Determination of Cyber Security Issues and Awareness Training for University Students

https://doi.org/10.3991/ijet.v17i18.32193

Botagoz Khamzina[1], Nabuova Roza[2], Gulsara Zhussupbekova[3], Karlygash Shaizhanova[4], Aiganym Aten[5], Baikulova Aigerim Meirkhanovna[4](✉)
[1]Saken Seifullin Kazakh Agro Technical University, Nur-Sultan, Kazakhstan
[2]Kazakh National Women's Teacher Training University, Almaty, Kazakhstan
[3]Sh. Ualikhanov Kokshetau University, Kokshetau, Kazakhstan
[4]Abai Kazakh National Pedagogical University, Almaty, Kazakhstan
[5]Al-Farabi Kazakh National University, Almaty, Kazakhstan
a.baikulova@abaiuniversity.edu.kz

Abstract—In this study, it is aimed to determine the cyber security problems and awareness training to university students. The research was carried out in the fall semester of 2021–2022. The study, which was carried out with the participation of 410 university education and psychology students, was carried out using the survey model. In the research, 4-week cyber security and cyberattack training was given online to university students. The cyber security measurement tool was developed and used by the researchers in order to collect data in the study. The data collection tool used in the research was delivered and collected by the online method. The analysis of the data was made using the SPSS programme, frequency analysis and *t*-test. The results were added to the research in the form of tables. As a result of the research, it was concluded that university cyber security and cyberattack training was designed and they were good in this field.

Keywords—cyber security, distance education, university students

1 Introduction

With the widespread use of the Internet all over the world, information and communication technologies have developed and this development has brought along easy accessibility [1,31]. The Internet has become an important need for society, as it makes daily tasks, such as access to information, information sharing, communication and shopping, easy and fast [2]. In the process of meeting these needs, a new and extremely important security area has emerged for Internet users. Along with the need for cyber security, the necessity for all Internet users to be aware of cyber security has emerged [32].

1.1 Theoretical and conceptual framework

The concept of cyber threat is seen as a concept that has become increasingly important in recent years and researches have been conducted on it. Cyber threats are generally expressed as obtaining confidential information belonging to other people by taking advantage of the vulnerabilities of the systems through programmes written by malicious people for the purpose of committing cybercrime [3]. Cyberattacks aimed at obtaining important information for individuals and societies are expressed as the systematic and coordinated attacks on the information systems or communication infrastructures of the targeted persons, companies, institutions and organisations, for commercial, political or military purposes [4]. Cyber warfare, on the other hand, covers infiltration activities carried out by one country to damage another country's Internet and information networks or to prevent it from working temporarily [5].

The concept of cyber security was first used by computer engineers in the 1990s to express security problems related to networked computers. Cyber security covers the whole of tools, policies, security concepts, guidelines, risk management approaches, activities, trainings, applications and technologies used to protect the assets of institutions, organisations and users in the cyber environment [6]. It is of great importance to draw attention to the issue of cyber security in order to prevent cybercrimes that are becoming more and more widespread in the Internet age we live in and not to be exposed to the possible consequences of these crimes [7]. In the literature, it is stated that human-induced errors have an important role behind exposure to cyberattacks and the negative consequences of these attacks by achieving their goals [8].

Goodrich and Tamassio [9] evaluated the provision of cyber security in three dimensions as 'confidentiality, integrity and availability'. Confidentiality means that the information can only be accessed by the owner or related persons. Integrity is expressed as the preservation of the existing structure of information without being altered, corrupted or destroyed. Availability, on the other hand, means that the information is accessible to the relevant people when necessary. The three aforementioned features are considered to be antecedents of cyber security.

Negative situations in cyber space and the increase in cyber threats day by day affect all countries of the world negatively. In order to minimise the negativities experienced, the need for qualified personnel must be met. For this purpose, many countries in various regions of the world provide cyber security training within universities [10].

1.2 Related research

Aksakallı [11] analysed the type and size of attacks on the cloud system in his research. In the research, the security problems in the cloud system were determined by scanning the literature. Then, cyber security threats and cyberattacks are classified. As a result of the research, it was emphasised that urgent measures should be taken to solve the cyber security problems in the cloud system.

