSL | Very Good | 4 | 1,2 | 8 | 4,6 | 20,707[a] | ,000* |
| | Good | 29 | 8,4 | 26 | 15,0 | | |
| | Average | 62 | 18,0 | 45 | 26,0 | | |
| | Few | 102 | 29,7 | 44 | 25,4 | | |
| | Very Few | 147 | 42,7 | 50 | 28,9 | | |
| How much do you know about cyber-attacks? | Very Good | 10 | 2,9 | 16 | 9,2 | 22,940[a] | ,000* |
| | Good | 43 | 12,5 | 33 | 19,1 | | |
| | Average | 96 | 27,9 | 56 | 32,4 | | |
| | Few | 96 | 27,9 | 42 | 24,3 | | |
| | Very Few | 99 | 28,8 | 26 | 15,0 | | |
| Do you follow the cyber-attacks in the world and your country? | Yes | 93 | 27,0 | 60 | 34,7 | 3,231[a] | ,072 |
| | No | 251 | 73,0 | 113 | 65,3 | | |

***p<0,05**

**TABLE 5.** The relationship between cybersecurity knowledge and age.

| | | Age | | | | | | Chi-Square | p |
|---|---|---|---|---|---|---|---|---|---|
| | | 17-20 | | 21-25 | | 26+ | | | |
| | | n | % | n | % | n | % | | |
| How competent do you feel about the use of the computer? | Very Good | 48 | 16,1 | 31 | 15,8 | 5 | 22,7 | 17,232[a] | ,028* |
| | Good | 100 | 33,4 | 92 | 46,9 | 13 | 59,1 | | |
| | Average | 107 | 35,8 | 53 | 27,0 | 4 | 18,2 | | |
| | Few | 32 | 10,7 | 15 | 7,7 | 0 | 0,0 | | |
| | Very Few | 12 | 4,0 | 5 | 2,6 | 0 | 0,0 | | |
| The knowledge of computer hardware, operating systems, network systems. | Very Good | 20 | 6,7 | 12 | 6,1 | 4 | 18,2 | 28,728[a] | ,000* |
| | Good | 67 | 22,4 | 71 | 36,2 | 12 | 54,5 | | |
| | Average | 128 | 42,8 | 75 | 38,3 | 4 | 18,2 | | |
| | Few | 66 | 22,1 | 25 | 12,8 | 1 | 4,5 | | |
| | Very Few | 18 | 6,0 | 13 | 6,6 | 1 | 4,5 | | |
| Attacks over network systems | Very Good | 16 | 5,4 | 8 | 4,1 | 2 | 9,1 | 23,394[a] | ,003* |
| | Good | 44 | 14,7 | 50 | 25,5 | 10 | 45,5 | | |
| | Average | 109 | 36,5 | 60 | 30,6 | 5 | 22,7 | | |
| | Few | 97 | 32,4 | 50 | 25,5 | 5 | 22,7 | | |
| | Very Few | 33 | 11,0 | 28 | 14,3 | 0 | 0,0 | | |
| "Social engineering" and "phishing" attacks | Yes I heard | 84 | 28,1 | 64 | 32,7 | 11 | 50,0 | 5,152[a] | ,076 |
| | No, I didn't hear | 215 | 71,9 | 132 | 67,3 | 11 | 50,0 | | |
| The knowledge of the concepts of HTTPS, secure connection, SSH, TSL | Very Good | 4 | 1,3 | 7 | 3,6 | 1 | 4,5 | 11,201[a] | ,191 |
| | Good | 29 | 9,7 | 24 | 12,2 | 2 | 9,1 | | |
| | Average | 62 | 20,7 | 36 | 18,4 | 9 | 40,9 | | |
| | Few | 85 | 28,4 | 55 | 28,1 | 6 | 27,3 | | |
| | Very Few | 119 | 39,8 | 74 | 37,8 | 4 | 18,2 | | |
| How much do you know about cyber-attacks? | Very Good | 11 | 3,7 | 11 | 5,6 | 4 | 18,2 | 13,908[a] | ,084 |
| | Good | 48 | 16,1 | 25 | 12,8 | 3 | 13,6 | | |
| | Average | 86 | 28,8 | 57 | 29,1 | 9 | 40,9 | | |
| | Few | 84 | 28,1 | 51 | 26,0 | 3 | 13,6 | | |
| | Very Few | 70 | 23,4 | 52 | 26,5 | 3 | 13,6 | | |
| Do you follow the cyber-attacks in the world and your country? | Yes | 90 | 30,1 | 53 | 27,0 | 10 | 45,5 | 3,306[a] | ,191 |
| | No | 209 | 69,9 | 143 | 73,0 | 12 | 54,5 | | |

***p<0,05**

## III. METHOD

### A. PARTICIPANTS

Although surveys have been conducted on cybersecurity awareness before, it was concluded that the number of participants did not reflect the general profile of the university. The main reason for considering the Kyrgyz-Turkish Manas University in this study was the wide student profile and the education of students from different countries.

The study obtained a sample of students from those attending the Kyrgyz Turkish Manas University. The questionnaire

**TABLE 6.** The relationship between cybersecurity knowledge and level of education.

| | | Level of Education | | | | Chi-Square | p |
|---|---|---|---|---|---|---|---|
| | | Undergraduate | | Master's Degree | | | |
| | | n | % | n | % | | |
| How competent do you feel about the use of the computer? | Very Good | 70 | 15,1 | 14 | 25,9 | 5,834[a] | ,212 |
| | Good | 185 | 40,0 | 20 | 37,0 | | |
| | Average | 148 | 32,0 | 16 | 29,6 | | |
| | Few | 43 | 9,3 | 4 | 7,4 | | |
| | Very Few | 17 | 3,7 | 0 | 0,0 | | |
| The knowledge of computer hardware, operating systems, network systems. | Very Good | 30 | 6,5 | 6 | 11,1 | 9,057[a] | ,060 |
| | Good | 128 | 27,6 | 22 | 40,7 | | |
| | Average | 193 | 41,7 | 14 | 25,9 | | |
| | Few | 85 | 18,4 | 7 | 13,0 | | |
| | Very Few | 27 | 5,8 | 5 | 9,3 | | |
| Attacks over network systems | Very Good | 24 | 5,2 | 2 | 3,7 | 13,721[a] | ,008* |
| | Good | 85 | 18,4 | 19 | 35,2 | | |
| | Average | 160 | 34,6 | 14 | 25,9 | | |
| | Few | 143 | 30,9 | 9 | 16,7 | | |
| | Very Few | 51 | 11,0 | 10 | 18,5 | | |
| "Social engineering" and "phishing" attacks | Yes I heard | 137 | 29,6 | 22 | 40,7 | 2,824[a] | ,093 |
| | No, I didn't hear | 326 | 70,4 | 32 | 59,3 | | |
| The knowledge of the concepts of HTTPS, secure connection, SSH, TSL | Very Good | 10 | 2,2 | 2 | 3,7 | 6,723[a] | ,151 |
| | Good | 45 | 9,7 | 10 | 18,5 | | |
| | Average | 93 | 20,1 | 14 | 25,9 | | |
| | Few | 134 | 28,9 | 12 | 22,2 | | |
| | Very Few | 181 | 39,1 | 16 | 29,6 | | |
| How much do you know about cyber-attacks? | Very Good | 23 | 5,0 | 3 | 5,6 | 1,084[a] | ,897 |
| | Good | 66 | 14,3 | 10 | 18,5 | | |
| | Average | 136 | 29,4 | 16 | 29,6 | | |
| | Few | 126 | 27,2 | 12 | 22,2 | | |
| | Very Few | 112 | 24,2 | 13 | 24,1 | | |
| Do you follow the cyber-attacks in the world and your country? | Yes | 134 | 28,9 | 19 | 35,2 | ,905[a] | ,342 |
| | No | 329 | 71,1 | 35 | 64,8 | | |

***p<0,05**

was distributed online because of the Covid-19 pandemic and distance education process. The response rate for the online questionnaire was 9.73%. Thus, the total sample was comprised of 517 students between 17 and 30+ years old. In our sample, 33.5% of the students were male and 66.5% were female. The majority of the participants were undergraduate students totaling 89.6%, and master's degree and PhD students totaling 10.4%.

