

## Examining Secondary School Students' Safe Computer and Internet Usage Awareness: An Example from Bartın Province

Ramazan YILMAZ<sup>\*a</sup>, F.Gizem KARAOĞLAN YILMAZ<sup>a</sup>, H.Tuğba ÖZTÜRK<sup>b</sup>, Tuğra KARADEMİR<sup>b</sup>

<sup>a</sup>Bartın University, Faculty of Education, Bartın/Turkey

<sup>b</sup>Ankara University, Faculty of Educational Sciences, Ankara/Turkey



### Article Info

DOI: 10.14527/pegegog.2017.004

#### Article history:

Received 25 January 2016  
Revised 17 June 2016  
Accepted 19 December 2016  
Online 06 February 2017

#### Keywords:

Children and teens,  
Information security awareness,  
Social engineering,  
Threats,  
Information security protections.

#### Article Type:

Research paper

### Abstract

Information and Communication Technologies (ICT) have been rapidly prevailed among the children and youths. Personal technologies facilitating the students to gain some learning experiences both in and out of the schools also include many threats. It is important for students to have high awareness of safe internet and computer use to overcome with these threats. In this research, it was aimed to reveal internet security and computer usage awareness profiles of students studying in the secondary school. The data were collected from 2029 students studying in the secondary schools in Bartın Province in Turkey by using a questionnaire developed by the researchers. The data obtained from the questionnaire were analyzed based on the pre-determined themes and the students' information security and computer usage awareness profiles were revealed. The findings indicate that the majority of the students are insufficient regarding information security and computer usage awareness and they could be under risk in online settings towards the threats. In the discussion section, some measures for the parents, schools and policy makers were mentioned to increase students' information security and computer usage awareness.

## Lise Öğrencilerinin Güvenli Bilgisayar ve İnternet Kullanım Farkındalıklarının İncelenmesi: Bartın İli Örneği

### Makale Bilgisi

DOI: 10.14527/pegegog.2017.004

#### Makale Geçmişi:

Geliş 25 Ocak 2016  
Düzeltilme 17 Haziran 2016  
Kabul 19 Aralık 2016  
Çevrimiçi 05 Şubat 2017

#### Anahtar Kelimeler:

Çocuk ve gençler,  
Bilgi güvenliği farkındalığı,  
Sosyal mühendislik,  
Tehditler,  
Bilgi güvenliği korunma yolları.

#### Makale Türü:

Özgün makale

### Öz

Bilgi ve iletişim teknolojilerinin (BİT) kullanımı çocuk ve gençler arasında hızla yaygınlaşmaktadır. Öğrencilere okul içinde ve dışında öğrenme deneyimleri ve fırsatları sunan kişisel teknolojiler aynı zamanda da birçok tehlikeyi bünyesinde barındırmaktadır. Bu tehlikelerle mücadelede ise kullanıcıların güvenli bilgisayar ve internet kullanım farkındalıklarının yüksek olması önemlidir. Bu çalışmada, lise öğrencilerinin güvenli bilgisayar ve internet kullanım farkındalık profillerinin ortaya konulması amaçlanmıştır. Araştırmanın verileri, Bartın il merkezindeki liselerde öğrenim gören 2029 öğrenciden, araştırmacılar tarafından geliştirilen bir anket aracılığıyla elde edilmiştir. Anketten elde edilen verilere göre öğrencilerin güvenli bilgisayar ve internet kullanım farkındalık profilleri daha önceden belirlenen temalar temel alınarak analiz edilmiştir. Araştırma sonuçları, öğrencilerin büyük bölümünün güvenli bilgisayar ve internet kullanım farkındalıklarının yeterli olmadığını ve birçok çevrimiçi risklere maruz kalabileceklerini göstermektedir. Araştırmanın tartışma bölümünde, öğrencilerin güvenli bilgisayar ve internet kullanım farkındalıklarını artırmak amacıyla aile, okul ve politika geliştiricilerinin alabileceği önlemlere yer verilmiştir.

## Introduction

Information and Communication Technologies (ICT) have been rapidly prevailed among the children and youths. In order to provide students with a variety of learning experiences and opportunities in and out of the schools, parents, educators and policy makers facilitated the students with PCs, mobile devices and internet access. Although these technologies could be regarded as an opportunity for the students to boost their cognitive and social development, these technologies might mean a threat and in secureness for them. Misuse of the technologies brings about a concern for the parents and educators. The children who use these technologies could be defenseless against the threats such as pornography, cyber bullying, misleading information, contents including the elements of violence and hatred, gambling and internet addiction, data loss and financial loss. It is important to ensure safe internet and computer use to protect the children and youths from the aforementioned threats and dangers (Yenilmez & Seferoğlu, 2013).

Researchers' remark that technical and legal obligations as well as implementations are considered as a solution (Ben-Asher & Gonzalez, 2015; Choo, 2011) but they stress that human factor is the most important factor in ensuring safe internet and computer usage (Arachchilage & Love, 2014; Shillair et al., 2015; Van Bruggen, 2014). Furthermore, it is remarked that in ensuring the information security of the users on the internet, it is important to raise awareness of the users rather than blockings, bans, obligations (Chou & Peng, 2011; Cole, 2014; Valcke, Schellens, Van Keer, & Gerarts, 2007; Yan, 2009). For instance, Vicks (2013) examines the use of internet filters in schools to ensure students' safe internet and computer use and finds out that extreme policies limiting user access might impede accessing educational resources. Vicks suggests that instead of implementing restrictive policies, it is important to foster a culture of appropriate use of the internet and raise information security awareness of the students. In a study conducted by Murray (2014), the students' behavior on cyber bullying and pornography as well as their safe use of internet in a catholic school were examined. It was found out that majority of the students go online every day; 96.00% of them use social media; their use of ICT is not safe and they often encounter with cyber bullying and pornography related problems. Murray (2014) points out a solution which concerns raising awareness of the students, parents and administrators on safe internet and computer usage. From this point of view, it could be concluded that in ensuring information security, some stakeholders including parents need to work collaboratively with the students.

In the research studies dealing with ensuring safe internet and computer usage through human factors and user awareness, in general, it was aimed to reveal out the users' safe internet and computer usage awareness and their behaviors on safe ICT use (Leach, 2003; Rhee, Kim, & Ryu, 2009; Van Bruggen, 2014), and also in the research it was examined that the impact of training about safe internet and computer usage on awareness of users (Chou & Peng, 2011; Harris, 2010). In information security studies, examples of variables could be given as revealing the profile of the students regarding their safe use of internet (Ngoqo & Flowerday, 2015), examining students' safe internet and computer usage awareness and issues on cyber bullying (Murray, 2014), information sharing behaviors in the social networks (Tamjidyamcholo et al., 2014) and students' opinions about use of filters in schools (Vicks, 2013). In these studies, participants of the studies are usually university students or adults. However, given that the age group who are mainly under threats about use of ICT is children and youths (Cole, 2014), and there are emerging research studies on these groups (Alhejaili, 2013; Al-Jerbie & Jali, 2014; Chen, 2014; Cole, 2014; Murray, 2014; Ngoqo & Flowerday, 2015; Tsim, 2006; Valcke et al., 2007; Vicks, 2013; Wishart, 2004; Yan, 2009). However, children's levels of information security awareness differ from country to country; therefore, there is a need to conduct a study demonstrating particular profiles of the students in a specific context. In line with this, according to Deisman (2008) it is helpful to conduct research studies on safe internet and computer usage awareness at a national/regional level since diversifying factors such as educational background of users, parents' awareness and internet access policies affect the safe internet and computer usage awareness of children and youths. Therefore, it is essential to conduct research studies dealing with awareness of children and youths at

the national/regional level and necessary legislations should be implemented and measures should be taken. According to the researchers, there is a need to conduct new studies on safe internet and computer usage awareness of children and youths dealing with specific variables such as age groups, the school's information security policies and status of using technologies, parental and environmental conditions (Berrier, 2007; Harshman, 2014; Vicks, 2013).

When national literature is examined, it could be seen that a variety of studies on safe internet and computer usage were conducted focusing on university students, adults and ICT coordinators in Turkey (Çakır, Hava, Gülen, & Özüdoğru, 2015; Demirel, Yörük, & Özkan, 2013; Gökmen, & Akgün, 2015; Karaoğlan Yılmaz, Yılmaz, & Sezer, 2014; Küçükali & Bülbül, 2015). However, the number of studies which sought to examine children and youths is limited (Kaşıkçı et al., 2014; Tekerek & Tekerek, 2013). In a comprehensive project regarding the aforementioned issues in Turkey titled as "EU Kids Online", the children's activities on the internet, the risks they encounter and parents' awareness of their children's experience on the internet in Europe and Turkey were reported (Kaşıkçı et al., 2014). Participants of the study consist of 1018 parents and students whose ages range from 9 to 16. The results show that 40.00% of the participants own either a PC or a laptop; 39.00% of them share a computer with other family members and use the internet for 74 minutes in a day on average. Furthermore, it was found out that 60.00% of the students connect to the internet in schools; 51.00% of the students use cyber cafes to access to the internet and parents cannot monitor their children as they connect to the internet outside of the house; the majority of the students do not have enough skills to use the internet and they are under online risks. In a study conducted by Tekerek and Tekerek (2013), it was aimed to examine primary and secondary school students' information security awareness in Maraş Province in Turkey. It was found out that the students' information security awareness of the ethical issues is at adequate level whereas their awareness level about the rules and knowledge-required issues is low. The related literature shows that the research whose participants are comprised of children and teenagers are scarce and there is a need to reveal out more information and findings regarding this issue.