Halevi et al. [12] evaluated the cultural and psychological dimensions of cyber security in their research aimed at increasing cyber security. In the research, it is stated that the importance to be taken in the field of cyber security is increasing day by day. This research was carried out in four countries: United States of America, India, United

Arab Emirates and Ghana. As a result of the research, it was determined that different countries of cross-cultural research have similar concerns and difficulties regarding cyber security. It is also stated that technology-based measures can be taken by taking advantage of the power of technology in providing cyber security, and it is also stated that cyber security awareness should be given to people for cyber security [13].

Agamba and Keengwe [14], in their study; investigated the pre-service teachers' precautionary behaviours to prevent cybercrime. In the research, the views of pre-service teachers on cybercrime awareness and prevention of cybercrime were taken. As a result of the research, it was determined that the pre-service teachers' cybercrime knowledge and awareness of using software related to cyber security were at a high level. However, it has been emphasised that teacher candidates are insufficient to take the necessary precautions to prevent cybercrime.

Pusey and Sadera [15] evaluated pre-service teachers' competencies in cyber security and informatics ethics. The competencies of teacher candidates to provide education in the field of cyber security were determined in line with the opinions of the teachers. As a result of the research, it has been revealed that teacher candidates have insufficient knowledge about information security and ethics and they are not qualified to provide training on this subject.

Taha and Dahabiyeh [16], on the other hand, stated in their research on cyber security that individuals' information security awareness is lacking and this deficiency opens the door to cyber security attacks. In addition, when the studies in the literature are examined, there are also studies emphasising the importance of running training programmes to improve the information security awareness of individuals in institutions or organisations [17–19].

1.3 Purpose of the research

The purpose of this research is to identify cyber security problems for university students and to provide online awareness training. In this direction, answers to the following questions were sought:

1. What are the cyber security scale scores of university students before and after online cyber security and cyberattack awareness training?
2. How are the cyber security perceptions of university students according to gender variable before and after online cyber security and cyberattack awareness training?
3. What are the cyber security perceptions of university students according to the class variable before and after online cyber security and cyberattack awareness training?

2 Method and materials

This section includes information about the method used in the research, the data collection tool, the study group from which the data will be collected and how the data will be evaluated.

2.1 Research method

The descriptive survey method, one of the quantitative research models, was used in the study. King and He [20] describe the descriptive survey method as a quantitative approach. Descriptive surveys are studies in which the views of groups on any phenomenon or subject are described. Therefore, in this study, the descriptive survey method was preferred in order to describe the cyber security and cyberattack awareness of university students participating in the research.

2.2 Participants

In the literature, there are different evaluations for determining the sample size in quantitative studies. In this study, the evaluation of at least 100–150 samples, which is the sample size determined by Ding et al. [21], was taken into consideration. Accordingly, 223 students were selected for the pilot application of the cyber security scale developed to collect research data, and 410 students were selected for the final application. The students participating in the research consisted of students studying in the field of education and psychology in the 2021–2022 academic year at various universities in Kazakhstan, who agreed to participate voluntarily in the research. Information on the demographic distribution of the students is given in Tables 1 and 2 in the findings section of the study.

2.3 Data collection tools

Research data were collected with the cyber security scale developed by the researchers. The measurement tool was applied twice, before and after the online cyber security and cyberattack awareness training was given to the students.

Cyber security scale. Certain steps were followed during the development of the scale. These steps are creation of the item pool and receiving expert opinion, conducting content and face validity studies, conducting a pilot application and obtaining data, analysing the obtained data, conducting validity and reliability studies and finally creating the final version of the scale with expert opinions. In the first stage, a literature review on cyber security was conducted, and an item pool of 96 items was created considering the education level of the students. In the second stage, item content validity analysis was carried out using the Lawshe technique [22,23]. In order to determine the comprehensive validity of 96 items in the item pool, the opinions of nine experts were consulted. In line with expert opinions, 23 items with a content validity index above 0.90 were determined to be used in the scale. In the third stage, 223 students studying in psychology departments at universities were selected for the pilot application of the scale. 147 female and 76 male students participated in the pilot application.