### B. MATERIALS

A questionnaire consisting of a few basic computers and data security questions was administered to the students to measure their level of cybersecurity awareness. The questionnaire consisted of a total of 36 questions distributed across eight sections according to their relevance. There were different questions in each section. Within the framework of cybersecurity awareness, the main aim of the survey was to measure how much information the participants had according to different situations such as malware and password security. In line with this information, the participants were first asked about their level of education, and then they were asked to give information about whether they had a personal computer. In addition, by asking questions about how the students connect to the internet, the situation of both those who have a personal computer and those who do not was analyzed. Questions about general computer knowledge, network, and information security were then asked using five different questions. The main purpose of these questions was to analyze whether the students knew computer hardware, operating systems, and attacks over the network before asking questions about cybersecurity awareness. In the remaining part, the students were asked questions about password security and social media accounts, and the information was analyzed.

While choosing the questions asked in the questionnaire, it was taken into account that not all of the students had a computer science background. 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. While analyzing the links between the questions, it was aimed to reveal what the factors affecting cybersecurity awareness are and to measure the effect level of the factors are.

**TABLE 7.** The relationship between cybersecurity knowledge and the students' major.

| | | Faculty | | | | | | | | | | | | | | | | | | Chi-Square | p |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Humanities | | Sciences | | Fine Arts | | Econ. And Man. | | Comm. | | Theology | | Eng. | | Veter. | | Agri. | | | |
| | | n | % | n | % | n | % | n | % | n | % | n | % | n | % | n | % | n | % | | |
| How competent do you feel about the use of computers? | Very Good | 13 | 10,1 | 8 | 20,5 | 0 | 0,0 | 11 | 9,5 | 7 | 21,9 | 3 | 13,0 | 37 | 33,9 | 3 | 14,3 | 2 | 8,3 | 62,384[a] | ,001* |
| | Good | 51 | 39,5 | 14 | 35,9 | 11 | 45,8 | 57 | 49,1 | 10 | 31,3 | 5 | 21,7 | 42 | 38,5 | 4 | 19,0 | 11 | 45,8 | | |
| | Average | 44 | 34,1 | 12 | 30,8 | 10 | 41,7 | 37 | 31,9 | 11 | 34,4 | 10 | 43,5 | 23 | 21,1 | 10 | 47,6 | 7 | 29,2 | | |
| | Few | 14 | 10,9 | 4 | 10,3 | 3 | 12,5 | 10 | 8,6 | 2 | 6,3 | 3 | 13,0 | 5 | 4,6 | 3 | 14,3 | 3 | 12,5 | | |
| | Very Few | 7 | 5,4 | 1 | 2,6 | 0 | 0,0 | 1 | ,9 | 2 | 6,3 | 2 | 8,7 | 2 | 1,8 | 1 | 4,8 | 1 | 4,2 | | |
| The knowledge of computer hardware, operating systems, network systems | Very Good | 7 | 5,4 | 5 | 12,8 | 1 | 4,2 | 3 | 2,6 | 3 | 9,4 | 0 | 0,0 | 14 | 12,8 | 1 | 4,8 | 2 | 8,3 | 69,666[a] | ,000* |
| | Good | 29 | 22,5 | 13 | 33,3 | 10 | 41,7 | 32 | 27,6 | 7 | 21,9 | 10 | 43,5 | 40 | 36,7 | 2 | 9,5 | 7 | 29,2 | | |
| | Average | 57 | 44,2 | 14 | 35,9 | 10 | 41,7 | 59 | 50,9 | 11 | 34,4 | 1 | 4,3 | 41 | 37,6 | 9 | 42,9 | 5 | 20,8 | | |
| | Few | 26 | 20,2 | 6 | 15,4 | 2 | 8,3 | 17 | 14,7 | 6 | 18,8 | 9 | 39,1 | 11 | 10,1 | 6 | 28,6 | 9 | 37,5 | | |
| | Very Few | 10 | 7,8 | 1 | 2,6 | 1 | 4,2 | 5 | 4,3 | 5 | 15,6 | 3 | 13,0 | 3 | 2,8 | 3 | 14,3 | 1 | 4,2 | | |
| Attacks over network systems | Very Good | 3 | 2,3 | 3 | 7,7 | 0 | 0,0 | 5 | 4,3 | 1 | 3,1 | 1 | 4,3 | 10 | 9,2 | 1 | 4,8 | 2 | 8,3 | 42,845[a] | ,095 |
| | Good | 23 | 17,8 | 7 | 17,9 | 6 | 25,0 | 24 | 20,7 | 9 | 28,1 | 4 | 17,4 | 26 | 23,9 | 1 | 4,8 | 4 | 16,7 | | |
| | Average | 42 | 32,6 | 13 | 33,3 | 13 | 54,2 | 39 | 33,6 | 7 | 21,9 | 6 | 26,1 | 40 | 36,7 | 8 | 38,1 | 6 | 25,0 | | |
| | Few | 44 | 34,1 | 13 | 33,3 | 4 | 16,7 | 36 | 31,0 | 8 | 25,0 | 7 | 30,4 | 27 | 24,8 | 4 | 19,0 | 9 | 37,5 | | |
| | Very Few | 17 | 13,2 | 3 | 7,7 | 1 | 4,2 | 12 | 10,3 | 7 | 21,9 | 5 | 21,7 | 6 | 5,5 | 7 | 33,3 | 3 | 12,5 | | |
| "Social engineering" and "phishing" attacks | Yes | 36 | 27,9 | 13 | 33,3 | 5 | 20,8 | 32 | 27,6 | 8 | 25,0 | 4 | 17,4 | 46 | 42,2 | 9 | 42,9 | 6 | 25,0 | 13,220[a] | ,105 |
| | No | 93 | 72,1 | 26 | 66,7 | 19 | 79,2 | 84 | 72,4 | 24 | 75,0 | 19 | 82,6 | 63 | 57,8 | 12 | 57,1 | 18 | 75,0 | | |
| The knowledge of the concepts of HTTPS, secure connection, SSH, and TSL | Very Good | 1 | ,8 | 2 | 5,1 | 1 | 4,2 | 0 | 0,0 | 0 | 0,0 | 0 | 0,0 | 6 | 5,5 | 1 | 4,8 | 1 | 4,2 | 56,106[a] | ,005* |
| | Good | 8 | 6,2 | 8 | 20,5 | 3 | 12,5 | 12 | 10,3 | 2 | 6,3 | 0 | 0,0 | 19 | 17,4 | 3 | 14,3 | 0 | 0,0 | | |
| | Average | 28 | 21,7 | 6 | 15,4 | 5 | 20,8 | 25 | 21,6 | 6 | 18,8 | 1 | 4,3 | 30 | 27,5 | 3 | 14,3 | 3 | 12,5 | | |
| | Few | 33 | 25,6 | 5 | 12,8 | 8 | 33,3 | 39 | 33,6 | 11 | 34,4 | 9 | 39,1 | 27 | 24,8 | 7 | 33,3 | 7 | 29,2 | | |
| | Very Few | 59 | 45,7 | 18 | 46,2 | 7 | 29,2 | 40 | 34,5 | 13 | 40,6 | 13 | 56,5 | 27 | 24,8 | 7 | 33,3 | 13 | 54,2 | | |
| How much do you know about cyber-attacks? | Very Good | 5 | 3,9 | 3 | 7,7 | 0 | 0,0 | 4 | 3,4 | 1 | 3,1 | 0 | 0,0 | 11 | 10,1 | 1 | 4,8 | 1 | 4,2 | 42,805[a] | ,096 |
| | Good | 15 | 11,6 | 7 | 17,9 | 2 | 8,3 | 16 | 13,8 | 8 | 25,0 | 1 | 4,3 | 24 | 22,0 | 2 | 9,5 | 1 | 4,2 | | |
| | Average | 36 | 27,9 | 6 | 15,4 | 11 | 45,8 | 38 | 32,8 | 7 | 21,9 | 5 | 21,7 | 35 | 32,1 | 6 | 28,6 | 8 | 33,3 | | |
| | Few | 35 | 27,1 | 10 | 25,6 | 7 | 29,2 | 36 | 31,0 | 9 | 28,1 | 9 | 39,1 | 19 | 17,4 | 5 | 23,8 | 8 | 33,3 | | |
| | Very Few | 38 | 29,5 | 13 | 33,3 | 4 | 16,7 | 22 | 19,0 | 7 | 21,9 | 8 | 34,8 | 20 | 18,3 | 7 | 33,3 | 6 | 25,0 | | |
| Do you follow the cyber-attacks in the world and your country? | Yes I do | 31 | 24,0 | 11 | 28,2 | 11 | 45,8 | 37 | 31,9 | 8 | 25,0 | 9 | 39,1 | 38 | 34,9 | 4 | 19,0 | 4 | 16,7 | 11,111[a] | ,195 |
| | No, I am not interested in | 98 | 76,0 | 28 | 71,8 | 13 | 54,2 | 79 | 68,1 | 24 | 75,0 | 14 | 60,9 | 71 | 65,1 | 17 | 81,0 | 20 | 83,3 | | |

