Determining Cyber Security-Related Behaviors of Internet Users: Example of the Faculty of Sport Sciences Students

Feray Küçükbaş Duman

Istanbul University

Abstract

The most practical and fastest way to access information in today's world is via the internet. Thanks to the internet, the necessary information can be reached in a short time. Nevertheless, in addition to the benefits of the internet, it can also pose risks for users. For this reason, it is important to increase the level of awareness of individuals against threats that may occur in the cyber network. Sports organizations, like other sectors, process sensitive personal data and may face cyber attacks. It is important to determine the cyber security behaviors of the students of the faculty of sport sciences, who will be taking part in different careers in sports in the future, and so to contribute to the students' development in this regard. In this study, the cyber security-related behaviors of the faculty of sport sciences students were examined in terms of gender, age, frequency of internet usage, frequency of monthly purchases of products or services over the internet, and level of knowledge about cyber security. The "Personal Cyber Security Provision Scale" developed by Erol and associates (2015) was used as a data collection tool. For this reason, ANOVA and Independent Samples t-Test were used to investigate the significant differences between the scale scores and the variables. According to the findings of the study, students' behaviors related to cyber security differ according to gender, daily internet usage, monthly product or service purchase frequency, and knowledge level about cyber security. The age variable, on the other hand, does not affect cyber security behaviors. According to the results obtained from the Personal Cyber Security Ensuring Scale, the students of the faculty of sport sciences have high cyber security awareness. However, it is seen that they have lower scores from the factors of "Take Precautions" and "Privacy Protection" compared to other factors on the scale. Therefore, it is important for students to be informed about cyber security practices, what kind of precautions they should take in this regard, and how they can learn about improvements in this field to create cyber security awareness.

Keywords: Sport, the faculty of sport sciences students, cyber security, information management training, internet

Introduction

The world is being reshaped by technological developments, and this change affects the lives of individuals. Nowadays, people perform many activities virtually, and the use of information technologies and the internet is encountered in almost every aspect of our lives.

The rapid development of information and communication technologies, especially in recent years, and the fact that they have become easily accessible to individuals have played an important role in the widespread use of the internet (Yiğit and Seferoğlu, 2019). The most practical and fastest way to access information in today's world is via the internet. The necessary information can thus be accessed in a short time. The internet provides great convenience in diverse areas such as education, banking transactions, shopping, entertainment and many others.

The usage of the internet, which is such an integral part of our lives, is also increasing. While the internet provides many benefits to people's lives, it also brings some innovations and changes (Bayzan, 2013). According to the "Information and Communication Technology (ICT) Usage Survey on Households and Individuals" conducted by the Turkish Statistical Institute (TUIK), the daily internet usage of individuals aged 16-74 was 82.6% in 2021. This value was determined at 79% in the previous year.

Improvements, such as rapid widespread internet access, computers becoming a portable technology and the use of mobile phones as computers with the help of software, have now brought about a transformation in the communication habits of individuals, and new problems have emerged, even though the internet shortens distances between people (Karakaya and Yetgin, 2020). The internet can create addiction, thanks to the convenience and opportunities it provides and the sense of freedom it creates in people. In addition to the benefits of the internet, it can also pose risks for users.

On the one hand, people can obtain information easily through widespread internet access. On the other hand, the loss or alteration of the information they already hold may occur. In particular, sharing files over the internet or some risky attitudes of shoppers can affect both themselves and all employees in the business where they work, in terms of information security.

In addition to its positive benefits, the internet can negatively affect its users, especially children and young adults. Just as there are criminals in the real world, the internet also contains its own criminals. Information shared on the internet can be used for fraudulent purposes. The internet negatively affects social life due to issues such as "obscenity", "online fraud", and "virtual gambling". Another negative consequence caused by the internet is internet addiction, which occurs due to

unconscious and uncontrolled use of the internet. People are left in a dilemma between participating in the virtual and real worlds due to this addiction. Furthermore, various crimes bracketed as "cyber crimes", such as unauthorized access to computer systems and services, fraud and forgery, the use of unauthorized software, the use of computer systems by illegal organizations and threats from them are dangerous situations that have entered our lives through the internet (Bayzan, 2013).

The risks arising from internet usage can negatively affect the users both mentally and physically, as well as socially and financially. While negative factors such as "viruses", "unwanted messages (spam)", and "ad fraud" are directly technology-focused, threats such as cyberbullying, privacy violation, and terrorism are non-technology-related risks (Erol et al., 2015).