### **Aspects of Information Security**

In terms of concerns of the information security in the literature, it is aimed to ensure that availability, confidentiality and integrity of information are not compromised (Güldüren & Keser, 2015; Kritzinger & Smith, 2008). Taking a closer look at these studies, according to research findings, it is stated that many threats and user error intended for different dimensions such as access and password security, social network security, threats and defense methods, software installation and updating, e-mail security, internet and network security, social engineering (manipulations of the people through some tricks such as hiding or disguising real life identities, and awareness of users cause the information security gaps (Alhejaili, 2013; Arachchilage & Love, 2014; Berrier, 2007; Chen, 2014; Van Bruggen, 2014; Valcke et al., 2007). For instance, the major factors such as common use of computers, choosing weak passwords, using the same password for different online environments, saving passwords in easily accessible areas, such as on a notepad, and sharing password with other people might result in information robbery. Furthermore, installing software obtained from online environments without testing its reliability, not updating security software, and sharing an unsafe file on the internet and networks can cause users to face with information security threats. In addition to this, lack of knowledge about harmful software and social engineering are the main factors which cause problems in safe computer and internet use. These problems expose the users with not only the information robbery but also several materials and psychological issues. In addition, it is seen that the research with regard to determining awareness of users about safe internet and computer use have focused only on specific variables. Moreover, when it is considered that information security requires taking a holistic approach, it is very important to conduct extensive research on determining user awareness as there is a gap in the literature.

Furthermore, In Turkey, although various studies about safe internet and computer use awareness have been conducted, there is still a need to do more academic research focusing on youth and children. According to the findings of a research conducted by Kasıkcı et al. (2014), it has been found out that the majority of the students studying in Turkey access the internet at cyber cafes and schools, also some part of students stated that they use the same computer with their parents at home. Accordingly, the students partly can be under control with internet filtering software at schools, cyber cafes, and parental monitoring at home. Even though cheaper technologies in recent years have rapidly been used by the teenagers, the measures taken about threats of these technologies on teens are still limited. Moreover, although safe internet and computer use is taught in ICT courses and internet filtering software is used at schools in addition to parental monitoring out-of-class, parental monitoring is limited with the shared computers. Providing students access to the internet with their personal technological devices such as mobile phones, it is true that control of parents will be decreasing. Therefore, it is needed to determine teenagers' habits and awareness of safe internet and computer use and take various measures according to this awareness stage.

To sum up, the research have shown that ensuring information security is possible with raising awareness of the individuals and using protection tools in the right time and right place (Güldüren & Keser, 2015). In this process, awareness is the first step to take and has roots in real life for the students for them to take measures. It has also been reported that cybercrimes in Turkey are increasing due to the threats on information security (Gökmen & Akgün, 2016), it is important to reveal out information security awareness of the youths before it is too late. However, to our best of knowledge, there is limited research examining information security awareness with comprehensive instruments at regional levels. Furthermore, information security awareness of the students change rapidly over time, there is a need for updated studies. Therefore, by taking into account of the research outcomes and recommendations about safe computer and internet use, the purpose of this research is to reveal the profile of the students studying at secondary schools. In line with this purpose, the following research questions were sought for:

1. What is the situation about the student awareness of access and password security?
2. What is the situation about the student awareness of social network security?
3. What is the situation about the student awareness of threats, defense methods, and software installation and upgrading?
4. What is the situation about student awareness of e-mail security?
5. What is the situation about student awareness of internet and network security?
6. What is the situation about student awareness of user awareness and social engineering?

## Method

### Research Design

In this study, a descriptive model used in quantitative studies was adopted. In a descriptive model, it is usually aimed to examine an existing situation based on the themes. In line with the aims of the present study, a descriptive model was adopted in order to find out the profile of the students studying in secondary school in relation to their safe internet and computer use awareness under a variety of themes.

### Participants

The study group in this research consists of students studying in secondary school in the center of Bartın Province in Turkey. According to the data obtained in 2014-2015 academic year, there are 17 secondary schools and 8299 students receive education in secondary schools in Bartın Province in

Turkey. While choosing the sample that represents the population, stratified sampling method has been utilized. Stratified sampling is a probability sampling procedure in which the target population is first separated into mutually exclusive, homogeneous segments (strata), and then a simple random sample is selected from each segment (stratum). The samples selected from the various strata are then combined into a single sample (Daniel, 2012). In this research, for the purpose of calculating sample, population was divided into 3 layers as follows: a) School type (Anatolian Schools, Science High School, School of Fine Arts and Imam Hatip Vocational School), b) Grade level (9., 10.,11., and 12. Grades), c) Major. As a result, 3029 students were chosen by using stratified sampling.

The data were collected on a volunteer basis through a questionnaire developed by the researchers of the present study. In the returned questionnaires, if the students did not fulfill more than 5.00% of the questionnaire, these students' questionnaires were not included in the study. Overall, the data obtained from 2029 students were analyzed. The demographic information of the students in the study is indicated as follows: 1087 female and 942 male students participated in the study. 94.00% (f=1907) of the participants have personal computer and mobile devices such as smartphone, tablet and also 76% of students (f=1542) have the internet connectivity on their personnel computer or mobile devices. 23.80% (f=482) of participants reported that they have received training on safe computer and internet use whereas 76.20% (f=1547) of them stated that they have not received any training on the issue yet. Regarding the length of time spent on the daily use of computers/mobile devices, 10.50% (f=396) of the students do not use computer/mobile devices every day; 22.10% (f=499) of them use approximately half an hour; 37.90% (f=768) of them use between 1 and 2 hours; 14.20% (f=289) of them use between 3 and 4 hours; 6.30% (f=127) of them use longer than 4 hours. Considering the length of time for daily internet use, 5.20% (f=105) of the students do not connect to the internet every day; 18.20% (f=369) of them connect almost for half an hour; 40.20% (f=816) of them connect between 1 and 2 hours; 21.30% (f=432) of them connect between 3 and 4 hours; 15.10% (f=307) connect longer than 4 hours. When these findings are compared to Turkey's average according to the May-June 2014 data obtained in the EU Kids Online report (Kaşıkçı et al., 2014), it could be assumed that length of time spent daily on the internet use of students in the sampling has increased.

## **Instrument**

The data were gathered through a questionnaire which was formed by the researchers of the present study. The reason why a questionnaire was formed in this research is that a comprehensive instrument consisting of sub-dimensions of safe computer and internet use awareness, access and password security, social network security, threats, protection methods, software installation and updating, e-mail security, internet and network security, user awareness and social engineering were intended to measure.

While the questionnaire was being developed, at the first stage the problem statement was identified and the literature was reviewed (Alhejaili, 2013; Al-Jerbie & Jali, 2014; Arachchilage & Love, 2014; Berrier, 2007; Chen, 2014; Chou & Peng, 2011; Kaşıkçı et al., 2014; Lawler & Molluzzo, 2010; Murray, 2014; Ngoqo & Flowerday, 2015; Shillair et al., 2015; Tsim, 2006; TÜBİTAK BİLGEM, 2011; Valcke et al., 2007; Van Bruggen, 2014), and subsequently themes were emerged. The subthemes determined at the end of the literature review are demographic information, computer and access security, social network security, threats and protection methods, e-mail security, password security, software installation and update security, internet and network security, web security, user awareness and social engineering. After identifying the themes, in the light of the literature, 60 items were created and an item pool was formed. Among the items in the item pool, 53 items were chosen and pre-implementation form was created in a form of a likert type questionnaire. In order to ensure validity of the questionnaire, a table of specifications was formed and opinions of five educational technologies experts who studied about information security and ethics and a Turkish Language expert were asked to finalize the form. While the linguist examined the items of questionnaire in terms of language and

expression and comprehensibility, educational technologists reviewed the items of questionnaire with regard to validity of scope, standard, structured, and aspect drawing on the feedback of the experts, necessary revisions were made on the questionnaire. Subsequently, it was administered to 60 students who enroll in a high school except for the pilot schools in the study and have computer and internet knowledge. Then, the questionnaire was reviewed and revised based on the criteria such as linguistic validity, clarity and appropriateness of the items. Final version of the questionnaire consists of nine sections and 47 questions in a likert style. After missing data among the data obtained via the questionnaire were removed, the data were subjected to frequency analysis and the results of the data analysis were reported based on the percentages and frequencies. Calculations were made for nine themes separately. In general, themes were reviewed and interpreted by grouping the students' responses of "never", and "rarely" together and "often" and "always" together.