The analysis in this study was performed using the SPSS 21.0 program and they were studied at a 95% confidence level. In the analysis, the frequency and percentage values were calculated for the categorical variables. The relationship between the categorical variables was analyzed using the chi-square test.

**TABLE 8.** The effect of the internet connection method on cybersecurity awareness.

| | | How do you connect to the Internet | | | | Chi-Square | p |
|---|---|---|---|---|---|---|---|
| | | Mobile Phone | | Notebook | | | |
| | | n | % | n | % | | |
| How competent do you feel about the use of computers? | Very Good | 48 | 11,8 | 35 | 34,0 | 32,311[a] | ,000* |
| | Good | 171 | 41,9 | 32 | 31,1 | | |
| | Average | 132 | 32,4 | 30 | 29,1 | | |
| | Few | 41 | 10,0 | 5 | 4,9 | | |
| | Very Few | 16 | 3,9 | 1 | 1,0 | | |
| The knowledge of computer hardware, operating systems, network systems | Very Good | 20 | 4,9 | 15 | 14,6 | 16,620[a] | ,002* |
| | Good | 117 | 28,7 | 33 | 32,0 | | |
| | Average | 169 | 41,4 | 34 | 33,0 | | |
| | Few | 73 | 17,9 | 19 | 18,4 | | |
| | Very Few | 29 | 7,1 | 2 | 1,9 | | |
| Attacks over network systems | Very Good | 15 | 3,7 | 11 | 10,7 | 11,607[a] | ,021* |
| | Good | 80 | 19,6 | 24 | 23,3 | | |
| | Average | 137 | 33,6 | 34 | 33,0 | | |
| | Few | 123 | 30,1 | 27 | 26,2 | | |
| | Very Few | 53 | 13,0 | 7 | 6,8 | | |
| "Social engineering" and "phishing" attacks | Yes | 111 | 27,2 | 47 | 45,6 | 13,071[a] | ,000* |
| | No | 297 | 72,8 | 56 | 54,4 | | |
| The knowledge of the concepts of HTTPS, secure connection, SSH, and TSL | Very Good | 6 | 1,5 | 6 | 5,8 | 20,335[a] | ,000* |
| | Good | 40 | 9,8 | 15 | 14,6 | | |
| | Average | 75 | 18,4 | 31 | 30,1 | | |
| | Few | 127 | 31,1 | 18 | 17,5 | | |
| | Very Few | 160 | 39,2 | 33 | 32,0 | | |
| How much do you know about cyber-attacks? | Very Good | 12 | 2,9 | 14 | 13,6 | 26,349[a] | ,000* |
| | Good | 53 | 13,0 | 21 | 20,4 | | |
| | Average | 123 | 30,1 | 29 | 28,2 | | |
| | Few | 113 | 27,7 | 23 | 22,3 | | |
| | Very Few | 107 | 26,2 | 16 | 15,5 | | |
| Do you follow the cyber-attacks in the world and your country? | Yes I do | 110 | 27,0 | 42 | 40,8 | 7,512[a] | ,006* |
| | No, I am not interested in | 298 | 73,0 | 61 | 59,2 | | |

*p<0,05

## IV. RESULTS AND DISCUSSION

### A. DEMOGRAPHICS

According to the survey results, female participants were the majority at 66.5% compared to male participants at 33.5%. Considering the age distribution of the participants, it can be seen that the rate of those aged 17-20 is the highest with 57.8% and the majority of the students participating in the survey are undergraduate students at a rate of 89.6%. Literature, economics and administrative sciences, and engineering students participated in the survey the most at 25.0%, 22.4%, and 21.1%, respectively.

While the rate of those who have a personal computer is 59.4%, the rate of those who connect to the internet with their mobile phone is 78.9%. This is followed by those who connect to the internet using a notebook at 19.9%. This shows that the use of mobile phones by university students is higher than those who use of computers. The distribution of the demographic variables is shown in Table 2 in detail.

### B. CYBERSECURITY AWARENESS

In this part, various analyses of the cybersecurity awareness of the students are presented. To make an effective evaluation, the questions were asked from general to specific. Since cybersecurity awareness is related in parallel to familiarity with the digital world and the frequency of computer and internet use, first of all, it was desirable to figure out how sufficient the students felt about their computer use. As can be seen in Table 3, the percentage of participants who find themselves to be very good and good at using computers is 16.2% and 39.7%, respectively.

Afterwards, an attempt was made to find out whether the students had more specific knowledge about computers. Students, like most ordinary users, may use computers frequently in practical terms but they may not be aware of the features of the operating system they use, the use and functionality of the hardware parts involved, and the details of the network environment that they use to transfer probably thousands of data to almost every day. Learning about this situation is of critical importance to prepare the groundwork for possible training in the future. Looking at the results, the percentage of those who think that they have a good or higher level of knowledge on technical issues such as computer hardware, operating systems, and network systems is 36.0% in total. Most of the participants see themselves as having an average level of knowledge on this subject.