In the fourth stage, SPSS 20.0 and SPSS Amos 25.0 programmes were used in the analysis of the data obtained as a result of the pilot application. The cyber security scale prepared for the pilot application was prepared in a 5-point Likert type. ‘Always’ was evaluated as 5 points, ‘Often’ as 4 points, ‘Sometimes’ as 3 points, ‘Rarely’ as 2 points and ‘Never’ as 1 point. Considering the item score ranges to be equal, 5.00–4.20 is always, 4.19–3.40 is often, 3.39–2.60 is sometimes, 2.59–1.80 is rarely and 1.79–1.00

is rated as never. In the fifth stage, the Kaiser–Meyer–Olkin (KMO) coefficient and Bartlett sphericity test were calculated before the exploratory and confirmatory factor analyses. The KMO value was found to be 0.812 and Bartlett's test was found to be below $P < 0.05$ ($P = 0.000$), and it was understood that the data set was suitable for factor analysis. Then, exploratory factor analysis was carried out. The eigenvalue and variance ratios of the scale were examined and two factors with eigenvalues greater than 1 were found. The variance rate explained by the factors was 92.6%.

According to the scree plot, the item factor load was found to be over 30, and two items loading a different factor were removed from the scale. After the exploratory factor analysis, confirmatory factor analysis was carried out. The goodness-of-fit index of the scale was $\chi^2/df = 1.887$, GFI = 0.992, CFI = 0.965, NFI-TLI = 0.927–0.953 and RMSEA = 0.051. The goodness-of-fit index of the scale was found to be high. The reliability study of the scale consists of 2 sub-dimensions and 21 items. The first sub-dimension is 'cyber security measures' and the second sub-dimension is 'cyberattack awareness'. There are 12 items in the first sub-dimension and 9 items in the second sub-dimension. The Cronbach alpha internal consistency coefficient of the scale was found to be 0.83. The results of exploratory and confirmatory factor analyses reveal that the Cyber Security Scale is a reliable measurement tool. In the sixth stage, the final version of the scale was converted into a form by taking expert opinion again, making it ready for application. The cyber security scale is given in Appendix 1.

Online cyber security and cyber attack awareness training. The 4-week online cyber security and cyberattack awareness training is programmed to be online for 2 hours, 2 days a week, for a total of 16 hours. The content of the training includes cyber threat, cyberattack, cyber warfare and cyber security. It is aimed to teach the students during the education by supporting the conceptual dimension of the subject with examples. In this direction, weekly gains were determined.

Week 1: Comprehending the concepts of cyber security and comprehending possible types of cyber threats. Week 2: Comprehending cyberattacks related to malicious software, cyber hackers, network and system weaknesses, having knowledge about the causes of cyber wars and how they are done. Week 3: Understanding the importance of cyber security and understanding cyber security applications. Week 4: Knowing what personal rights are in the field of cyber security and learning the crime dimension and legal processes in cyberattacks.

In order to ensure student gains, students were expected to show sensitivity about participation in the programme.

2.4 Data collection process

The data of the research were collected over a period of approximately 2 months due to the application of the cyber security scale twice and the provision of online cyber security and cyber awareness training between the two applications.

2.5 Data collection analysis

SPSS 20.0 programme was used in the analysis of the research data. The Cyber Security Scale was applied to the study group of the research twice, before and after the 4-week online cyber security and cyberattack awareness training. According to the Kolmogorov–Smirnov normality test results, since $P > .05$ was found, it was determined that the data showed normal distribution. For this reason, the answers given by the students to the items in the scale were converted into findings by applying parametric tests. In the findings, frequency, percentage, standard deviation, weighted average calculations and *t*-test results are given in tables.

3 Results

In this study, the findings regarding the 'cyber security measures' and 'cyberattack awareness' of university students were tested with the Cyber Security Scale.

Demographic information regarding the gender distribution of university students participating in the research is given in Table 1.

Table 1. Distribution of students by gender

Gender	F	%
Female	236	57.6
Male	174	42.4
Sum	410	100

Demographic information regarding the gender distribution of university students participating in the research is given in Table 1. 57.6% of the students participating in the research were female and 42.4% were male. A total of 410 students, 236 women and 174 men, participated in the study.

In Table 2, demographic information about the class distribution of the university students participating in the research is given.