### Data Analysis

KMO (Kaiser-Meyer-Olkin) index was used in order to measure sampling adequacy, Bartlett Test was used to measure consistency between items and Cronbach Alfa was used to measure reliability. Factor loadings of forty-seven items varied between .26 and .62. KMO was found as .86. As KMO value approaches to 1, result of factor analysis becomes more significant. The KMO value between the .50 and .70 is regarded as medium level, between .71 and .80 is regarded as good level, between .81 and .90 is regarded as very good level and greater than .91 is regarded as great level (Field, 2005). Drawing on this, it could be said that the sample in this research is enough to proceed to analyze the data. Also, it was found that Bartlett test analysis is significant (Chi-square=16025.23,  $p < .01$ ). After reliability of questionnaire was examined, Cronbach alfa reliability coefficient was found as .86. The findings show that the questionnaire is reliable. Percentage and frequencies were calculated for all items based on the themes from the data obtained from students studying in secondary school.

### Results

The findings of the research are presented below based on the sub-themes in the questionnaire. Table 1 shows the findings regarding the awareness of the students of the password and access security as a first theme.

When Table 1 is examined, it could be seen that almost half of the students' awareness is high while other half of the students are under risk in terms of their awareness of this theme. Table 1 shows that 49.40% of the students log in their computers/electronics devices with a passport while 46.40% students log in their computers with a password when they temporary log off and re-log in. Also it is indicated that majority of students use common computers and other mobile devices and share their computer and other mobile devices with others.

In addition, Table 1 shows that 15.10% of the students do not record their passwords; 43.90% of the students can save their account when it is hacked; 13.80% of the students never use the same passwords in his/her different accounts; 55.80% of the students' passwords include at least 8 characters; 45.00% of the students include special characters in their passwords; 23.00% of the students include sequential characters in the passwords while 21.70% of the students do not include personal information in their passwords. In general, drawing on the data in Table 5, it could be said that less than half of the students' knowledge and awareness of e-mail security are high. In other words, majority of the students are under risk in terms of protecting their email accounts. Table 2 below shows students' awareness of social network security under theme two.

**Table 1.**  
*Students' Awareness of Password and Access Security.*

<b>Awareness</b>		<b>Never</b>	<b>Rarely</b>	<b>Sometimes</b>	<b>Often</b>	<b>Always</b>
When I turn on my computer or other electronic devices, I log in with a password.	f	216	312	497	500	504
	%	10.60	15.40	24.50	24.60	24.80
When I temporarily quit working on my computer or other electronic devices, I log off and then log in with a password.	f	217	400	470	467	475
	%	10.70	19.70	23.20	23.00	23.40
I share my personnel computer and cell phone with people such as members of my family, friends and relatives and use them together.	f	152	357	500	462	558
	%	7.50	17.60	24.60	22.80	27.50
I save my passwords which I use on the internet, email and Facebook in a notebook in order not to forget them.	f	306	429	512	359	423
	%	15.10	21.10	25.20	17.70	20.80
I can take my account back when it is hacked.	f	231	262	536	524	476
	%	11.40	12.90	26.40	25.80	23.50
I use the same password on the environments requiring me to log in (computer, email, mobile phone, Facebook, etc).	f	281	387	481	469	411
	%	13.80	19.10	23.70	23.10	20.30
I use passwords consisting of at least 8 characters.	f	187	279	431	475	657
	%	9.20	13.80	21.20	23.40	32.40
I use capital and small letters as well as numbers and special characters such as "? , @ , ! , # , % , + , - , * , %" in my passwords.	f	319	364	433	465	448
	%	15.70	17.90	31.30	22.90	22.10
My passwords include sequential characters such as 1,2,3,4 or order of the letters in the alphabet such as a,b,c,d.	f	467	292	483	406	381
	%	23.00	14.40	23.80	20.00	18.80
My passwords include personal information such as a name, surname, date of birth, date of place and national ID number.	f	441	347	395	508	338
	%	21.70	17.10	19.50	25.00	16.70

**Table 2.**  
*Students' Awareness of Social Network Security.*

<b>Awareness</b>		<b>Never</b>	<b>Rarely</b>	<b>Sometimes</b>	<b>Often</b>	<b>Always</b>
I share my personal information (Date of birth, Date of place, mobile number, home address and my school information etc) on social networks (Facebook, Twitter etc)	f	340	518	434	408	329
	%	16.80	25.50	21.40	20.10	16.20
I block the messages/ posts/ notifications/ friend requests from the people whom I do not know on social networks.	f	100	323	428	563	615
	%	4.90	15.90	21.10	27.70	30.30
I can change my security settings regarding who could see my postings.	f	169	261	379	421	799
	%	8.30	12.90	18.70	20.70	39.40
I can make a complain about posting/message which disturbs me on social networks.	f	204	271	379	453	722
	%	10.10	13.40	18.70	22.30	35.60
I can change the privacy settings of the pages/groups which I formed on social networks.	f	140	303	411	470	705
	%	6.90	14.90	20.30	23.20	34.70
I can change my social network setting the way that it appeals me when logging in a social network from the different devices or browsers.	f	164	306	510	419	630
	%	8.10	15.10	25.10	20.70	31.00

91.80% (f=1863) of the students in the study reported that they use a social network while 8.20% (f=166) do not use a social network. Among the students who use a social network, 1799 students stated that their parents are aware of their social network account; 34 students stated that their parents are not aware of their account and 30 students stated that they are not entirely sure whether their parents know or not. Table 2 reveals that 42.30% of the students do not share their personal information on the social network; 58.00% of the students can block the messages/posts/notifications/friend requests from the people whom they do not know; 60.10% of the students could secure their postings, 57.90% of the students can make a complain about disturbing messages/posts; 57.90% of the students can change privacy settings of the groups/pages. In general, drawing on Table 2, it could be seen that more than half of the students have considerable knowledge and high awareness of social network security. A possible reason could be that the students use social networks very often and they might have gained experience. Table 3 given below shows the students' awareness of the threats, protection methods and software installation and upgrading which was investigated under the third theme.

**Table 3.**  
*Students' Awareness of the Threats, Protection Methods and Software Installation and Upgrading about Information Security.*

Awareness		Never	Rarely	Sometimes	Often	Always
I am aware of the malicious computer programs (virus, spyware, Trojan, etc) and how they can harm my computer or my electronic device (tablet, mobile phone etc.).	f	121	310	451	494	653
	%	6.00	15.30	22.20	24.30	32.20
I am aware of the protecting software (antivirus, spyware protections etc.) and benefits of the protecting software.	f	126	293	434	468	708
	%	6.20	14.40	21.40	23.10	34.90
I install protecting software on my computer.	f	147	350	403	460	669
	%	7.20	17.20	19.90	22.70	33.00
I can understand if my computer and other devices are infected by malicious software.	f	148	305	448	582	546
	%	7.30	15.00	22.10	28.70	26.90
I download and install software without a license (pirate) on my computer or other electronic devices.	f	349	354	451	438	437
	%	17.20	17.40	22.20	21.60	21.50
I investigate whether the website on which I download program etc. is safe.	f	250	332	438	480	529
	%	12.30	16.40	21.60	23.70	26.10

Table 3 demonstrates that 56.50% of the students are aware of the malicious computer software; 58.00% of the students are aware of the benefits of the protecting software; 55.70% of the students can actively use protecting software and 55.60% of the students can understand whether their computers are infected by malicious software or not. In general, it could be said that almost half of the students have considerable knowledge and high awareness of how to ensure their information security towards the threats. Other half of the students are under risk in terms of their proficiency and awareness of this theme.

In addition, when Table 3 is analyzed, it could be seen that 34.60% of the students do not install pirate software on their computers/other electronic devices; 49.80% of the students investigate whether the website on which they download program etc. is safe. In addition to the items in Table 3, the students were also asked how often they update their antivirus software. 17.20% (f=348) of the students reported that they do not update; 3.60% (f=73) update every day; 3.20% (f=64) update weekly; 3.10% (f=62) update monthly; 3.30% (f=67) update biannually; 4.10% (f=83) of the students update annually or longer and 65.60% (f=1332) of the students update automatically. The students were also asked how often they backup their digital files. It was found out that 45.90% (f=931) do not backup, 5.20% (f=105) backup every day; 7.30% (f=148) of the students backup weekly; 14.20% (f=288) of the



students backup monthly; 12.80% (f=260) of the students backup biannually; 14.60% (f=297) of the students backup annually or longer. In general, when the themes of software installation, updating and backing up are considered based on the data, it could be seen that less than half of the students' awareness of information security is high. In other words, given their awareness status and proficiency in aforementioned themes, majority of the students are under risk. The students' awareness of e-mail security was categorized under theme 4 as could be seen in Table 4.