After this stage, the students were asked ''cybersecurity-based'' questions on cyberattacks, basic network security protocols, and related components. There may be students

**TABLE 9.** The relationship between the possession of a personal computer and cybersecurity awareness.

| | | Personal Computer | | | | Chi-Square | p |
|---|---|---|---|---|---|---|---|
| | | Yes | | No | | | |
| | | n | % | n | % | | |
| How competent do you feel about the use of computers? | Very Good | 55 | 17,9 | 29 | 13,8 | 11,092[a] | ,026* |
| | Good | 126 | 41,0 | 79 | 37,6 | | |
| | Average | 96 | 31,3 | 68 | 32,4 | | |
| | Few | 26 | 8,5 | 21 | 10,0 | | |
| | Very Few | 4 | 1,3 | 13 | 6,2 | | |
| The knowledge of computer hardware, operating systems, network systems | Very Good | 26 | 8,5 | 10 | 4,8 | 6,318[a] | ,177 |
| | Good | 93 | 30,3 | 57 | 27,1 | | |
| | Average | 120 | 39,1 | 87 | 41,4 | | |
| | Few | 54 | 17,6 | 38 | 18,1 | | |
| | Very Few | 14 | 4,6 | 18 | 8,6 | | |
| Attacks over network systems | Very Good | 20 | 6,5 | 6 | 2,9 | 11,814[a] | ,019* |
| | Good | 68 | 22,1 | 36 | 17,1 | | |
| | Average | 105 | 34,2 | 69 | 32,9 | | |
| | Few | 75 | 24,4 | 77 | 36,7 | | |
| | Very Few | 39 | 12,7 | 22 | 10,5 | | |
| "Social engineering" and "phishing" attacks | Yes | 106 | 34,5 | 53 | 25,2 | 5,053[a] | ,025* |
| | No | 201 | 65,5 | 157 | 74,8 | | |
| The knowledge of the concepts of HTTPS, secure connection, SSH, and TSL | Very Good | 12 | 3,9 | 0 | 0,0 | 9,442[a] | ,051 |
| | Good | 31 | 10,1 | 24 | 11,4 | | |
| | Average | 65 | 21,2 | 42 | 20,0 | | |
| | Few | 81 | 26,4 | 65 | 31,0 | | |
| | Very Few | 118 | 38,4 | 79 | 37,6 | | |
| How much do you know about cyber-attacks? | Very Good | 22 | 7,2 | 4 | 1,9 | 7,531[a] | ,110 |
| | Good | 43 | 14,0 | 33 | 15,7 | | |
| | Average | 88 | 28,7 | 64 | 30,5 | | |
| | Few | 79 | 25,7 | 59 | 28,1 | | |
| | Very Few | 75 | 24,4 | 50 | 23,8 | | |
| Do you follow the cyber-attacks in the world and your country? | Yes I do | 92 | 30,0 | 61 | 29,0 | ,051[a] | ,822 |
| | No, I am not interested in | 215 | 70,0 | 149 | 71,0 | | |

who are trained in these subjects and therefore have knowledge and there may be students who are personally interested in security. Apart from this, the number of participants who are unaware of these issues may be too high to be underestimated. The analyses undertaken to justify these assumptions have concluded that there is a serious lack of knowledge among the students on security-based issues.

It can be seen that the number of those who have very good knowledge about attacks made over network systems is less than the average. The rate of those who are aware of ''social engineering'' and ''phishing'' attacks is 30.8%.

The rate of those who find their knowledge of HTTPS, secure connection, SSL, TSL concepts very good and good is 2.3% and 10.6%, respectively. This is understandable, considering students' majors.

While the rate of those who think that they have superior knowledge about cyberattacks is relatively low, similarly, the rate of those who follow cyberattack events around the world and in their own countries is less than those who do not.

Various analyses were conducted to examine the relationship between the demographics of the participants and their awareness of cybersecurity. An attempt was made to determine whether characteristics such as gender, age, education level, and the department of the students has any effect on cybersecurity awareness. For the cybersecurity awareness assessment, the answers given to the questions were given in a hierarchical order from general to specific. These have been presented in the previous table and were taken as a basis.

The chi-square test results for examining the relationship between cybersecurity awareness and demographics are given in Tables 4 - 7.

Table 4 shows the relationship between the gender variables and cybersecurity awareness. When the significant results were examined ($p<0.05$), the level of feeling competent about computer use, the level of knowledge about computer hardware, operating systems, network systems, and the level of knowledge about attacks made over network systems were higher among the male students than among the female students.

Similarly, it was seen that the rate of hearing about ''social engineering'' and ''phishing'' attacks, the level of knowledge about HTTPS, secure connection, SSL, and TLS concepts, and the knowledge of cyberattacks were higher in male students.

Considering these results, it can be said that male students are more conscious of cybersecurity.

The chi-square test results following the examination of the relationship between age and cybersecurity awareness are given in Table 5.

**TABLE 10. The relationship between cybersecurity awareness and the possibility of being exposed to cyber threats.**

| | | Have you ever encountered a situation where your password was stolen or your account was hacked in online systems? | | | | Chi-Square | p |
|---|---|---|---|---|---|---|---|
| | | Yes | | No | | | |
| | | n | % | n | % | | |
| How competent do you feel about the use of computers? | Very Good | 23 | 27,4 | 61 | 72,6 | 3,928[a] | ,416 |
| | Good | 52 | 25,4 | 153 | 74,6 | | |
| | Average | 33 | 20,1 | 131 | 79,9 | | |
| | Few | 9 | 19,1 | 38 | 80,9 | | |
| | Very Few | 2 | 11,8 | 15 | 88,2 | | |
| The knowledge of computer hardware, operating systems, network systems | Very Good | 11 | 30,6 | 25 | 69,4 | 6,703[a] | ,152 |
| | Good | 34 | 22,7 | 116 | 77,3 | | |
| | Average | 49 | 23,7 | 158 | 76,3 | | |
| | Few | 14 | 15,2 | 78 | 84,8 | | |
| | Very Few | 11 | 34,4 | 21 | 65,6 | | |
| Attacks over network systems | Very Good | 6 | 23,1 | 20 | 76,9 | 5,027[a] | ,285 |
| | Good | 31 | 29,8 | 73 | 70,2 | | |
| | Average | 42 | 24,1 | 132 | 75,9 | | |
| | Few | 28 | 18,4 | 124 | 81,6 | | |
| | Very Few | 12 | 19,7 | 49 | 80,3 | | |
| "Social engineering" and "phishing" attacks | Yes | 45 | 28,3 | 114 | 71,7 | 3,619[a] | ,057 |
| | No | 74 | 20,7 | 284 | 79,3 | | |
| The knowledge of the concepts of HTTPS, secure connection, SSH, and TSL | Very Good | 3 | 25,0 | 9 | 75,0 | 3,698[a] | ,448 |
| | Good | 17 | 30,9 | 38 | 69,1 | | |
| | Average | 23 | 21,5 | 84 | 78,5 | | |
| | Few | 37 | 25,3 | 109 | 74,7 | | |
| | Very Few | 39 | 19,8 | 158 | 80,2 | | |
| How much do you know about cyber-attacks? | Very Good | 6 | 23,1 | 20 | 76,9 | 6,452[a] | ,168 |
| | Good | 22 | 28,9 | 54 | 71,1 | | |
| | Average | 41 | 27,0 | 111 | 73,0 | | |
| | Few | 30 | 21,7 | 108 | 78,3 | | |
| | Very Few | 20 | 16,0 | 105 | 84,0 | | |
| Do you follow the cyber-attacks in the world and your country? | Yes I do | 46 | 30,1 | 107 | 69,9 | 6,092[a] | ,014* |
| | No, I am not interested in | 73 | 20,1 | 291 | 79,9 | | |

***p<0,05**

When the significance of the relationships was evaluated ($p<0.05$), it was revealed that the sum of the rates of feeling very good and good about computer use is the highest in those aged 26 and over. The sum of the rates decreases as the age decreases.