Table 2. Class distribution of students

Class	F	%
1. Class	94	22.9
2. Class	106	25.9
3. Class	112	27.3
4. Class	98	23.9
Sum	410	100

In Table 2, the distribution of the university students participating in the research according to the class variable is given. 22.9% of the students are 1st grade, 25.9% 2nd grade, 27.3% 3rd grade and 23.9% 4th grade.

Before online cyber security and cyberattack awareness training. In Table 3, the online cyber security scale, cyber awareness measures, cyberattack awareness sub-dimensions and the overall mean and standard deviation of the scale are given.

Table 3. Cyber security scale and its sub-dimensions

	X	SS
Cyber security measures sub-dimension	2.19	0.889
Cyberattack awareness sub-dimension	2.28	0.675
Cyber Security Scale	2.21	0.719

When Table 3 is examined, it is seen that university students participating in the research have a low level of awareness in the cyber security measures sub-dimension (X = 2.19) and in the cyberattack awareness sub-dimension (X = 2.28). In general, it was concluded that the cyber security awareness of university students (X = 2.21) is at a low level in the cyber security scale.

In Table 4, the cyber security perceptions of the students participating in the research before the online cyber security and cyberattack awareness training are given according to the gender variable.

Table 4. The *t*-test results of students' cyber security perceptions by gender variable before online cyber security and cyberattack awareness training

Gender	N	X	SS	F	P
Female	236	1.93	0.466	19.613	.000
Male	174	2.61	0.588		

When Table 4 is examined, it is seen that there is a significant difference (F = 19.613, P < .05) between university students' cyber security awareness before online cyber security and cyberattack awareness training according to gender variable. According to the *t*-test results, it was determined that the awareness of male students was higher than that of female students.

In Table 5, the cyber security perceptions of the students participating in the research before the online cyber security and cyberattack awareness training are given according to the class variable.

Table 5. The *t*-test results of students' cyber security perceptions by class variable before online cyber security and cyberattack awareness training

Class	N	X	SS	F	P
1. Class	94	2.27	0.568	6.715	.516
2. Class	106	2.23	0.597		
3. Class	112	2.19	0.601		
4. Class	98	2.16	0.577		

In Table 5, the cyber security awareness of university students was evaluated before the online cyber security and cyberattack awareness training according to the grade level they are studying. According to the table, X = 2.27 for 1st grade, X = 2.23 for 2nd grade, X = 2.19 for 3rd grade and X = 2.16 for 4th grade. It has been determined that there is no significant difference between the cyber security awareness of university students according to the class variables they are studying.

After online cyber security and cyberattack awareness training. In Table 6, the cyber security scale, cyber awareness measures, cyberattack awareness sub-dimensions and the overall mean and standard deviation of the scale are given.

Table 6. Cyber security scale and its sub-dimensions

	X	SS
Cyber security measures sub-dimension	3.56	0.926
Cyberattack awareness sub-dimension	3.63	0.915
Cyber Security Scale	3.59	0.881

When Table 6 is examined, it is seen that university students participating in the research have a high level of awareness in the cyber security measures sub-dimension (X = 3.56) and in the cyberattack awareness sub-dimension (X = 3.63). In general, it was concluded that the cyber security awareness of university students (X = 3.59) is at a high level in the cyber security scale.

In Table 7, the cyber security perceptions of the students participating in the research after the online cyber security and cyberattack awareness training are given according to the gender variable.

Table 7. The *t*-test results of students' cyber security perceptions by gender variable after online cyber security and cyberattack awareness training

Gender	N	X	SS	F	P
Female	236	3.58	0.710	11.442	.265
Male	174	3.61	0.792		

When Table 7 is examined, it is seen that there is no significant difference between university students' cyber security awareness according to gender after online cyber security and cyberattack awareness training (F = 11.442, P > .05).

In Table 8, the cyber security perceptions of the students participating in the research after the online cyber security and cyberattack awareness training are given according to the class variable.

Table 8. The *t*-test results of students' cyber security perceptions by class variable after online cyber security and cyberattack awareness training

Class	N	X	SS	F	P
1. Class	94	3.56	0.466	19.215	.425
2. Class	106	3.59	0.514		
3. Class	112	3.61	0.409		
4. Class	98	3.60	0.489		

In Table 8, cyber security awareness of university students was evaluated after online cyber security and cyberattack awareness training according to their grade level. According to the table, X = 3.56 is for 1st grade, X = 3.59 for 2nd grade, X = 3.61 for 3rd grade and X = 3.60 for 4th grade. It has been determined that there is no significant difference between the cyber security awareness of university students according to the class variable they are studying.