**Table 4.**  
*Students' Awareness of E-mail Security.*

Awareness		Never	Rarely	Sometimes	Often	Always
I hide the receivers' email addresses when I send an email to more than one person.	f	322	338	411	440	518
	%	15.90	16.70	20.30	21.70	25.50
I can mark emails, which I do not want to receive, as spam emails.	f	198	227	464	510	630
	%	9.80	11.20	22.90	25.10	31.00
I check the source of an attachment sent by an email before I download and open it.	f	272	358	533	382	484
	%	13.40	17.60	26.30	18.80	23.90
I do not reply an email which I do not know and cannot recognize its sender.	f	204	287	422	432	684
	%	10.10	14.10	20.80	21.30	33.70
I do not click on the links in an email sent by whom I do not know and cannot recognize.	f	158	336	420	496	619
	%	7.80	16.60	20.70	24.40	30.50

Table 4 signifies that 47.20% of the students hide the receivers' email addresses when sent to multiple receivers, 56.10% of the students can mark unwanted emails as spam, 42.70% of the students scan the email attachments for viruses, 55.00% of the students do not reply the emails which they do not know the sender, 54.90% of the students do not click on the links in the emails which they do not know the senders. In general, Table 4 shows that almost half of the students' awareness of email security is high. Other half of the students are under risk in terms of their proficiency and awareness of this theme. The students' awareness of internet and network security was categorized under theme 5 as could be seen in Table 5.

**Table 5.**  
*Students' Awareness of the Internet and Network Security.*


Awareness		Never	Rarely	Sometimes	Often	Always
I change my modem password regularly.	f	254	437	492	441	405
	%	12.50	21.50	24.20	21.70	20.00
I share my modem password with my friends/neighbors or I use their passwords if they share with me.	f	287	400	454	548	340
	%	14.10	19.70	22.40	27.00	16.80
I connect to the wireless networks, which I know, from my computer or other electronic devices.	f	156	319	484	529	541
	%	7.70	15.70	23.90	26.10	26.70
I take security measures necessary for safe online shopping.	f	237	269	492	509	522
	%	11.70	13.30	24.20	25.10	25.70
I click on "yes" or "OK" options without reading the messages when I surf on the internet.	f	254	380	492	467	436
	%	12.50	18.70	24.20	23.00	21.50
I prefer to use web sites which have  icons and https.	f	225	289	507	429	579
	%	11.10	14.20	25.00	21.10	28.50
I use video, music, film, etc. files and software which I downloaded or received from my friend by scanning them with antivirus software.	f	219	428	434	518	430
	%	10.80	21.10	21.40	25.50	21.20
I scan the files shared through software such as LimeWire, Ares for viruses before opening them.	f	240	409	477	464	439
	%	11.80	20.20	23.50	22.90	21.60

Table 5 points out that 41.70% of the students change their modem password regularly; 33.80% of the students do not share their modem password with others; 52.80% of the students only connect to the wireless network which they recognize. According to the data given at Table 8, it could be seen that 50.80% of the students take measures on doing online shopping; 31.20% of the students do not click on the irrelevant messages during surfing; 28.50% of the students prefer to use websites with https characteristics; 49.60% of the students scan the movie/music/video files which they downloaded from the internet; 44.50% of the students scan the files which they obtained from file exchange software. In general, based on the data on Table 5, it could be said that less than half of the students' awareness of internet and network security remains high. In other words, given their awareness status and proficiency in aforementioned themes, majority of the students are under risk. The students' awareness of user awareness and social engineering was categorized under theme 6 as could be seen in Table 6.

**Table 6.**  
*Students' Awareness of User Awareness and Social Engineering.*

Awareness		Never	Rarely	Sometimes	Often	Always
I am aware of what the meaning of safe computer and internet use is.	f	149	311	524	479	566
	%	7.30	15.30	25.80	23.60	27.90
I am aware of the responsibilities in ensuring safe computer and internet use as an individual.	f	155	233	474	596	571
	%	7.60	11.50	23.40	29.40	28.10
I am aware of whom to issue my complaints and where to apply when I face with a safe computer and internet use related situation.	f	130	329	483	545	542
	%	6.40	16.20	23.80	26.90	26.70
I am aware of what exactly the cybercrimes and their scope are.	f	216	352	473	473	515
	%	10.60	17.30	23.30	23.30	25.40
I am aware that I should not share the folder including copyrights such as mp3, software on the internet.	f	138	326	406	549	610
	%	6.80	16.10	20.00	27.10	30.10
I am aware that I should not download the folder including copyrights such as mp3, software on the internet.	f	152	337	515	413	612
	%	7.50	16.60	25.40	20.40	30.20
I follow the policies/implications of the Ministry of Education and the government in ensuring safe computer and internet use.	f	279	376	468	431	475
	%	13.80	18.50	23.10	21.20	23.40
I tell my family about disturbing situations regarding safe computer and internet use which I encounter on the internet.	f	200	419	511	426	473
	%	9.90	20.70	25.20	21.00	23.30
I tell my teacher about disturbing situations regarding safe computer and internet use which I encounter on the internet.	f	326	407	451	446	399
	%	16.10	20.10	22.20	22.00	19.70
I tell my friend about disturbing situations regarding safe computer and internet use which I encounter on the internet.	f	179	384	478	442	546
	%	8.80	18.90	23.60	21.80	26.90
My parents monitor my electronic devices such as my computer and my mobile phone.	f	289	382	515	405	438
	%	14.20	18.80	25.40	20.00	21.60
My parents inform me about whether I could ensure safe computer and internet use when using my computer and other electronic devices.	f	252	408	415	514	440
	%	12.40	20.10	20.50	25.30	21.70

When Table 6 is examined, it could be seen that 57.50% of the students are aware of the responsibilities in ensuring information security as an individual; 53.60% of the students know whom to issue his/her complains and where to apply when they encounter with safe internet and computer use related problems; 48.70% of the students know what cyber-crimes are and scope of cyber-crimes;

44.60% of the students follow the policies and implementations in relation to safe internet and computer use. Furthermore, when students encounter with the safe internet and computer use related problems, 44.30% of the students share with their parents; 41.70% of the students share with their teachers; 48.70% of the students share with their friends. In addition, 41.60% of the students' parents monitor their use of electronic devices; 47.00% of the students are acknowledged by their parents. In general, drawing on the data in Table 6, it could be said that majority of the students' awareness of user awareness is low.

### **Discussion, Conclusion and Implementation**

In the light of the findings based on the themes, the data were almost equally spread between each choice of “never”, “rarely”, “sometimes”, “often”, and “always” for access and password security, social network security, threats and protection methods, software installation and upgrading e-mail security, internet and network security, user awareness and social engineering themes. This suggests that the number of the students with high safe computer and internet use awareness is low, in general. In line with the findings of our study, Kasikci et al. (2014) reported that although 83.40% of the children in Turkey said that “I know a lot about internet”, in reality their internet literacy awareness was very low. However, compared to Kasikci et al. (2014)'s study, it could be claimed that the students' average internet use got higher in the schools nowadays. In addition, Kasikci et al. (2014) found that even though 40.20% of the students in Turkey use their own computers to access to the internet, parents still claim that they experience difficulties in monitoring their children's internet use. On the other hand, according to European Online Children study results, 70.00% of the parents speak to their children about their online activities and 58.00% of the parents monitor their children's internet use (Kasikci et al., 2014). When it is considered that 95.00% of students in the sampling population have their personal computer and mobile devices it could be concluded that parents' supervision would be even more difficult. The most significant reason for this situation is that students who have their own mobile computers or mobile devices can connect to the internet from any part of their home or outside of their home. A further important dimension of risks arising from the aforementioned issue is that according to this study's findings, majority of the students did not share the occasions they experienced about safe computer and internet use with their parents. In this context, it can be said that the students' parents' awareness levels regarding computer and internet use are low.

Parents are naturally concerned about how their children use computer and the internet and act in the virtual worlds. Information is needed to ensure that parents are able to decide, with their child, what is appropriate and safe for their use (ENISA, 2011). Nevertheless, the families who are not aware of information security enough will fail to help both children and themselves. Many institutions from policymakers to schools have failed to solve these problems. Policymakers should ensure environments and new policies which will decrease the level of parents' information security awareness. To provide new environments, policy makers and schools can perform new education concertedly. The purpose of awareness education is basically to draw attention on security (Wilson & Hash, 2003). In addition to these findings, it is seen that students' daily computer usage frequency is also influenced by students' information security awareness. In Europe Online Kids Project, it is stated that 25 percent of the students in Turkey were exposed to online hazards because of excessive use of the internet; this rate is 33.00% all across Europe (EU Kids Online, 2011). According to the data obtained from Turkish statistical institute in 2015 April, rate of families who have internet access throughout Turkey is 69.50% and the individuals whose age range vary from 16 to 74 utilize the internet at home. If students' daily computer use has an influence on students' information security awareness, parents should monitor their children while they utilize the internet at home. For this, some measures could be taken as follows (ENISA, 2011):

- Install filtering and parental control software on children's computers.
- Advise children not to share their passwords with friends or others.
- Be part of children's activities in the Virtual World,
- Educate children about taking responsibility of using technology in general.