Similarly, when the level of knowledge about computer hardware, operating systems, network systems and the level of knowledge about attacks made over network systems were examined, it can be seen that while the sum of the rates of feeling very good and good was the highest in those aged 26 and over, the sum of the rates decreases as the age decreases.

These results reveal that there is mostly a direct correlation between age and cybersecurity awareness.

As the student age increases, it can be considered reasonable that their cybersecurity awareness has also increased based on their experience and knowledge. However, it should be taken into account that the students' knowledge and the department they studied in may have prepared them with a groundwork, especially for computer and network security. Based on this situation, some analyses were undertaken in an attempt to understand whether the education level and departments of the students affect their cybersecurity awareness.

In Table 6, the results of the chi-square test performed to examine the relationship between education level and cybersecurity awareness are given.

The only significant result was between the level of education and the level of knowledge about the attacks made over network systems ($p<0.05$). The results show that the graduate students have more knowledge about network attacks than undergraduate students.

The results of the chi-square test conducted to examine the relationship between the students' majors and cybersecurity awareness are given in Table 7.

When considering the significance of the relationship ($p<0.05$), the highest percentage of students who were the best at using computers and had a high level of knowledge about computer hardware, operating systems, and network systems were found in the Engineering faculty. The lowest rate was found in the Veterinary faculty.

When the relationship between the students' major and their knowledge of the concepts of HTTPS, secure connection, SSL and TLS was examined, it was seen that the students from the Faculty of Engineering were at the top in terms of considering themselves competent in total, whereas the students from the Faculty of Theology were at the bottom.

**TABLE 11.** Knowledge of social engineering and phishing attacks.

| | | n | % |
|---|---|---|---|
| Knowing "social engineering" and "phishing" attacks | Yes | 159 | 30,8 |
| | No | 358 | 69,2 |

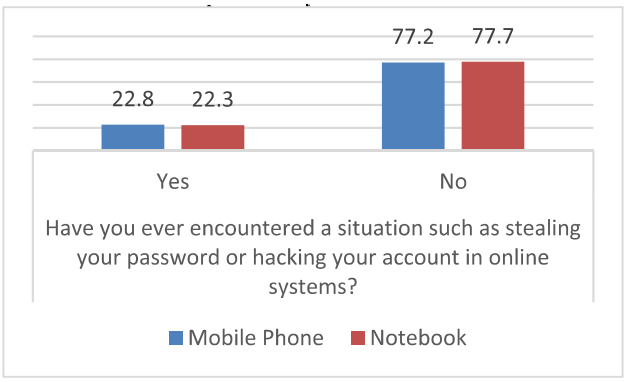


**FIGURE 1.** Rate of exposure to cyberattacks.

Since this section asks questions on specific topics related to network security, it is not surprising that the Science and Engineering students indicate that they are more proficient in the subject. It is possible that this rate has increased especially since the Computer Engineering students have taken courses related to these subjects during their education. However, considering all of the phases of the study, it has been revealed that there are other factors affecting cybersecurity awareness.

The relationship between the use of technological tools and cybersecurity awareness is illustrated in Tables 8-9. There is a significant relationship between the method of connecting to the internet and the level of feeling competent about computer use. This is as well as the level of knowledge about computer hardware, operating systems, and network systems ($p<0.05$). When the results were examined, those who connect to the internet using a notebook find themselves more competent in these matters.

Those who connect to the internet through their notebooks seem to be ahead compared to those who use other methods in terms of their level of knowledge about the attacks made over network systems, their hearing about ''social engineering'' and ''phishing'' attacks, and their level of knowledge about the HTTPS, secure connection, SSL, and TLS concepts.

Similarly, when the results were examined in terms of the level of knowledge about cyberattacks and their following of cyberattacks around the world, it can be seen that the rates are higher for those who connect to the internet via a notebook (Table 8).

Considering that most of the participants are from the Z generation, it is thought that their mobile phone use is more intense than their computer use. This situation is likely to have an effect on the statistical analysis results to come out in this direction.

**TABLE 12.** The relationship between computer and network knowledge and cyberattack awareness.

| | | "Social engineering" and "phishing" attacks | | | | Chi-Square | p |
|---|---|---|---|---|---|---|---|
| | | Yes | | No | | | |
| | | n | % | n | % | | |
| How competent do you feel about the use of computers? | Very Good | 45 | 53,6 | 39 | 46,4 | 42,284[a] | ,000* |
| | Good | 74 | 36,1 | 131 | 63,9 | | |
| | Average | 30 | 18,3 | 134 | 81,7 | | |
| | Few | 8 | 17,0 | 39 | 83,0 | | |
| | Very Few | 2 | 11,8 | 15 | 88,2 | | |
| The knowledge of computer hardware, operating systems, network systems | Very Good | 28 | 77,8 | 8 | 22,2 | 55,109[a] | ,000* |
| | Good | 56 | 37,3 | 94 | 62,7 | | |
| | Average | 51 | 24,6 | 156 | 75,4 | | |
| | Few | 22 | 23,9 | 70 | 76,1 | | |
| | Very Few | 2 | 6,3 | 30 | 93,8 | | |
| Attacks over network systems | Very Good | 18 | 69,2 | 8 | 30,8 | 59,852[a] | ,000* |
| | Good | 52 | 50,0 | 52 | 50,0 | | |
| | Average | 56 | 32,2 | 118 | 67,8 | | |
| | Few | 25 | 16,4 | 127 | 83,6 | | |
| | Very Few | 8 | 13,1 | 53 | 86,9 | | |

***p<0,05**

As shown in Table 9, the rate of students who have personal computers who feel competent about their computer use and who have knowledge about attacks made over network systems is higher than that among the other students. Likewise, having a personal computer increases the likelihood of hearing about attacks such as ''social engineering'' and ''phishing''. The reason why students who own personal computers are more cyber-aware than other students may be that they spend more time on their computer. It is also possible that they are more knowledgeable about malware as they probably install antivirus-like software on their personal computers upon purchase. On the other hand, security measures can often be ignored on computers that are in common use. Most of the time, people who use computers that are common use do not care if a precaution is taken to protect them from malicious software as they will only use them for a short time.