4 Discussion

University students participating in the research were given online cyber security and cyberattack awareness training. It was determined that the cyber security awareness of the students was low before the training and at a high level after the training. In their study, Zhang and Li [24] based the increase in the number of cyber security attack victims on a low level of information security awareness. Allam et al. [25] stated that the design and implementation of cyber security awareness programmes have become important. Bada et al. [17] showed cyber security awareness programmes as one of the effective tools in raising cyber security awareness and improving cyber security practices.

It is seen that there is a significant difference between the awareness of the university students participating in the research according to the gender variable before the online cyber security and cyberattack awareness training. It has been determined that the cyber security awareness of male students is higher than that of male students. After the online cyber security awareness training, it was determined that there was no significant difference between the cyber security awareness of female and male students. Makhabbat and Gülseçen [26] evaluated students' cyber security awareness in their study and found that male students had more cyber security awareness than female students. This study reveals similar findings with the awareness levels of the students before the online cyber security and cyberattack awareness training of the research. Harrington et al. [27], on the other hand, found that gender did not have a significant effect on cyber security attitudes and behaviours. This finding supports the results that emerged after the online cyber security and cyber awareness training in the research. Laato et al. [28] also examined the effects of variables, such as age and gender, on cyber security knowledge. At the end of the research, it was revealed that male students were more knowledgeable than female students.

It has been determined that there is no significant difference according to the grade level of the university students participating in the research before and after the online cyber security and cyberattack awareness training. Karacı et al. [29] also revealed in their research, in parallel with the results of this research, that there is no significant difference between the cyber security behaviours of students studying in different classes. As cyber threats continue to increase exponentially, the educational need to raise information security conscious individuals should extend far beyond Information Technologies subjects in the curriculum of universities [30].

5 Conclusion

In the age of technology we live in, the Internet has become an indispensable part of our daily life. With the development of information and communication technologies, information security has become an important subject area, and user behaviour has become increasingly important. Concepts such as cyber security, cyber threat, cyber war and cyberattack have become problem areas of information communication technologies. Therefore, in this research, it is aimed to identify online cyber security problems and to provide awareness training for university students. As a result of the research, it is revealed that the low level of cyber security awareness of university students increased after online cyber security and cyberattack awareness training. Before the online cyber security and cyberattack awareness training of the university students participating in the research, a significant difference was determined in favour of male students according to the gender variable, but it was determined that the difference disappeared after the training. In addition, it was determined that there was no significant difference according to the grade level of the university students participating in the research before and after the online cyber security and cyberattack awareness training.

6 Recommendations

The results obtained from the research reveal that university students need cyber security and cyberattack awareness training. If students are educated, their awareness of cyber security will increase. Universities need to ensure that students are aware of general security threats and protection procedures. In addition, new types of attacks and new security measures that may occur due to technological developments in universities should be given to students regularly through awareness programmes.

7 References

[1] Saltanat, A., Kaldykul, S., Zaure, K., Saniya, K., Gulbanu, U., Karas, K., & Bagdat, B. (2022). Opinions of university students on technology literacy. *International Journal of Engineering Pedagogy*, *12*(2), 141–154. https://doi.org/10.3991/ijep.v12i2.29341

[2] Rahim, N.H.A., Hamid, S., Mat Kiah, M.L., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, *44*(4), 606–622. https://doi.org/10.1108/K-12-2014-0283

[3] Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

[4] Fichtner, L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review*, *7*(2), 1–19. https://doi.org/10.14763/2018.2.788

[5] Carr, J. (2012). *Inside cyber warfare: Mapping the cyber underworld*. " O'Reilly Media, Inc.". https://books.google.com.tr/books?hl=tr&lr=&id=5LIyXzpKhYsC&oi=fnd&pg=PR3&ots=0W45BHXkUf&sig=2qBVmWdt5HGU3T6kUXdMdTauzM0&redir_esc=y#v=onepage&q&f=false