However, in order to implement these measures, parents must have awareness of information security and sufficient level of knowledge about it. When the students' responses under the social networking awareness theme are analyzed in the study; the number of the students who could (or did) control sharing personal information, block messages and applications from unwanted people, adjust security settings of their profiles/pages were higher than average; and compared to other themes, students' awareness was higher in this theme. In the Europe Online Kids Project, it is found that 59.00% of the children varying between 9-16 ages have a social media account and 26.00% of children having a social media account have public profiles (EU Kids Online, 2011). Additionally, in some of the studies conducted to assess security on social networking sites, it is found that youth have inadequate knowledge about security on social networking sites (Kasikci et al., 2014; Lawler & Molluzzo, 2010). The differences in the results of this study and the aforementioned studies could be derived from the different level of use of the social networking sites as majority of the students use these networks and thus, they are expected to be more knowledgeable which in turn leads them to have high level of awareness.

Children and youths experience the following technical problems while using computer and internet; computers are infected with virus and trojan software due to user actions, breaking down the computer, and losing information and files (documents) and compromising software settings due to the previous problems (Canbek & Sagirolu, 2007). In this study, students' answers under the threats and protection methods theme revealed that students had high awareness level due to the damages that dangerous software and viruses cause, awareness of protection software against malware, using this type of software, and recognizing whether there was an infection of this type of software. It was found out in a study conducted by Yildirim and Varol (2013) that many users did not use antivirus software. Similarly, in the study conducted by Tekerek and Tekerek (2013) it is found that students' awareness of malicious software scanning, document protection, personal computer protection, firewall and filtering software is low. In addition, students reported that their knowledge about safe internet and computer use is inadequate. While anti-spam and antivirus software usage rates are 72.00% in Europe, it is 46.00% in Turkey (Kasikci et al., 2014). In our study, it is seen that students' antivirus software use rate was increased. This rise could be a consequence of the students' adaption of computer and mobile devices due to personal usage and as a result of intention of protecting personal information. In other words, students may not be taking serious of protecting their personal information on the ICT tools that they share with their parents, since they may be limiting their personal information on them; however they might be taking protecting their personal information seriously on their personal ICT tools.

E-mail, and instant messaging types of communication environments are open to exploit children (Bilgin, 2007; cite in Celen, Celik, & Seferolu, 2011). Probability of students being exploited got high due to possibility of students interacting with others online both in school and outside of the school with an increasing possibility on the personal computers and internet access used by teens. For this reason, it is expected that students have awareness of this issue. For the questions to assess awareness of the students of email security, almost half of the students claimed that they hide the identities of the receivers in multiple emails, mark the emails from unknown senders as a spam, scan the attached documents with antivirus software before opening them, and do not click on the links in the emails from unknown senders. In the fourth theme of password protection, most of the students reported that they save their passwords in notebooks in order not to forget them, use the same passwords for different environments, could not create strong and secure passwords, and did not know how to retake their accounts back when their passwords were hacked. In general, it could be said that students' awareness of email use is higher than their awareness of creating a secure password. However, when we consider that the use of secure password is a prerequisite for safe email usage; students were under a security risk even for this use. In the study conducted by Tekerek and Tekerek (2013) on K-12 students, it is found that students' password security awareness is low. In another study conducted by Mert, Bulbul and Sagirolu (2012) on eight grade students, it is found that 30.00% of the students only used small letters, 17.00% of the students used only numbers, 17.00% of the students used various combinations of uppercase, small case and numbers, and only 1.00% used special characters in their passwords. The

research conducted by Kruger, Drevin and Steyn (2010) was revealed that half of the participants do not know the meaning of a strong password. The findings about the email and password security issues emerged from the present study are similar to the findings in their study.

In general, majority of the students' awareness and knowledge of social networking security, threats, and protection methods theme were found to be high. Almost half of the students' awareness of the themes regarding access and password security and email security awareness were found to be high in comparison to the other themes; however majority of the students' threats and protection methods, software installation, internet and network security, user awareness and social engineering were found to be low. In general, themes were reviewed and interpreted by grouping the students' responses of "never", and "rarely" together and "often" and "always" together. However, when considering safe computer and internet use as a sensitive issue, the ideal interpretation of the student responses should be in both ends; for instance, only "always" and "never" responses as both ends should be considered due to the fact that information security is either (always) ensured or not (never).

In summary, it could be said that nowadays students have an individual technology access since computer and internet technologies are getting cheaper, however the students' safe computer and internet use awareness under these six themes was found to be low. Although there are internet filtering software used in schools and safe internet and computer use content is taught in ICT courses, these implications are not enough to raise sufficient awareness of the students regarding safe internet and computer use. Furthermore, although it was acknowledged that safe ICT usage would significantly take place in the schools and thanks to the revision in ICT courses, it is seen that this provision is not implemented effectively as intended. In the future studies, students', teachers', and administrators' opinions on using internet filtering software at the schools could be investigated. Curriculum studies about safe internet and computer use in ICT courses could be conducted. Although pre-service students enrolled in the Department of Computer and Instructional Technologies Education claimed that they have necessary knowledge and skills to ensure personal safe internet and computer use (Kurtoğlu Erden, 2014), it is suggested that pre-service teachers should have training on internet access, ICT literacy, technical infrastructure, ethical and legal issues for citizen groups, information security and security to increase their awareness in order to improve e-democracy culture and online political process (Yıldız & Seferoğlu, 2014). According to Kaya and Tuna (2010) regardless of parents' education levels if the parents do not spend enough time with their children, if they do not guide their children on using ICT safely and do not have enough knowledge on these issues, it is highly likely that their children spend plenty of time with these technologies and develop unwanted behaviors or habits. For this reason, it is essential to inform the public about the educational activities on these aspects. A good example of a web based resource to improve safe internet and computer use awareness could be a web site developed by TUBITAK BILGEM in the "I am Protecting my Information E-Learning Project". In order to establish the widespread effects of these resources, they could be used in ICT courses and in the courses delivered by Public Education Centers. Also, public service announcement can be prepared regarding these issues for teachers, managers and students. The parents can be acknowledged about safe internet and computer use through seminars at the schools.

### **Limitations and Suggestion for Future Research**

The present research adopting a descriptive survey method has several limitations. Firstly, research data were gathered with a questionnaire developed by the researchers. In the future studies, both quantitative and qualitative methods could be used for gaining deeper understanding of the related issues. Also, items of questionnaire were written by taking account of students' most frequent behaviors on safe computer and internet use. However given that this topic is an extensive topic, user awareness can be measured by utilizing different instruments that are broader in scope and with additional themes. The other limitation of this research is that sampling is limited to the students who study in secondary schools in Bartın Province in Turkey and who are in 15-18 age groups. In other words,

research findings represent only secondary school students' safe internet and computer use awareness. In the future studies, conducting different studies dealing with the students from different age groups and grades and different provinces would contribute to the literature. Also, new studies could be carried out with administrators, policy makers, parents and teachers. Considering that safe internet and computer use is a cultural phenomenon and the families have the most important role, studies with parents would contribute to the literature.

#### **Acknowledge**

This research was supported by the Scientific Research Projects Commission of Bartın University, Turkey (Project No: 2014-SOS-A-004).

## Türkçe Sürüm

### Giriş

Bilgi ve iletişim teknolojilerinin (BİT) kullanımı çocuk ve gençler arasında hızla yaygınlaşmaktadır. Öğrencilere, okulda ve okul dışı zamanlarda çeşitli öğrenme deneyim ve fırsatları sağlamak adına ebeveynler, eğitimciler ve politika belirleyiciler bilgisayar, mobil aygıt ve internet erişimi gibi çeşitli teknolojik imkânlar sunmaya çalışmaktadır. Her ne kadar bu teknolojiler, çocuk ve gençlerin bilişsel ve sosyal gelişimleri için bir fırsat olsa da, aynı zamanda onları birçok tehdit ve tehlike ile karşı karşıya da bırakabilmektedir. Bu teknolojilerin çocuk ve gençler tarafından yanlış kullanımı ebeveynler ve eğitimciler üzerinde ciddi kaygılar oluşturmaktadır. Bu teknolojileri kullanan çocuk ve gençler; pornografi, siber zorbalık, çevrimiçi yağmacılık, yanlış bilgilendirme, şiddet ve nefret içeren içerikler, kumar ve internet bağımlılığı, veri kayıpları, maddi kayıplar gibi tehdit ve tehlikelere karşı savunmasız kalabilmektedir. Söz konusu bu tehdit ve tehlikelerle mücadele etmede ise güvenli bilgisayar ve internet kullanımının sağlanması önemli bir olgu olarak karşımıza çıkmaktadır (Yenilmez & Seferoğlu, 2013).