Sharing all kinds of information on different platforms in social media has made the information belonging to individuals and organizations prone to certain dangers in terms of confidentiality and integrity. For this reason, the importance of information security is increasing day by day. Thus, it is necessary for both individuals and institutions to take more precautions against these risks that may arise from the internet. The most important precaution may well be informing and raising awareness of individuals about cyber security (Karakaya and Yetgin, 2020).

The word cyber is used to express concepts covering computers and their networks. Today, cyber security has become an important concept in national security strategies. With the continuous development in technology, improvements in cyber security happen very quickly. For this reason, it is important to increase the level of awareness of individuals against threats that may occur in the cyber network (Aslay, 2017). The low awareness of internet users about cyber security, their carelessness, and negligence while surfing the internet, may allow for cyber crime and harm people. For these reasons, the importance of cyber security has emerged (Yiğit and Seferoğlu, 2019).

When the literature is examined, it is seen that there are many studies on cyber security and threats on the internet (Yavanoğlu et al., 2012; Lang et al., 2009; Nagy and Pecho, 2009; Kaşıkçı et al., 2014; Karaoğlan Yılmaz et al., 2014; Öğütçü, 2010; Furnell et al., 2005; Demirel et al., 2012; Yiğit and Seferoğlu, 2019; Avcı and Oruç, 2020). Like other sectors, the sports sector is also affected by technological developments. In the report named The Cyber Threat to Sports Organizations, it is stated that at least 70% of the sports clubs interviewed have encountered a cyber attack at least once. Sports clubs and organizations process a significant amount of sensitive personal data and conduct many financial transactions each year. Moreover, almost every sports organization has a web page and can keep customer and personnel records digitally (https://www.ncsc.gov.uk/files/Cyber-threat-to-sports-organisations.pdf). From this point of view, technology is used intensively in the sports sector, as it is in other sectors.

It is important to determine the cyber security behaviors of the sports science faculty students, who will be taking part in different careers in sport in the future, and in this way to contribute to the students' development in this regard. Therefore, this study aimed to determine the cyber security behaviors of the students of the Faculty of Sport Sciences. The research questions guiding the study are as follows:

What are the personal cyber security behavior levels of the students of the faculty of sport sciences?

Do these students' personal cyber security behavior levels differ significantly according to various demographic characteristics (gender, age, daily internet usage, frequency of monthly purchases of products or services over the internet, and level of knowledge about cyber security)?

Methodology

Research Model

The study was carried out using the cross-sectional survey method, one of the quantitative research methods. According to Büyüköztürk and associates (2020), in this method, data is collected to determine certain characteristics belonging to a group. This study aims to determine the cyber security-related behaviors of the students of the Faculty of Sport Sciences. Ethics committee approval for the study was obtained from Istanbul University Social and Human Sciences Research Ethics Committee dated 14.09.2021 and numbered E-35980450-663.05-466515.

Participants

Participants were determined according to the convenient sampling method, which is one of the non-random sampling methods. In convenience sampling, participants are selected from people who can be easily accessed and applicable units due to such limitations as time and workforce (Büyüköztürk et al., 2020). The study sample consisted of 221 people who are continuing their education in sport sciences faculties of various universities.

Data Collection

The **"**Personal Cyber Security Provision Scale" developed by Erol and associates (2015) was used as a data collection tool. This scale consists of 5 factors and 25 items. These factors are named as "Privacy Protection", "Avoiding Unsafe", "Take Precautions", "Protection Payment Information" and "Left No Trace". Items are evaluated on the 5-Point Likert scale (1-Never, 2-Rarely, 3-Sometimes, 4-Often, 5-Always). Items 5, 7, 12, 13, 17, 18, 19, 20, 24, 25 in the scale were included as reverse items. The Cronbach's alpha for the overall scale was calculated as 0.921.

Data Analysis

The data obtained with the Personal Cyber Security Ensuring Scale were analyzed using SPSS 28. It was determined that data are normally distributed (Kurtosis: -0.410,

Skewness: -0.379). For this reason, ANOVA and Independent Samples t-Test were used to investigate the significant differences between the scale scores and the variables of gender, age, daily internet usage, frequency of monthly purchases of products or services over the internet, and the level of knowledge about cyber security. The statistical significance level of the study was determined as $p<0.05$.