[6] Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

[7] Furnell, S. (2008). End-user security culture: a lesson that will never be learnt? *Computer Fraud & Security*, *2008*(4), 6–9. https://doi.org/10.1016/S1361-3723(08)70064-2

[8] Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

[9] Goodrich, M. T., & Tamassia, R. (2011). *Introduction to computer security*. London, UK: Pearson. https://www.ece.ufl.edu/wp-content/uploads/syllabi/Spring2017/EEL4930_Cross_Layer_Sec_Spring_2017.pdf

[10] Önaçan, M. B. K., & Atan, H. (2016). Postgraduate education in cyber security: The example of naval academy. *Trakya University Journal of Engineering Sciences*, *17*(1), 13–21. https://dergipark.org.tr/en/pub/tujes/issue/21551/370293

[11] Aksakallı, İ. K. (2019). Security vulnerabilities and threats in cloud computing and security recommendations for these threats. *International Journal of Information Security Engineering*, *5*(1), 8–34. https://dergipark.org.tr/tr/pub/ubgmd/issue/43392/544054

[12] Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., ... & Chen, J. (2016, November). Cultural and psychological factors in cyber-security. In *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services* (pp. 318–324). https://doi.org/10.1145/3011141.3011165

[13] Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

[14] Agamba, J. J., & Keengwe, J. (2012). Pre-service teachers' perceptions of information assurance and cyber security. *International Journal of Information and Communication Technology Education (IJICTE)*, *8*(2), 94–101. https://doi.org/10.4018/jicte.2012040108

[15] Pusey, P., & Sadera, W. A. (2011). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education*, *28*(2), 82–85. https://doi.org/10.1080/21532974.2011.10784684

[16] Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. *Education and Information Technologies*, *26*(2), 1721–1736. https://doi.org/10.1007/s10639-020-10330-0

[17] Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*. https://arxiv.org/abs/1901.02672

[18] Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers & Security*, *70*, 663–674. https://doi.org/10.1016/j.cose.2017.08.001

[19] Koohang, A., Anderson, J., Nord, J. H., & Paliszkiewicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*. https://doi.org/10.1108/IMDS-07-2019-0412

[20] King, W. R., & He, J. (2005). Understanding the role and methods of meta-analysis in IS research. *Communications of the Association for Information Systems*, *16*(1), 32. https://doi.org/10.17705/1CAIS.01632

[21] Ding, L., Velicer, W. F., & Harlow, L. L. (1995). Effects of estimation methods, number of indicators per factor, and improper solutions on structural equation modeling fit indices. *Structural Equation Modeling: A Multidisciplinary Journal*, *2*(2), 119–143. https://doi.org/10.1080/10705519509540000

[22] Yesilyurt, S., & Capraz, C. (2018). A road map for the content validity used in scale development studies. *Journal on Erzincan University Education Faculty*, *20*(1), 251–564. https://dergipark.org.tr/en/download/article-file/459092

[23] Elci, E., & Uzunboylu, H. (2020). The development of a universal and cultural values scale for values education. *South African Journal of Education*, *40*(1), S1–S8. https://doi.org/10.15700/saje.v40ns1a1850

[24] Zhang, P., & Li, X. (2015). Determinants of information security awareness: An empirical investigation in higher education. https://aisel.aisnet.org/icis2015/proceedings/SecurityIS/15/

[25] Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, *42*, 56–65. https://www.sciencedirect.com/science/article/pii/S0167404814000169?casa_token=5NNv-j1oAJrAAAAAA:nD_ltpKVslgyEhjE9SI_kpDqmGRm2DWGr344XbRJNq4o4CG-7g2lQhgSqOKgcbsxn43MxVhPdhA; https://doi.org/10.1016/j.cose.2014.01.005

[26] Makhabbat, A., & Gülseçen, S. (2021). Cyber security awareness status of secondary school students. *International Student*, 37. https://www.udef.org.tr/media/publication/pdf/b88db-950ec4014d35b086e741ce897059.pdf#page=37

[27] Harrington, S., Anderson, C., & Agarwal, R. (2006). Practicing safe computing: Message framing, self-view, and home computer user security behavior intentions. *ICIS 2006 Proceedings*, 93. https://aisel.aisnet.org/icis2006/93/