Araştırmacılar güvenli bilgisayar ve internet kullanımının sağlanmasında, teknik ve yasal yaptırım ve uygulamaların bir çözüm olarak kullanıldığını ifade etmekle birlikte (Ben-Asher & Gonzalez, 2015; Choo, 2011), güvenliğin sağlanmasında en önemli unsurun insan faktörü olduğunu belirtmektedir (Arachchilage & Love, 2014; Shillair et al., 2015; Van Bruggen, 2014). Ayrıca, kullanıcıların internet ortamındaki güvenliklerini sağlayabilmede; engellemeler, yasaklamalar, yaptırımlar yerine bireysel bilgi ve farkındalıklarının artırılmasının daha önemli olduğu ifade edilmektedir (Chou & Peng, 2011; Cole, 2014; Valcke et al., 2007; Yan, 2009). Örneğin, Vicks (2013) tarafından gerçekleştirilen araştırmada, ortaokulda öğrenim gören öğrencilerin güvenli bilgisayar ve internet kullanımının sağlanmasında okuldaki internet filtrelerinin kullanımının etkisi incelenmiş, araştırma sonucunda aşırı kısıtlayıcı politikaların eğitsel çevrimiçi kaynaklara erişimi engelleyebildiği ifade edilmiştir. Araştırmacı, kısıtlamalar yerine güvenli internet kullanımına yönelik bilgi ve farkındalığın artırılmasına, doğru internet kullanım kültürünün oluşturulmasına dikkat çekmektedir. Murray (2014) tarafından gerçekleştirilen araştırmada ise, teknoloji destekli Katolik lisesinde öğrenim gören gençlerin güvenli internet kullanımları ile zorbalık ve pornografi davranışları incelenmiştir. Araştırma sonucunda öğrencilerin büyük çoğunluğunun her gün internete girdiği, %96.00'sinin sosyal medya kullandığı, BİT kullanımlarının güvenli olmadığı ve çok sık zorbalık ve pornografi durumları ile karşılaştığı görülmüştür. Araştırmacı bunun çözümü için de öğrenci, ebeveyn, öğretmen ve yöneticilerin güvenli bilgisayar ve internet kullanımı farkındalıklarının artırılmasına dikkat çekmektedir. Bu noktadan hareketle, bilgi güvenliğini çocuklarda kazandırmada anne ve babalar da dâhil olmak üzere birçok paydaşın işbirliğine ihtiyaç olduğu görüşüne ulaşılabilmektedir.

Güvenli bilgisayar ve internet kullanımının sağlanmasında insan faktörünü ve kullanıcı farkındalığını ele alan araştırmalarda genel olarak; kullanıcıların güvenli bilgisayar ve internet kullanımı farkındalık durumları, güvenli BİT kullanım davranışlarının ortaya betimlenmeye çalışıldığı (Leach, 2003; Rhee, Kim, & Ryu, 2009; Van Bruggen, 2014), bazı araştırmalarda da güvenli bilgisayar ve internet kullanımı eğitimlerinin kullanıcı farkındalığına olan etkisinin incelendiği görülmektedir (Chou & Peng, 2011; Harris, 2010). Bilgi güvenliği ile ele alınan bazı değişkenler siber zorbalık (Murray, 2014), sosyal ağlarda bilgi paylaşım davranış durumları (Tamjidyamcholo et al., 2014), okullarda internet filtresi kullanımıyla ilgili öğrenci görüşleri ortaya konulmaya (Vicks, 2013) şeklinde örneklendirilebilir. Yapılan araştırmaların büyük çoğunluğunda da üniversite öğrencileri ve yetişkinler ile çalışılmıştır. Öte yandan, BİT kullanımının getirmiş olduğu riskler açısından en çok tehdit altındaki grubun çocuk ve gençler olduğu (Cole, 2014) dikkate alındığında ise bu gruplar üzerinde yeni araştırmalar yapılmaya başlandığı görülmektedir (Alhejaili, 2013; Al-Jerbie & Jali, 2014; Chen, 2014; Cole, 2014; Murray, 2014; Ngoqo & Flowerday, 2015; Tsim, 2006; Valcke, Schellens, Van Keer, & Gerarts, 2007; Vicks, 2013; Wishart, 2004; Yan, 2009). Ancak çocukların bilgi güvenliği düzeyi her ülkede farklılık göstermektedir; dolayısıyla yerel sınırlar içinde

durumu ortaya koyan çalışmalara ihtiyaç vardır. Buna koşut olarak, Deisman'a (2008) göre güvenli bilgisayar ve internet kullanımı farkındalık araştırmalarının ulusal/bölgesel düzeyde incelenmesinde yarar vardır. Çünkü eğitim düzeyi, ebeveyn farkındalık durumları, internet erişim politikalarındaki farklılaşmalar gibi birçok faktör çocuk ve gençlerin güvenli bilgisayar ve internet kullanımı farkındalık düzeylerinde değişikliğe yol açabilmektedir. Bu nedenle konuyla ilgili çocuk ve gençlerin farkındalık durumlarının ulusal/bölgesel düzeyde araştırılması ve buna göre planlamalar yapıp önlemler alınması önemlidir. Araştırmacılara göre çocuk ve gençlerin güvenli bilgisayar ve internet kullanımı farkındalıklarını; yaş grubu, okulun teknoloji kullanım durumu ve güvenlik politikaları, ailesel ve çevresel koşullar gibi daha spesifik değişkenleri ele alarak inceleyen yeni araştırmalara ihtiyaç duyulmaktadır (Berrier, 2007; Harshman, 2014; Vicks, 2013).

Ulusal alanyazın incelendiğinde, Türkiye'de güvenli bilgisayar ve internet kullanımıyla ilgili olarak katılımcıları yetişkinler, formatör öğretmenler ve üniversite öğrencileri olan çeşitli araştırmaların (Çakır, Hava, Gülen, & Özüdoğru, 2015; Demirel, Yörük, & Özkan, 2013; Gökmen & Akgün, 2015; Karaoğlan Yılmaz, Yılmaz, & Sezer, 2014; Küçükali & Bülbül, 2015) yapıldığı görülmektedir. Öte yandan, çocuk ve gençler üzerine yapılan araştırmaların sayısının ise sınırlı kaldığı (Kaşıkçı et al., 2014; Tekerek & Tekerek, 2013) söylenebilir. Bu konuda yapılmış kapsamlı araştırmalardan biri olan Avrupa Çevrimiçi Çocuklar Projesinde, Türkiye ve Avrupa'daki çocukların internetteki faaliyetleri, karşılaştıkları riskler ve ebeveynlerin çocuklarının internet yaşantıları ile ilgili farkındalıkları raporlanmıştır (Kaşıkçı et al., 2014). Araştırmaya 9-16 yaş arasında olup internet kullanan 1018 öğrenci ve ebeveyn dâhil edilmiştir. Sonuçlar, katılımcıların %40.00'inin kendisine ait bilgisayar ya da dizüstü bilgisayara sahip olduğunu, %39.00'unun ise diğer aile fertleri ile bilgisayarı paylaştıklarını ve günde ortalama 74 dakika internet kullandıklarını göstermiştir. Ayrıca araştırma, Türkiye'deki çocukların %60.00'inin okulda internet'e bağlandığı, %51.00'inin ise internet kafeleri kullandığı ve ev dışı kullanımlar nedeniyle ebeveynlerin çocukların internet kullanımını denetleyemediği, çocukların büyük bölümünün internet kullanım becerilerinin yeterli olmadığını ve birçok çevrimiçi risklere maruz kaldıklarını göstermektedir. Tekerek ve Tekerek (2013) tarafından yapılan farklı bir araştırmada ise, Maraş ilinde ilköğretim ve lise öğrencilerinin bilgi güvenliği farkındalık durumları ortaya konulmaya çalışılmıştır. Araştırma sonucunda öğrencilerin etik konulardaki bilgi güvenliği farkındalık düzeylerinin yeterli seviyede olduğu bulunmuştur. Ancak öğrencilerin kurallar ve bilgi gerektiren konulardaki farkındalık düzeylerinin düşük olduğu gözlenmiştir.