Findings

The findings of the study are given in the tables below.

Table 1: Demographic Characteristics of Participants

Variables	Group	Frequency	%
Gender	Female	119	53.8
	Male	102	46.2
Age	18-19	41	18.6
	20-21	86	38.9
	22-23	69	31.2
	24-25	25	11.3
Daily internet usage	Less than 1 hour	73	33.0
	1-2 hour/s	50	22.6
	3-4 hours	58	26.2
	5 hours or more	40	18.2
Frequency of monthly purchases of products or services over the internet	None	15	6.8
	1-2 time/s	74	33.5
	3-4 times	82	37.1
	5-6 times	47	21.3
	7 times or more	3	1.4
Level of knowledge about cyber security	No knowledge	5	2.3
	Low	49	22.2
	Moderate	67	30.3

	High	68	30.8
	Advanced	32	14.5

When the participants' scores on the Personal Cyber Security Ensuring Scale were analyzed in terms of the whole scale and the sub-dimensions, the findings in Table 2 were reached.

Table 2: The Scores of the Participants on the Personal Cyber Security Ensuring Scale

	Overall Scale	Privacy Protection	Avoiding Unsafe	Take Precautions	Protection Payment Information	Left No Trace
Mean	4.28	3.98	4.40	3.80	4.42	4.38
Min.	3.33	3.40	3.25	3.00	2.50	3.25
Max.	5.00	5.00	5.00	5.00	5.00	5.00

According to these findings, the average score of the participants on the overall scale is 4.28, from the dimension of protecting personal privacy 3.98, from the dimension of avoiding untrustworthy sites 4.40, from the dimension of taking precautions 3.80, from the dimension of protecting payment information 4.42, and from the dimension of leaving no traces 4.38.

Table 3: Statistical Analysis Results Between Participants' Scale Scores and Gender

Gender	Number	Mean	Std. Deviation	t	p
Female	119	109.4286	8.99677	1.710	**0.044**
Male	102	107.1765	10.58058		

***p < 0.05**

The relationship between the scale scores of the participants and their gender was examined with the Independent Samples t-Test. The results are indicated in Table 3. Accordingly, it was determined that there was a significant difference ($p<0.05$) between the gender variable and the scale scores.

Table 4: Statistical Analysis Results Between Participants' Scale Scores and Ages

Age	Number	Mean	Std. Deviation	F	p
18-19	41	108.1707	10.68387	0.664	**0.575**
20-21	86	108.6512	9.99149		
22-23	69	107.4058	9.48423		
24-25	25	110.5600	8.60271		

The relationship between the scale scores and the ages of the participants was examined with the ANOVA, and the results are shown in Table 4. No significant difference was found between the ages and scale scores of the participants ($p > 0.05$).

Table 5: Statistical Analysis Results between Participants' Scale Scores and Daily Internet Usage

Frequency of Internet Usage	No.	Mean	Std. Deviation	F	p
Less than 1 hour	73	116.0137	5.14105	106.600	**0.001**
1-2 hour/s	50	113.6200	5.24070		
3-4 hours	58	101.0690	7.05085		
5 hours or more	40	98.5500	7.94516		

$p < 0.05$

The relationship between the scale scores of the participants and their daily internet usage was examined with the ANOVA. The results can be seen in Table 5. A significant difference was found between the participants' daily internet usage and scale scores ($p < 0.05$). Findings of the Post Hoc Scheffe test are shown in Table 6.

Table 6: The Post Hoc Scheffe Test Results between Scale Scores of Participants and Daily Internet Usage

Groups (I)	Groups (J)	Mean Difference (I-J)	Std. Deviation	Sig.
Less than 1 hour	1-2 hour/s	2.39370	1.15191	0.232
	3-4 hours	**14.94473***	**1.10375**	**<0.001**
	5 hours or more	**17.46370***	**1.23441**	**<0.001**
1-2 hour/s	Less than 1 hour	-2.39370	1.15191	0.232
	3-4 hours	**12.55103***	**1.21094**	**<0.001**
	5 hours or more	**15.07000***	**1.33112**	**<0.001**
3-4 hours	**Less than 1 hour**	**-14.94473***	**1.10375**	**<0.001**
	1-2 hour/s	**-12.55103***	**1.21094**	**<0.001**
	5 hours or more	2.57897	1.28967	0.285
5 hours or more	**Less than 1 hour**	**-17.46370***	**1.23441**	**<0.001**
	1-2 hour/s	**-15.07000***	**1.33112**	**<0.001**
	3-4 hours	-2.51897	1.28967	0.285

p < 0.05

According to Table 6, there is a significant difference between the scale scores of the users whose daily internet use is less than 1 hour and 1-2 hours, and the scale scores of those who use the internet for 3-4 hours and 5 hours or more.