### C. SECURITY VULNERABILITIES AND CYBER THREATS

In this part, the analyses related to security vulnerabilities and cyber-attacks are presented. Whether the participants have been subjected to any form of cyberattack and whether they have faced the risk of a security vulnerability has been

**TABLE 13.** Technical knowledge of network systems and attacks.

| | | The knowledge of the concepts of HTTPS, secure connection, SSH, and TSL | | | | | | | | | | Chi-Square | p |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Very Good | | Good | | Average | | Few | | Very Few | | | |
| | | n | % | n | % | n | % | n | % | n | % | | |
| How competent do you feel about the use of computers? | Very Good | 10 | 11,9 | 20 | 23,8 | 24 | 28,6 | 15 | 17,9 | 15 | 17,9 | 122,790[a] | ,000* |
| | Good | 2 | 1,0 | 25 | 12,2 | 52 | 25,4 | 66 | 32,2 | 60 | 29,3 | | |
| | Average | 0 | 0,0 | 10 | 6,1 | 28 | 17,1 | 47 | 28,7 | 79 | 48,2 | | |
| | Few | 0 | 0,0 | 0 | 0,0 | 3 | 6,4 | 17 | 36,2 | 27 | 57,4 | | |
| | Very Few | 0 | 0,0 | 0 | 0,0 | 0 | 0,0 | 1 | 5,9 | 16 | 94,1 | | |
| The knowledge of computer hardware, operating systems, network systems | Very Good | 9 | 25,0 | 12 | 33,3 | 9 | 25,0 | 3 | 8,3 | 3 | 8,3 | 195,211[a] | ,000* |
| | Good | 2 | 1,3 | 29 | 19,3 | 45 | 30,0 | 37 | 24,7 | 37 | 24,7 | | |
| | Average | 1 | ,5 | 12 | 5,8 | 45 | 21,7 | 70 | 33,8 | 79 | 38,2 | | |
| | Few | 0 | 0,0 | 2 | 2,2 | 8 | 8,7 | 29 | 31,5 | 53 | 57,6 | | |
| | Very Few | 0 | 0,0 | 0 | 0,0 | 0 | 0,0 | 7 | 21,9 | 25 | 78,1 | | |
| Attacks over network systems | Very Good | 9 | 34,6 | 4 | 15,4 | 10 | 38,5 | 0 | 0,0 | 3 | 11,5 | 250,258[a] | ,000* |
| | Good | 3 | 2,9 | 27 | 26,0 | 33 | 31,7 | 26 | 25,0 | 15 | 14,4 | | |
| | Average | 0 | 0,0 | 18 | 10,3 | 43 | 24,7 | 58 | 33,3 | 55 | 31,6 | | |
| | Few | 0 | 0,0 | 6 | 3,9 | 18 | 11,8 | 50 | 32,9 | 78 | 51,3 | | |
| | Very Few | 0 | 0,0 | 0 | 0,0 | 3 | 4,9 | 12 | 19,7 | 46 | 75,4 | | |

*p<0,05

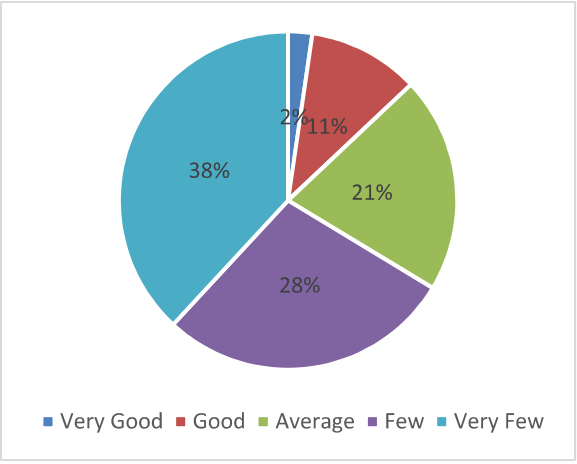


**FIGURE 2.** Knowledge of HTTPS, secure connection, SSL, and TLS concepts.

**TABLE 14.** Students' status following cyberattacks.

| | | Do you follow the cyber attacks in the world and your country? | | | | Chi-Square | p |
|---|---|---|---|---|---|---|---|
| | | Yes | | No | | | |
| | | n | % | n | % | | |
| How much do you know about cyber-attacks? | Very Good | 20 | 76,9 | 6 | 23,1 | 117,689[a] | ,000* |
| | Good | 45 | 59,2 | 31 | 40,8 | | |
| | Average | 61 | 40,1 | 91 | 59,9 | | |
| | Few | 20 | 14,5 | 118 | 85,5 | | |
| | Very Few | 7 | 5,6 | 118 | 94,4 | | |

*p<0,05

examined. Looking at the results, the rate of those who have encountered a situation such as having their password stolen or their account hacked in an online system is 23.0% (Figure 1).

To determine whether there is a relationship between connecting to the internet via phone or notebook and the possibility of being exposed to cyber threats, an analysis was conducted. As shown in Table 10, there was found to be no significant relationship between the method of connecting to the Internet and the fact that the passwords were stolen from online systems or the account hacked (p>0,05).

Interestingly, it was observed that the majority of students who were exposed to cyber-attacks such as password stealing or account hacking in online systems were students who followed cyberattacks in the news (Table 10). This is probably because the students are not aware of the concept of cyber threat or they are not aware of it when they encounter such an attack.

### D. CYBERSECURITY KNOWLEDGE

Information obtained on cybersecurity plays an important role in increasing cybersecurity awareness. For this reason, in this part, various analyses about the cybersecurity knowledge of the students are presented. As can be seen in Table 11 and Figure 2, the rate of participants who have heard of "social engineering" and "phishing" attacks is 30.8%. The rate of those who have a good or higher level of knowledge about the HTTPS, secure connection, SSL, and TLS concepts is 12.9% in total.

According to the results, the number of participants who have never heard of the concepts of "social engineering" and "phishing" is more than twice that of those who have.

The results of the chi-square test conducted to examine the relationship between the awareness of "social engineering"

**TABLE 15.** The relationship between the students' technical knowledge and their following of cyberattacks.

| | | How much do you know about cyber-attacks? | | | | | | | | | | Chi-Square | p |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Very Good | | Good | | Average | | Few | | Very Few | | | |
| | | n | % | n | % | n | % | n | % | n | % | | |
| "Social engineering" and "phishing" attacks | Yes | 22 | 84,6 | 32 | 42,1 | 70 | 46,1 | 23 | 16,7 | 12 | 9,6 | 95,848[a] | ,000* |
| | No | 4 | 15,4 | 44 | 57,9 | 82 | 53,9 | 115 | 83,3 | 113 | 90,4 | | |
| The knowledge of the concepts of HTTPS, secure connection, SSH, and TSL | Very Good | 10 | 38,5 | 1 | 1,3 | 1 | ,7 | 0 | 0,0 | 0 | 0,0 | 344,110[a] | ,000* |
| | Good | 9 | 34,6 | 21 | 27,6 | 17 | 11,2 | 7 | 5,1 | 1 | ,8 | | |
| | Average | 5 | 19,2 | 31 | 40,8 | 52 | 34,2 | 16 | 11,6 | 3 | 2,4 | | |
| | Few | 0 | 0,0 | 14 | 18,4 | 48 | 31,6 | 53 | 38,4 | 31 | 24,8 | | |
| | Very Few | 2 | 7,7 | 9 | 11,8 | 34 | 22,4 | 62 | 44,9 | 90 | 72,0 | | |

*p<0,05

and "phishing" attacks and having knowledge about computer and network security issues are given in Table 12.

When the results were examined, the rate of being aware of cyberattacks was found to be the highest in those who feel very good about computer use, whereas the rate of awareness decreases as the computer use competence decreases.

Similarly, as the level of knowledge on computer hardware, operating systems, network systems, and network attacks increases, the awareness of attacks also increases.

As can be seen from the results, it is normal that having knowledge about the concepts related to computer and network security increases the level of awareness of cyber-attacks. This situation shows that possible cybersecurity training organized for students will be beneficial when it comes to developing their cybersecurity awareness.

Additional analyses were needed to understand whether the current level of knowledge of the participants is sufficient for cybersecurity awareness. This is because sometimes the fact that participants state that they are "informed" may not mean that they are actually knowledgeable. For this reason, the results of the analysis where questions were asked about specific concepts related to network security may allow for a more accurate inference.