[28] Laato, S., Farooq, A., Tenhunen, H., Pitkamaki, T., Hakkala, A., & Airola, A. (2020, July). AI in cybersecurity education-a systematic literature review of studies on cybersecurity moocs. In *2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)* (pp. 6–10). IEEE. https://ieeexplore.ieee.org/abstract/document/9156050?casa_token=8hdMUIEwPEsAAAAA:0cUKm4hhBCiBf_ff6oLj8xv0NUh6gUJEcb5Llto1i-F2u7uuyEj4TixHHbwU7akQ-z9fTxgBspg

[29] Karacı, A., Akyüz, H. İ., & Bilgici, G. (2017). Examining the cyber security behaviors of university students. *Kastamonu Journal of Education*, *25*(6), 2079–2094. https://doi.org/10.24106/kefdergi.351517

[30] Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy and Security*, *8*(4), 3–26. https://doi.org/10.1080/15536548.2012.10845664

[31] Folk, K., Marquart, M., Florio, M. B., & Garay, K. (2021). Developing technical expertise to support synchronous online classes: the Columbia University school of social work institute on technical skills for online event production. *International Journal of Advanced Corporate Learning*, *14*(1). https://doi.org/10.3991/ijac.v14i1.19873

[32] Nikishina, V. B., Sokolskaya, M. V., Musatova, O. A., Zapesotskaya, I. V., Danilova, A. V., & Balykina A. M. (2021). Dynamic characteristics of students' communicative behavior in social networks. *World Journal on Educational Technology: Current Issues*, *13*(4), 863–889. https://doi.org/10.18844/wjet.v13i4.6272

8 Appendix 1. Cyber Security Scale

	Cyber Security Scale	Never	Rarely	Sometimes	Often	Every Time
	Cyber security measures					
1	I check security links (https://) and certificates on web pages					
2	I keep anti-virus software on my computer					
3	I do not share my personal information (TC No. Date of Birth. Telephone No. etc.) on the Internet.					
4	I do not prefer easy and memorable passwords					
5	I do not respect e-mails (requests for card number, password etc.) from sites such as banks, online shopping sites.					
6	I do not download files from sites I do not trust					
7	I do not shop through advertisements on social networks					
8	I clean web history					
9	I do not share my personal information on social networking sites.					
10	I log out when I'm done with accounts such as social network, e-mail					
11	I make sure that my information is not left on the computers I use other than my personal computer.					
12	I do not respond to authentication messages (requests for username, password etc.)					
	Cyberattack awareness					
13	I realise that I have been hacked					
14	I file a criminal complaint when I'm cyberattacked					
15	I'm afraid of being hacked					
16	I believe that cybersecurity measures reduce the likelihood of being hacked.					
17	I raise awareness of people around me about cyberattacks					
18	I investigate my legal responsibilities in the face of cyberattacks					
19	I research the measures that can be taken against cyberattacks					
20	I take precautions regarding types of cyberattacks					
21	I heed the warnings about cyberattacks					

9 Authors

Botagoz Khamzina, is a Doctor of pedagogical sciences and associate professor at the Saken Seifullin Kazakh Agro Technical University (E-mail: b.khamzina@kazatu.kz).

Nabuova Roza, is a Candidate of pedagogical Sciences and associate Professor, at the Department of Preschool and Primary Education, at the Kazakh National Women's Teacher Training University (E-mail: nabuova.0@qyzpu.edu.kz).

Gulsara Zhussupbekova, is an associate professor and has PhD, at the Sh. Ualikhanov Kokshetau University (E-mail: g.g.zhussupbek@shokan.edu.kz).

Karlygash Shaizhanova, is a Candidate of Psychological Sciences, Associate Professor of the Department of Special Pedagogy Abai Kazakh National Pedagogical University (E-mail: K.Shaizhanova@abaiuniversity.edu.kz).

Aiganym Aten, is a specialist Department of Information Systems, at the Al-Farabi Kazakh National University (E-mail: aiganym.aten@kaznu.edu.kz).

Baikulova Aigerim, is a Meirkhanovna, doctor of Philosophy PhD, at the postdoctoral Abai Kazakh National Pedagogical University (E-mail: a.baikulova@abaiuniversity.edu.kz).

Article submitted 2022-05-03. Resubmitted 2022-08-09. Final acceptance 2022-08-09. Final version published as submitted by the authors.