Table 7: Statistical Analysis Results between Scale Scores of Participants and Frequency of Monthly Purchases of Products or Services Over The Internet

Frequency of Monthly Purchases of Products or Services Over The Internet	**No.**	**Mean**	**Std. Deviation**	**F**	**p**
None	15	117.4667	3.50238	27.983	**0.001**
1-2 time/s	74	114.2838	6.31050		
3-4 times	82	106.0488	9.98753		
5-6 times	47	101.0638	7.50769		
7 times or more	3	96.3333	9.23760		

p<0.05

The relationship between the scale scores of the participants and the frequency of monthly purchases of products or services over the internet was examined with the ANOVA test, and the results are given in Table 7. A significant difference was found between the monthly frequency of purchasing products or services and the scale scores of the participants (p< 0.05). Findings of the Post Hoc Scheffe test are shown in Table 8.

Table 8: The Post Hoc Scheffe Test Results between Scale Scores of Participants and Frequency of Monthly Purchases of Products or Services over the Internet

Groups (I)	Groups (J)	Mean Difference (I-J)	Std. Deviation	Sig.
None	1-2 time/s	3.18288	2.27331	0.743
	3-4 times	**11.41789***	**2.25454**	**<0.001**
	5-6 times	**16.40284***	**2.38082**	**<0.001**
	7 times or more	**21.13333***	**5.07756**	**0.002**
1-2 times	None	-3.18288	2.27331	0.743
	3-4 times	**8.23500***	**1.28725**	**<0.001**

	5-6 times	**13.21995***	**1.49745**	**<0.001**
	7 times or more	**17.95045***	**4.72818**	**0.007**
3-4 times	**None**	**-11.41789***	**2.25454**	**<0.001**
	1-2 time/s	**-8.23500***	**1.28725**	**<0.001**
	5-6 times	**4.98495***	**1.46880**	**0.024**
	7 times or more	9.71545	4.71918	0.377
5-6 times	**None**	**-16.40284***	**2.38082**	**<0.001**
	1-2 time/s	**-13.21995***	**1.49745**	**<0.001**
	3-4 times	**-4.98495***	**1.46880**	**0.024**
	7 times or more	4.73050	4.78080	0.913
7 times or more	**None**	**-21.13333***	**5.07756**	**0.002**
	1-2 time/s	**-17.95045***	**4.72818**	**0.007**
	3-4 times	-9.71545	4.71918	0.377
	5-6 times	-4.73050	4.78080	0.913

p<0.05

When Table 8 is examined, there is a significant difference between the scale scores of the participants who do not purchase products or services over the internet and those who purchase 1-2 times a month, and the scale scores of the participants who purchase products or services 3-4, 5-6, and 7 or more times a month. The scale scores of the participants who do not buy products or services over the internet and who make purchases 1-2 times a month are significantly higher than the scale scores of the other participants.

Table 9: Statistical Analysis Results between Scale Scores and Level of Knowledge about Cyber Security

Level of Knowledge about Cyber Security	No.	Mean	Std. Deviation	F	p
No knowledge	5	100.0000	7.96869	61.394	**0.001**
Low	49	99.4898	6.48435		
Moderate	67	104.1791	8.72114		
High	68	115.5147	4.94294		
Advanced	32	117.0000	5.57066		

p < 0.05

The relationship between the scale scores of the participants and level of knowledge about cyber security was examined with the ANOVA, and the results are given in Table 9. Accordingly, a significant difference was found between the level of knowledge about cyber security and their scale scores ($p < 0.05$). Findings of the Post Hoc Scheffe test are shown in Table 10.