The results of the chi-square test are given below to help analyze whether the students who feel competent about computer use and network knowledge know about concepts such as HTTPS, secure connections, SSL, and TLS (Table 13).

When the results were examined, 11.9% felt very good about computer use, 25.0% felt that their knowledge of computer hardware, operating systems, and network systems was decent, and 34.6% of those who felt very good about attacks over network systems had a very good knowledge of HTTPS, secure connections, SSL, and TLS as concepts.

This shows that as the level of interest and knowledge of network systems increases, the dominance of technical concepts also increases.

**TABLE 16.** Students' cyber security awareness training status.

| | | n | % |
|---|---|---|---|
| Have you ever received cyber security awareness training? | Yes | 120 | 23,2 |
| | No | 397 | 76,8 |
| If you haven't, would you like to receive such training? | Yes | 360 | 90,7 |
| | No | 37 | 9,3 |

**TABLE 17.** Distribution of those who want to receive cybersecurity training by faculty.

| | | If you haven't, would you like to receive such training? | | | | Chi-Square | p |
|---|---|---|---|---|---|---|---|
| | | Yes | | No | | | |
| | | n | % | n | % | | |
| Faculty | Humanities | 99 | 89,2 | 12 | 10,8 | 12,463[a] | ,132 |
| | Sciences | 30 | 90,9 | 3 | 9,1 | | |
| | Fine Arts | 15 | 88,2 | 2 | 11,8 | | |
| | Economics and Management | 85 | 93,4 | 6 | 6,6 | | |
| | Communication | 18 | 75,0 | 6 | 25,0 | | |
| | Theology | 21 | 95,5 | 1 | 4,5 | | |
| | Engineering | 59 | 95,2 | 3 | 4,8 | | |
| | Veterinary Medicine | 13 | 81,3 | 3 | 18,8 | | |
| | Agriculture | 20 | 95,2 | 1 | 4,8 | | |

*p<0,05

Communication tools such as social media sites, news sources on the internet, and television often provide information about cyberattacks and the necessity of precautions being taken. An analysis has been undertaken to look into whether these environments have an effect on the development of cybersecurity awareness. The results show that there is a significant relationship between the students' status of following the cyberattacks in their own country and the world and their knowledge level about cyberattacks ($p<0.05$). When the results were examined, 76.9% of those who felt that their level of knowledge about cyberattacks was very good

**TABLE 18.** The effect of getting cybersecurity training on computer and network knowledge.

| | | Have you ever received cyber security awareness training? | | | | Chi-Square | p |
|---|---|---|---|---|---|---|---|
| | | Yes | | No | | | |
| | | n | % | n | % | | |
| How competent do you feel about the use of computers? | Very Good | 42 | 35,0 | 42 | 10,6 | 51,138[a] | ,000* |
| | Good | 51 | 42,5 | 154 | 38,8 | | |
| | Average | 21 | 17,5 | 143 | 36,0 | | |
| | Few | 5 | 4,2 | 42 | 10,6 | | |
| | Very Few | 1 | ,8 | 16 | 4,0 | | |
| The knowledge of computer hardware, operating systems, network systems | Very Good | 24 | 20,0 | 12 | 3,0 | 60,783[a] | ,000* |
| | Good | 47 | 39,2 | 103 | 25,9 | | |
| | Average | 37 | 30,8 | 170 | 42,8 | | |
| | Few | 11 | 9,2 | 81 | 20,4 | | |
| | Very Few | 1 | ,8 | 31 | 7,8 | | |
| Attacks over network systems | Very Good | 18 | 15,0 | 8 | 2,0 | 76,136[a] | ,000* |
| | Good | 43 | 35,8 | 61 | 15,4 | | |
| | Average | 41 | 34,2 | 133 | 33,5 | | |
| | Few | 13 | 10,8 | 139 | 35,0 | | |
| | Very Few | 5 | 4,2 | 56 | 14,1 | | |
| "Social engineering" and "phishing" attacks | Yes | 75 | 62,5 | 84 | 21,2 | 73,952[a] | ,000* |
| | No | 45 | 37,5 | 313 | 78,8 | | |
| The knowledge of the concepts of HTTPS, secure connection, SSH, and TSL | Very Good | 8 | 6,7 | 4 | 1,0 | 78,239[a] | ,000* |
| | Good | 27 | 22,5 | 28 | 7,1 | | |
| | Average | 43 | 35,8 | 64 | 16,1 | | |
| | Few | 26 | 21,7 | 120 | 30,2 | | |
| | Very Few | 16 | 13,3 | 181 | 45,6 | | |
| How much do you know about cyber-attacks? | Very Good | 19 | 15,8 | 7 | 1,8 | 129,515[a] | ,000* |
| | Good | 39 | 32,5 | 37 | 9,3 | | |
| | Average | 50 | 41,7 | 102 | 25,7 | | |
| | Few | 8 | 6,7 | 130 | 32,7 | | |
| | Very Few | 4 | 3,3 | 121 | 30,5 | | |
| Do you follow the cyber-attacks in the world and your country? | Yes I do | 74 | 61,7 | 79 | 19,9 | 77,152[a] | ,000* |
| | No, I am not interested in | 46 | 38,3 | 318 | 80,1 | | |

***p<0,05**

followed cyberattack developments through various media tools (Table 14).

When the students' awareness of ''social engineering'' and ''phishing'' attacks was examined, 84.6% of the students who claimed that their knowledge level about cyberattacks was very good stated that they knew about ''social engineering'' and ''phishing'' attacks. However, as can be seen in Table 15, only 38.5% of the students who thought that they have a very good level of knowledge about cyber threats and attacks had a very good knowledge of the HTTPS, secure connections, SSL, and TLS concepts.

This situation not only shows that the majority of the participants have a lack of knowledge about network security concepts but it also reveals the fact that the participants thought that they had an efficient level of cyber awareness even though they have relatively superficial information. In this case, it can be concluded that cybersecurity education including technical details is necessary for the students.

### *E. CYBERSECURITY TRAINING*

The analysis up to this stage has revealed that the participants mostly need to receive proper cybersecurity training. There is a need for a quantitative analysis looking into whether the students have received any cybersecurity training before, regardless of the quality of the training. For this reason, in this part, some of the analyses related to the cybersecurity training of the participants are presented. The rate of those who have never received cybersecurity awareness training is 76.8% and the ratio of those who have not received training before and who want to receive this training is 90.7% (Table 16).

Considering the distribution across the faculties and the willingness to receive cybersecurity training ($p>0.05$), no particular faculty came to the fore as shown in Table 17. This shows that regardless of the faculty, the majority of students want to receive cybersecurity education.

When the chi-square analysis on the effect of having cybersecurity training on computer and network knowledge was examined, the following results were obtained. It was observed that the students who had previously received cybersecurity awareness training felt much better about their computer use. Similarly, the results showed that the level of knowledge about computer hardware, operating systems, network systems, and cyberattacks was higher in those who had received such an education. Most of the students who had heard of attacks such as social engineering and phishing, and

**TABLE 19.** Students' awareness of cybercrime and cyber law.

| | | n | % |
|---|---|---|---|
| Do you know that cyberattacks and trying to obtain the personal information of others through hacking are a form of crime and legal sanction? | Yes | 405 | 78,3 |
| | No | 112 | 21,7 |
| Do you have information about international agreements or conventions regarding cybercrime? | Yes | 133 | 25,7 |
| | No | 384 | 74,3 |
| Have you encountered someone who has been prosecuted for cybercrime before? | Yes | 33 | 6,4 |
| | No | 484 | 93,6 |

who have a high level of knowledge about the concepts of HTTPS, secure connection, SSL, and TSL, were also educated (Table 18).