Ulusal alanyazında yapılan çalışmalar genel olarak değerlendirildiğinde, hedef kitlesi çocuk ve gençler olan araştırma sayısının sınırlı olduğu ve bu hedef kitleye yönelik kapsamlı araştırma bulgularına ihtiyaç duyulduğu anlaşılmaktadır. Türkiye'de çocuk ve gençlerin güvenli bilgisayar ve internet kullanımı farkındalıklarını inceleyen çeşitli araştırmaların yapılmaya başlandığı görülmektedir. Ancak çocuk ve gençlerin güvenli bilgisayar ve internet kullanımı farkındalıkları konusunda hala bilimsel araştırmalara ihtiyaç vardır. Kaşıkçı vd. (2014) tarafından gerçekleştirilen araştırma sonuçlarına göre Mayıs ve Haziran 2010 yılı verilerine göre Türkiye'deki öğrencilerin büyük çoğunluğunun okul ve internet kafelerden, bir kısmının da ebeveynleri ile ortak kullanılan bilgisayarlardan internete eriştikleri görülmektedir. Dolayısıyla okul ve internet kafelerde internet filtre programları, evde ise ebeveyn faktörü ile öğrenci denetimi kısmen de olsa sağlanabilmektedir. Son yıllarda ucuzlayan bilgisayar ve internet teknolojileri gençler arasında hızla yaygınlaşsa da bu teknolojilerin gençler üzerinde oluşturacağı tehditlerle ilgili alınan önlemlerin hala sınırlı olduğu söylenebilir. Okul içinde BT dersleri ve internet filtresi, okul dışında ise ebeveyn kontrolü ile kısmen de olsa güvenli bilgisayar ve internet kullanımı sağlanmaktadır. Ancak ebeveyn kontrolü yalnızca ortak kullanılan bilgisayarlara ile sınırlıdır. Günümüzde bireysel teknoloji erişim imkânları (özellikle mobil cihazlar ile) göz önünde bulundurulduğunda ise ebeveyn denetimlerinin de azalabileceği bir gerçektir. Bu nedenle gençlerin bireysel güvenli bilgisayar ve internet kullanım alışkanlıklarının belirlenmesi, farkındalıklarının bilinmesi ve bu farkındalık durumlarına göre çeşitli önlemler alınması gerekmektedir.



### **Bilge Güvenliği Kapsamında Ele Alınan Konular**

Alanyazındaki çalışmalarda, hangi konuların bilgi güvenliği dâhilinde ele alındığına bakıldığında ise genellikle şu üç başlık vurgulanmaktadır: Gizlilik, bütünlük ve erişilebilirlik (Güldüren & Keser, 2015; Kritzinger & Smith, 2008). Bu başlıklar ayrıtıldığında, araştırma sonuçlarına göre özellikle; erişim ve şifre güvenliği, sosyal ağ güvenliği, tehditler ve korunma yolları, yazılım yükleme ve güncelleme, e-posta güvenliği, internet ve ağ güvenliği, sosyal (veya toplum) mühendisliği (bir bilgisayar korsanının kimliğini gizleyerek veya farklı göstererek karşı tarafı aldatmaya dönük hileleri) ve kullanıcı farkındalığı gibi farklı boyutlara yönelik birçok tehdidin ve kullanıcı hatalarının bilgi güvenliği açıklarına yol açtığı ifade edilmektedir (Alhejaili, 2013; Arachchilage & Love, 2014; Berrier, 2007; Chen, 2014; Van Bruggen, 2014; Valcke et al., 2007).

Örneğin; bilgisayarın ortak kullanımı, güçlü olmayan şifrelerin tercih edilmesi, şifre isteyen tüm ortamlarda aynı şifrenin kullanılması, şifrenin not defteri gibi herkesin ulaşabileceği ortamlara yazılması, şifrelerin başkaları ile paylaşılması bilgi hırsızlığına yol açan başlıca durumlardandır. Yine, bilgisayara güvenirliliği test edilmemiş ortamlardan program yüklenmesi ve bilgisayardaki güvenlik yazılımlarının güncellenmemesi, internet ve ağ ortamlarında güvenli olmayan paylaşımların yapılması kullanıcıları bilgi güvenliği tehditleri ile karşı karşıya bırakabilmektedir. Ayrıca kullanıcıların tehdit olabilecek zararlı programları bilmemesi, sosyal mühendislik gibi kavramlara aşina olmaması da güvenli bilgisayar ve internet kullanımı sorunlarına yol açan başlıca durumlardır. Bu problemler kullanıcıları yalnızca bilgi hırsızlığı değil, aynı zamanda pek çok maddi ve psikolojik sorunlarla da karşı karşıya bırakmaktadır. Bununla birlikte güvenli bilgisayar ve internet kullanımına ilişkin kullanıcı farkındalığını belirlemeye yönelik çalışmalarda kullanıcı farkındalığının çoğunlukla belirli boyutlar açısından incelendiği görülmektedir. Ancak bilgi güvenliğinin bir bütün olduğu göz önüne alındığında kullanıcı farkındalığını belirlemeye yönelik kapsamlı çalışmalara duyulan ihtiyaç alanyazında kendini hissettirmektedir.

Sonuç olarak, alanyazındaki çalışmaların da ortaya koyduğu gibi bilgi güvenliğini sağlamanın en temel ekseninde teknolojilere yatırım yapmaktan ve de korunma amaçlı teknolojileri kullanmaktan ziyade insanların bilinçlenmesi, güvenlik teknolojilerini doğru zamanda ve yerde kullanması (Güldüren & Keser, 2015) ve bu doğrultuda farkındalıklarının artırılması gerekmektedir. Farkındalık, öğrencilerin mağdur olmaması için dikkate alınması gereken ilk faktörlerdendir ve bu yönü ile öğrencilerin kendilerini korumalarında hayata dönük temelleri olan bir etkidir. Ancak, ülkemizde giderek artan bilişim güvenliği tehditlerinin sonucunda ortaya çıkan bilişim suçları (Gökmen & Akgün, 2016) dikkate alındığında özellikle genç yaştaki bireylerin mağdur olmadan güvenlik karnelerinin ortaya çıkarılması gerekmekte iken özellikle genç yaştaki öğrencilerin bilgi güvenliği profilini farklı açılardan bütüncül olarak ortaya koyan ulusal/bölgesel düzeyde bir çalışmaya ihtiyaç duyulmaktadır. Ayrıca, öğrencilerin bilgi güvenliği durumlarının zaman içinde değişiklikler gösterebileceği dikkate alındığında, güncel bir çalışmaya ihtiyaç duyulmaktadır. Dolayısıyla, güvenli bilgisayar ve internet kullanımı farkındalığı ile ilgili araştırma sonuç ve önerileri dikkate alındığında gerçekleştirilen bu araştırmanın amacı, lise öğrencilerinin güncel güvenli bilgisayar ve internet kullanım farkındalık profillerini ortaya koymaktır. Bu amaç doğrultusunda araştırmada geliştirilen alt-temalar dikkate alınarak aşağıdaki sorulara yanıt aranmaya çalışılmıştır:

1. Öğrencilerin erişim ve şifre güvenliği hakkındaki farkındalıkları ne düzeydedir?
2. Öğrencilerin sosyal ağ güvenliği hakkındaki farkındalıkları ne düzeydedir?
3. Öğrencilerin tehditler, korunma yolları, yazılım yükleme ve güncellemeye ilişkin farkındalıkları ne düzeydedir?
4. Öğrencilerin e-posta güvenliğine ilişkin farkındalıkları ne düzeydedir?
5. Öğrencilerin internet ve ağ güvenliğine ilişkin farkındalıkları ne düzeydedir?
6. Öğrencilerin kullanıcı farkındalıkları ve sosyal mühendisliğe ilişkin farkındalıkları ne düzeydedir?

## Yöntem

### Araştırma Modeli

Bu çalışmada, nicel araştırma yöntemlerinden betimsel modelden yararlanılmıştır. Betimsel modelde amaçlanan, var olan bir durumu istenilen temalar altında ortaya koymak ve açıklamaktır. Araştırmada da, liselerde öğrenim gören öğrencilerin güvenli bilgisayar ve internet kullanım farkındalıklarını farklı temalar altında inceleyerek var olan durum ortaya koymak istendiği için betimsel model seçilmiştir.

### Katılımcılar

Araştırmanın evrenini Bartın İl Merkezindeki liselerde öğrenim gören öğrenciler oluşturmaktadır. 2014 – 2015 eğitim öğretim yılı verilerine göre Bartın il merkezinde lise düzeyindeki okul sayısı 17, öğrenci sayısı ise 8299'dur. Evreni temsil edecek örnekleme seçilirken "Tabakalı Örneklem Tekniği" kullanılmıştır. Tabakalı örnekleme evrene ait tüm elemanların eşit seçilme şansına sahip olduğu bir tekniktir. Bu çalışmada örnekleme belirlemek amacıyla evren; a. Okul türleri (Anadolu liseleri, Fen lisesi, Mesleki ve teknik anadolu liseleri, Güzel sanatlar lisesi ve İmam hatip liseleri), b. Sınıf düzeyi (9., 10., 11. ve 12. Sınıf) c. Şube olmak üzere 3 tabakaya ayrılmıştır. Bu çalışmada "tabakalı örnekleme yöntemi" ile belirlenen 3029 öğrenci çalışmanın örneklemini oluşturmaktadır.