Table 10: The Post Hoc Scheffe Test Results between Scale Scores of Participants and Level of Knowledge about Cyber Security

Groups (I)	Groups (J)	Mean Difference (I-J)	Std. Deviation	Sig.
No knowledge	Low	0.51020	3.17694	1.000
	Moderate	**-4.17910***	**3.13718**	**0.017**
	High	**-15.51471***	**3.13557**	**<0.001**
	Advanced	**-17.00000***	**3.25414**	**<0.001**

Low	No knowledge	-0.51020	3.17694	1.000
	Moderate	**-4.68931***	**1.27200**	**0.010**
	High	**-16.02491***	**1.26805**	**<0.001**
	Advanced	**-17.51020***	**1.53803**	**<0.001**
Moderate	**No knowledge**	**4.17910***	**3.13718**	**0.017**
	Low	**4.68931***	**1.27200**	**0.010**
	High	**-11.33560***	**1.16485**	**<0.001**
	Advanced	**-12.82090***	**1.45412**	**<0.001**
High	**No knowledge**	**15.51471***	**3.13557**	**<0.001**
	Low	**16.02491***	**1.26805**	**<0.001**
	Moderate	**11.33560***	**1.16485**	**<0.001**
	Advanced	-1.48529	1.45066	0.902
Advanced	**No knowledge**	**12.00000***	**3.25414**	**<0.001**
	Low	**17.51020***	**1.53803**	**<0.001**
	Moderate	**12.82090***	**1.45412**	**<0.001**
	High	**1.48529**	**1.45066**	**0.902**

p<0.05

There is a significant difference between the scale scores of the participants who state that they do not have knowledge about cyber security or have little knowledge, and the scale scores of those who state that they have moderate, high or advanced knowledge. The scale scores of the participants who have little or no knowledge about cyber security are significantly lower than those of the other participants. The scale scores of the participants who state that they have moderate knowledge about cyber

security are significantly lower than the scale scores of the participants who state that they have high or advanced knowledge about cyber security.

Discussion and Conclusion

Nowadays, the internet is a necessity that we benefit from in our daily lives in many areas such as accessing and sharing information, communication and shopping. In addition to the conveniences provided by the internet, people are faced with some cyber risks and threats over the internet.

In this study, the cyber security-related behaviors of the students of the faculty of sport sciences were examined in terms of gender, age, daily internet usage, frequency of monthly purchases of products or services over the internet, and how they define their level of knowledge about cyber security. According to the findings of the study, the students' behaviors related to cyber security differ according to gender, daily internet usage, monthly product or service purchase frequency, and knowledge level about cyber security. The age variable, on the other hand, does not affect cyber security behaviors.

According to the results obtained from the Personal Cyber Security Ensuring Scale, the total scores of the students of the faculty of sport sciences were found to be high (4.28 points out of 5). While the factor with the highest average was “Protection Payment Information” (mean score 4.42), the factor with the lowest average was “Take Precautions” (mean score 3.80). Therefore, it is possible to say that students exhibit behaviors related to cyber security in their daily lives. This finding is similar to some studies in the literature (Avcı and Oruç, 2020; Karacı, Akyüz and Bilgici, 2017; Yiğit and Seferoğlu, 2019). It is seen that the students consider especially important the categories “Protection Payment Information” and “Avoiding Unsafe”. On the other hand, students pay the least attention to “Take Precautions”. Thus, it is important to increase the participants' awareness about taking precautions.

Another result of this research is that students' cyber security behaviors differ depending on gender. Female students have more positive cyber security behavior than male students. In the literature, some studies found that cyber security behaviors do not differ in terms of gender (Karacı, Akyüz and Bilgici, 2017; Subramaniam, 2017; Yiğit and Seferoğlu, 2019; Yan et al., 2018), but in the studies conducted by Akgün and Topal (2015), Kınay (2012) and Topçu (2008), male students took more risks than female students in matters related to security. In addition, according to Tekerek and Tekerek (2013), female students were more aware of information security than male students. Likewise, in a study conducted by Mart (2012), women were aware of the

dangers they may face compared to men in terms of information security. The differences between the results of the studies may be due to the fact that the studies were conducted on different groups. In addition, it would be useful to conduct qualitative research about the main factors behind these differences.

According to the results of this study, students' cyber security behaviors do not differ depending on age. The obtained finding is similar to the study conducted by Gökmen and Akgün (2015).