It is obvious that the students who receive an education have more advantages in terms of their cybersecurity awareness compared to the students who do not receive such an education. However, the quality of the education given to the students is important as it is a necessity. High-tech training that includes the key points of network security will likely yield better results. This is because without knowing the working mechanisms behind cyberattacks or having sufficient knowledge about security vulnerabilities, it will not be possible to understand the importance of the precautions to be taken.

### *F. AWARENESS OF CYBERCRIMES AND LAWS*

It is important to be aware of the legal dimension of cybercrimes as well as the necessity of being knowledgeable about the technical details of cybersecurity. Knowing that attempting to violate the privacy of personal information through cyberattacks is a crime and that there are sanctions will allow people to act more carefully in this regard.

In this part, some of the analyses related to the awareness of cybercrimes and laws is presented. The rate of those who know that cyberattacks and trying to obtain the personal information of others through hacking are crimes and involve legal sanctions is 78.3%. The rate of those who know about the international agreements and conventions related to cybercrime is 25.7%, and the rate of those who have previously encountered someone who is on trial for cybercrime is 6.4% (Table 19).

The results of the chi-square test conducted to examine the relationship between the students' faculties and the state of knowing that cyber-attacks are a crime and have legal sanctions were evaluated. The awareness level of the students in the faculty of communication was the highest. The students of the faculty of fine arts had the lowest awareness level (Table 20).

The fact that the communication faculty students have some law courses in their curriculum may be the reason for this situation. In addition, if cybersecurity is given as an elective course to all students regardless of their faculty, their awareness is likely to increase.

**TABLE 20.** Distribution of the students' awareness of cybercrime and cyber law by faculty.

| | | Do you know that cyber-attacks and trying to obtain the personal information of others through hacking are crimes and legal sanctions? | | | | Chi-Square | p |
|---|---|---|---|---|---|---|---|
| | | Yes | | No | | | |
| | | n | % | n | % | | |
| Faculty | Humanities | 102 | 79,1 | 27 | 20,9 | 22,403[a] | ,004* |
| | Sciences | 23 | 59,0 | 16 | 41,0 | | |
| | Fine Arts | 13 | 54,2 | 11 | 45,8 | | |
| | Economics and Management | 92 | 79,3 | 24 | 20,7 | | |
| | Communication | 28 | 87,5 | 4 | 12,5 | | |
| | Theology | 17 | 73,9 | 6 | 26,1 | | |
| | Engineering | 93 | 85,3 | 16 | 14,7 | | |
| | Veterinary Medicine | 17 | 81,0 | 4 | 19,0 | | |
| | Agriculture | 20 | 83,3 | 4 | 16,7 | | |

**TABLE 21.** Examining the relationship between the faculty and students' knowledge of the international agreements and conventions on cybercrime.

| | | Do you have information about international agreements or conventions regarding cybercrime? | | | | Chi-Square | p |
|---|---|---|---|---|---|---|---|
| | | Yes | | No | | | |
| | | n | % | n | % | | |
| Faculty | Humanities | 27 | 20,9 | 102 | 79,1 | 14,853[a] | ,062 |
| | Sciences | 8 | 20,5 | 31 | 79,5 | | |
| | Fine Arts | 6 | 25,0 | 18 | 75,0 | | |
| | Economics and Management | 34 | 29,3 | 82 | 70,7 | | |
| | Communication | 10 | 31,3 | 22 | 68,8 | | |
| | Theology | 6 | 26,1 | 17 | 73,9 | | |
| | Engineering | 38 | 34,9 | 71 | 65,1 | | |
| | Veterinary Medicine | 2 | 9,5 | 19 | 90,5 | | |
| | Agriculture | 2 | 8,3 | 22 | 91,7 | | |

*p<0,05

As shown in Table 21, there is a non-significant relationship between the knowledge of international agreements and conventions related to cybercrime and the students' faculty (p>,05).

## V. CONCLUSION AND FUTURE DIRECTIONS

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 cybersecurity 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. Cybersecurity 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 cybersecurity 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 cybersecurity 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 cybersecurity 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.

## REFERENCES


[1] M. Zwilling, G. Klien, D. Lesjak, Ł. 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/pdffiles1/Digitization/118214NCJRS.pdf

[9] *Definition of Cybersecurity*. Accessed: Mar. 2, 2022. [Online]. Available: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.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. Wakefield, S. Kim, and T. Kim, "Security awareness: The first 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 gamified 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, New Zealand, Dec. 2016, pp. 223–228.

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

[27] A. Garba, M. Siraj, S. Othman, and M. Musa, "A study on cybersecurity awareness among students in Yobe state university, Nigeria: A quantitative approach," *Int. J. Emerg. Technol.*, vol. 11, no. 5, pp. 41–49, 2020.

[28] G. H. Kirwan, C. Fullwood, and B. Rooney, "Risk factors for social networking site scam victimization among Malaysian students," *Cyberpsychology, Behav., Social Netw.*, vol. 21, no. 2, pp. 123–128, Feb. 2018.

[29] K. Senthilkumar and E. Sathishkumar, ''A survey on cyber security awareness among college students in Tamil Nadu,'' in *Proc. IOP Conf. Mater. Sci. Eng.*, 2017, pp. 1–10.
[30] A. A. Al Shamsi, ''Effectiveness of cyber security awareness program for young children: A case study in UAE,'' *Int. J. Inf. Technol. Lang. Stud.*, vol. 3, no. 2, pp. 8–29, 2019.
[31] A. Moallem, ''Cyber security awareness among college students,'' in *Advances in Human Factors in Cybersecurity* (Advances in Intelligent Systems and Computing). 2019, pp. 79–87.
[32] R. Ismailova, G. Muhametjanova, T. D. Medeni, I. T. Medeni, D. Soylu, and O. A. Dossymbekuly, ''Cybercrime risk awareness rate among students in central asia: A comparative study in Kyrgyzstan and Kazakhstan,'' *Inf. Secur. Journal: A Global Perspective*, vol. 28, nos. 4–5, pp. 127–135, Sep. 2019.

**MEHMET EMIN ERENDOR** was born in Kilis, Turkey, in 1985. He received the bachelor's degree in international relations from the University of Kırıkkale, Turkey, in 2008, the master's degree in international law: rights and responsibilities from the University of Sussex, Brighton, in 2011, and the Ph.D. degree in international relations from the University of Southampton, in 2017.

From 2017 to 2018, he worked as a Research Assistant at the University of Çukurova. Since 2018, he has been an Associate Professor with the Department of International Relations, Adana Alparslan Türkeş Science and Technology University. He is currently working with the Department of International Relations, Kyrgyzs-Turkish Manas University. His research interests include cybersecurity, terrorism, human rights, humanitarian interventions, and international organizations.

**MERVE YILDIRIM** received the B.Sc. degree in computer engineering from Haliç University, Turkey, in 2010, and the M.Sc. degree in advanced computer science and the Ph.D. degree in informatics and software engineering from the University of Sussex, U.K., in 2012 and 2017, respectively.

She is currently an Assistant Professor with the Department of Computer Engineering, Erzurum Technical University, Turkey. She has been working as the Head of the Department, since 2021. Her research interests include cybersecurity, the Internet of Things, human–computer interactions, and network systems.