The study also investigated the effect of students' daily internet use on cyber security behaviors. According to the findings, students' cyber security behaviors differ depending on time spent online. According to this, the scale scores of the users whose daily internet use is less than 1 hour or 1-2 hours are significantly higher than the scale scores of the participants who use the internet for 3-4 hours or 5 hours or more. Based on this result, it can be said that students with low daily internet usage time have higher cyber security awareness. In a similar study conducted by Yiğit and Seferoğlu (2019), no significant difference was found between students' cyber security behaviors and the time spent on the internet. In another study, the awareness of the group that uses the internet more than the average and ethical awareness are negatively correlated (Akgün and Topal, 2012). These results may be due to the fact that the studies were conducted on different groups. In addition, for what purpose the participants use the internet and which websites they spend time on are also issues that need to be emphasized.

In this article, the frequency of monthly purchases of products or services over the internet, and the cyber security behaviors of the participants differed. The scale scores of the participants who do not buy products or services over the internet and those who make purchases 1-2 times a month are significantly higher than the scale scores of the other participants. This result is consistent with the findings of the analysis regarding the duration of internet use, which is another variable of the study. In addition, considering that the students of the faculty of sport sciences participating in the study are weak in the factors of "Take Precautions" and "Privacy Protection", compared to the other factors on the scale, the importance of the cyber security behaviors of the participants in online shopping emerges.

According to the findings of the study, the scale scores of the participants who stated that they have knowledge about cyber security is high. This shows that the participants' level of cyber security knowledge affects their awareness and is reflected in their behaviors. In the literature, the importance of raising awareness on an individual basis is mentioned, as well as the precautions that can be taken in terms

of technology to ensure cyber security (Keser and Güldüren, 2015; Şahinaslan, Kandemir and Şahinaslan, 2009; Shaw, Chen, Harris and Huang, 2009). In addition, attention is drawn to the importance of the human factor in exposure to cyber attacks, and it is stated that human error is an important factor in the negative results of these attacks. (Anwar et al., 2017; Öğütçü, Testik and Chouseinoglou, 2016; Sasse, Brostoff and Weirich, 2001;Yan et al., 2018). For this reason, increasing the awareness of individuals about cyber security through training has an important role in reducing the effects of cyber risks.

According to the results of the study, it is possible to say that the students of the faculty of sport sciences have high cyber security awareness based on the scores they get from the scale. However, it is seen that they are weak in the dimensions of taking precautions and protecting personal privacy compared to other dimensions of the scale. In today's world, where rapid changes are experienced in technological developments, it is important to inform students about cyber security practices, what kind of precautions they should take in this regard and how they can follow the developments in this field to create cyber security awareness. For the students of the faculty of sport sciences, who will take part in different application areas of sports in the future, in order to have enough information about the risks they may encounter during their use of the internet and how they can manage these risks, training can be provided or courses related to cyber security can be placed in the curriculum.

Suggestions can be made for future studies in this area. It should be noted that this study is limited to 221 students and a data collection tool. It is possible to conduct more in-depth studies with larger samples. In addition, studies can be conducted to determine the needs and expectations of students regarding cyber security in the field of sports.

References

[1] Anwar, M., He W., Ash I., Yuan X., Li L. and Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, doi: 10.1016/j.chb.2016.12.040.
[2] Akgün, Ö. E. and Topal, M. (2015). Information security awareness of the senior teacher students: Sakarya University sample. Sakarya University Journal of Education, 5 (2), 98anw121.
[3] Aslay, F. (2017). Siber Attack Methods and Current Situation Analysis of Turkey's Ciber Safety. International Journal of Multidisciplinary Studies and Innovative Technologies, 1(1), 24-28.

[4] Avcı, Ü. and Oruç, O. (2020). Investigation of the students' personal cyber security behaviour and information security awareness. Inonu University Journal of the Faculty of Education, 21 (1), 284-303.
[5] Bayzan, Ş. (2013). İnternet Bağımlılığı: Sorunlar ve Çözümler (Editor: Melek Kalkan ve Canani Kaygusuz) içinde İnternetin Bilinçli ve Güvenli Kullanımı, 259-278, Anı Yayıncılık.
[6] Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö.E., Karadeniz, Ş. and Demirel, F. (2020). Eğitimde bilimsel araştırma yöntemleri, Pegem Akademi.
[7] Demirel, M., Yörük, M. and Özkan, O. (2012). Safe internet for children: a study on safe internet service and parental views. Mehmet Akif Ersoy University Journal of Social Sciences Institute,4 (7), 54-68.
[8] Erol, O., Şahin, Y. L. , Yılmaz, E. and Haseski, H. İ. (2015). Personal Cyber Security Provision Scale development study. International Journal of Human Sciences, 12 (2), 75-91.
[9] Furnell, S. M., Jusoh A. and Katsabas D. (2005). The challenges of understanding and using security: A survey of end-users. Computers and Security, 25 (5), 27 – 35.
[10] Gökmen, Ö. F. and Akgün, Ö. E. (2015). An Analysis of Computer Education and Instructional Technology Student Teachers' Knowledge of Information Security According to Several Variables. Çukurova University Faculty of Education Journal, 44 (1), 61-84.
[11] Karacı, A., Akyüz, H. İ. and Bilgici, G. (2017). Investigation of cyber security behaviors of university students. Kastamonu Education Journal, 25 (6), 2079-2094.
[12] Karakaya, A. and Yetgin, M.A. (2020). A survey on personal cyber security: the case of Karabuk University. Kahramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 10 (2), 157 – 172.
[13] Karaoğlan Yılmaz, G., Yılmaz, R. and Sezer, B. (2014). Secure information and communication technology usage behavior of university students and an overview to information security training. Bartın Üniversitesi Eğitim Fakültesi Dergisi, 3 (1), 176 - 199.
[14] Kaşıkçı, D.N., Çağıltay, K., Karakuş, T., Kurşun, E. and Ogan, C. (2014). Internet habits and safe internet use of children in Turkey and Europe. Eğitim ve Bilim, 39 (171), 230-243.
[15] Keser, H. and Güldüren, C. (2015). Development of information security awareness acale. Kastamonu Education Journal, 23(3), 1167-1184.
[16] Kınay, H. (2012). An analysis of the relation between cyberbullying sensibility and risk behaviour, conservative behaviour, exposure to offence and risk perception and in relation to various variables of lycee students [Unpublished master's thesis
[17] Lang M., Devitt J., Kelly S., Kinneen A., O'Malley J. and Prunty D. (2009). Social Networking and Personal Data Security: A Study of Attitudes and Public

Awareness in Ireland. IEEE, Conference Paper , Conference: International Conference on Management of e-Commerce and e-Government (ICMeCG).

[18] Nagy J. and Pecho P. (2009). Social Network Security", Conference Paper Conference: The Third International Conference on Emerging Security Information. Systems and Technologies, SECURWARE 2009, 18-23 June 2009, Athens/Glyfada, Greece.

[19] Mart, İ. (2012). Information security awareness in informatics culture [Unpublished master's thesis

[20] National Cyber Security Center (2020). https://www.ncsc.gov.uk/files/Cyber-threat-to-sports-organisations.pdf

[21] Öğütçü. G. (2010). E-dönüşüm dürecinde kişisel bilişim güvenliği davranışı ve farkındalığının analizi [Unpublished doctoral thesis

[22] Öğütçü, G., Testik, Ö. M. and Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. Computers and Security, 56, 83-93.

[23] Sasse, M. A., Brostoff, S. and Weirich, D. (2001). Transforming the 'weakest link'-a human/computer interaction approach to usable and effective security. BT Technology Journal, 19, 122-131.

[24] Shaw, R. S., Chen, C. C., Harris, A. L. and Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. Computers and Education, 52(1), 92-100.

[25] Subramaniam, S. R. (2017). Cyber security awareness among Malaysian pre-university students. E-Proceeding of the 6th Global Summit on Education, 1-14.

[26] Şahinaslan, E., Kandemir, R. and Şahinaslan, Ö. (2009). Bilgi Güvenliği Farkındalık Eğitim Örneği, Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri, 11-13 Şubat 2009 Harran University, Şanlıurfa.

[27] Tekerek, M. and Tekerek, A. (2013). A research on students' information security awareness. Turkish Journal of Education, 2 (3), 61-70.

[28] Topçu, Ç. (2008). The relationship of cyberbullying to empathy, gender, traditional bullying, internet use and adult monitoring [Unpublished master's thesis

[29] TÜİK (2021). Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2021-37437

[30] Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q. and Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?. Computers in Human Behavior, 84, 375-382.

[31] Yavanoğlu. U., Sağıroğlu. Ş. and Çolak.İ. (2012). Information Security Threats and Taking Privacy Precausions in Social Networks. Politeknik Dergisi, 15 (1). 15-27.

[32] Yiğit, M.F. and Seferoğlu, S.S. (2019). Investigating students' cyber security behaviors in relation to big five personality traits and other various variables. Mersin University Journal of the Faculty of Education, 15 (1): 186-215.