Gönüllülük esasına dayalı olarak toplanan verilerde, araştırmacılar tarafından geliştirilip uygulanan anketin %5.00'ünden fazlasını eksik dolduranların anketleri geçersiz sayılmış ve toplam 2029 öğrenciden elde edilen veriler analiz edilmiştir. Araştırmaya katılan öğrencilerin demografik özelliklerine aşağıda yer verilmiştir. Araştırma kapsamında 1087 kız ve 942 erkek öğrenciye ulaşılmıştır. Söz konusu öğrencilerin %94.00'ü (f=1907) bireysel olarak kullandığı bilgisayar ya da mobil cihaza (akıllı telefon, tablet bilgisayar vb.) sahip olduğunu ve öğrencilerin %76.00'si (f=1542) da kişisel bilgisayar ya da mobil cihazlarında internet bağlantısına sahip olduklarını belirtmişlerdir. Örnekleme oluşturan öğrencilerin %23.80'i (f=482) güvenli bilgisayar ve internet kullanımı konusunda eğitim aldığını belirtirken, %76.20'si (f=1547) bu konuda herhangi bir eğitim almadığını belirtmiştir. Öğrencilerin günlük bilgisayar / mobil cihaz kullanma sürelerine bakıldığında %10.50'inin (f=396) her gün bilgisayar/mobil cihaz kullanmadığı, %22.10'unun (f=499) yaklaşık yarım saat, %37.90'ının (f=768) 1 ila 2 saat arasında, %14.20'sinin (f=289) 3 ila 4 saat arasında ve %6.30'unun (f=127) 4 saatten fazla kullandığı belirlenmiştir. Öğrencilerin günlük internet kullanma sürelerine bakıldığında %5.20'sinin (f=105) her gün internet kullanmadığı, %18.20'sinin (f=369) yaklaşık yarım saat, %40.20'sinin (f=816) 1 ila 2 saat arasında, %21.30'unun (f=432) 3 ila 4 saat arasında ve %15.10'unun (f=307) 4 saatten fazla kullandığı belirlenmiştir. Bu bulgular Avrupa Çevrimiçi Çocuklar Projesindeki (Kaşıkçı et al., 2014) Mayıs ve Haziran 2010 yılı verilerine göre Türkiye ortalaması ile karşılaştırıldığında örnekleme oluşturan öğrencilerin günlük internet kullanım sürelerinin arttığı anlaşılmaktadır.

### Veri Toplama Araçları

Bu çalışmadaki veriler, araştırmacılar tarafından geliştirilmiş olan bir anket ile elde edilmiştir. Araştırmada veri toplama aracı olarak anketin tercih edilmesinin temel nedeni alanyazında güvenli bilgisayar ve internet kullanımı farkındalığını belirlemede kullanılan; erişim ve şifre güvenliği, sosyal ağ güvenliği, tehditler, korunma yolları, yazılım yükleme ve güncelleme, e-posta güvenliği, internet ve ağ güvenliği, kullanıcı farkındalıkları ve sosyal mühendislik alt boyutlarını da içeren bir ölçme aracına ihtiyacın olmasıdır.

Anket geliştirme sürecinin birinci aşamasında problem durumu belirlenmiş ve alanyazın (Alhejaili, 2013; Al-Jerbie & Jali, 2014; Arachchilage & Love, 2014; Berrier, 2007; Chen, 2014; Chou & Peng, 2011; Kaşıkçı et al., 2014; Lawler & Molluzzo, 2010; Murray, 2014; Ngoqo & Flowerday, 2015; Shillair et al., 2015; Tsim, 2006; TÜBİTAK BİLGEM, 2011; Valcke et al., 2007; Van Bruggen, 2014) incelenerek bu problem durumuna uygun temalar belirlenmiştir. Bu alt temalar; erişim ve şifre güvenliği, sosyal ağ

güvenliği, tehditler, korunma yolları, yazılım yüklemeye ve güncelleme, e-posta güvenliği, internet ve ağ güvenliği, kullanıcı farkındalıkları ve sosyal mühendislik şeklindedir. Alt temaların belirlenmesinin ardından alanyazın taramasından elde edilen bilgiler doğrultusunda, 60 madde yazılarak bir madde havuzu oluşturulmuştur. Madde havuzundan anket taslak formunda yer alması uygun bulunan 53 madde seçilmiş ve likert tipi derecelendirme ile ön uygulama formu oluşturulmuştur. Anketin geçerliğini sağlamak üzere bir belirtke tablosu, oluşturularak bir Türk Dili uzmanı ve bilgi güvenliği ve etik konularında çalışan beş eğitim teknolojisi alan uzmanının görüşüne başvurulmuştur. Dil uzmanı yazılan anket maddelerini dil ve anlatım, anlaşılabilirlik açılarından incelemiştir. Eğitim teknolojisi alan uzmanları ise anket maddelerini kapsam, ölçüt, yapı ve görünüş geçerliği açısından değerlendirmişlerdir. Uzmanlardan gelen dönütler doğrultusunda anket üzerinde gerekli düzenlemeler yapılmıştır. Ardından anketin pilot uygulaması örneklem dışındaki bir lisede öğrenim gören ve bilgisayar ve internet kullanan 60 öğrenci üzerinde gerçekleştirilmiş ve dil geçerliği, anlaşılabilirlik, seviyeye uygunluk gibi kriterler açısından değerlendirilerek yeniden düzenlenmiş ve ankete son şekli verilmiştir. Anketin son hali, dokuz bölüm ve 47 sorudan oluşan beşli likert olarak yapılandırılmıştır. Araştırmacılar tarafından uygulanan anket sonucunda elde edilen veriler arasından eksik veriler çıkarıldıktan sonra frekans analizine tabii tutularak araştırma bulguları raporlanmıştır. Hesaplamalar dokuz tema için ayrı ayrı yapılmıştır. Genel olarak temaların değerlendirilmesi sürecinde “hiçbir zaman” ile “nadiren”; “çoğu zaman” ile “her zaman” gözenekleri birlikte yorumlanarak değerlendirilmiştir.

### Verilerin Analizi

Ankete ilişkin faktör yük değerleri, ölçümler için örneklemin uygunluğunu belirlemede KMO (Kaiser-Meyer- Olkin Mesasure of Sampling Adequacy) katsayı değeri, maddeler arası tutarlılığı belirlemede Bartlett Testi ve güvenilirlik için Cronbach Alfa Güvenirlik Katsayısı'na bakılmıştır. 47 maddenin faktör yük değerleri .36 ile .62 arasında değişmektedir. KMO değeri ise .86 bulunmuştur. KMO değeri 1'e yaklaşıkça yapılan faktör analizi daha anlamlı hale gelmektedir. KMO değerinin .50 ve .70 arasında olması orta düzey, .71 ve .80 arasında olması iyi düzey ve .81 ve .90 arasında olması çok iyi düzey ve .91 ve üzeri olması mükemmel olarak adlandırılmaktadır (Field, 2005). Buradan hareketle örneklemin veri analizi için yeterli olduğu söylenebilir. Yapılan Bartlett testiyle analizlerin sonucunun anlamlı olduğu görülmüştür (Ki-kare= 16025.23,  $p < .01$ ). Anketin güvenilirliği incelendiğinde Cronbach Alfa Güvenirlik Katsayısı'nın .86 olduğu belirlenmiştir. Bu sonuçlar ölçme aracının güvenilir olduğunu göstermektedir. Toplanan verilerin analizinde frekans ve yüzde değerleri kullanılmıştır.

### Bulgular

Araştırma bulguları veri toplama aracının geliştirilmesi sürecinde belirlenen temalar doğrultusunda aşağıda sırasıyla sunulmuştur. Birinci alt tema olan erişim ve şifre güvenliği konusunda öğrencilerin farkındalıklarını belirlemeye yönelik olarak toplanmış olan verilere Tablo 1'de yer verilmiştir. Tablo 1 incelendiğinde öğrencilerin yaklaşık yarısının bilgisayar ve erişim güvenliği konusunda farkındalıklarının yüksek olduğu, diğer öğrencilerin ise bu konulardaki farkındalıkları açısından risk altında olduğu anlaşılmaktadır. Tablo 1'e göre öğrencilerin %49.40'ının bilgisayar/diğer elektronik cihazlara şifre ile giriş yaptığı, %46.40'ının bu cihazların geçici olarak kapandığında da oturumu tekrar şifre ile açtıkları belirlenmiştir. Ayrıca öğrencilerin büyük çoğunluğunun bilgisayar ve diğer mobil cihazlarını başkaları ile kullandıkları/paylaştıkları görülmektedir. Tablo 1'deki bulgulara göre öğrencilerin %15.10'unun hesaplarının şifrelerini herhangi bir yere yazmadığı, %43.90'ının hesabı başkası tarafından ele geçirildiğinde geri alabildiği, %13.8'inin hesaplarında aynı şifreyi hiç kullanmadığı, %55.80'inin şifrelerinin en az sekiz karakterden oluştuğu, %45.00'inin şifrelerinde özel karakterlerin bulunduğu, %23.00'ünün şifrelerinde sıralı karakter bulunmadığı görülürken, %21.70'inin de şifrelerinde kişisel bilgi bulundurmadığı belirlenmiştir. Tablo 1'deki maddeler dışında öğrencilere şifrelerini ne kadar sıklıkla güncelledikleri sorulmuştur. Öğrencilerin %23.60'ının (f=478) güncelleme yapmadığını, %16.70'inin (f=338) her ay, %19.20'si (f=389) üç ayda bir, %14.10'u (f=286) altı ayda bir, %14.20'si (f=289) yılda bir ya da daha uzun sürede yaptığını ve %12.30'u (f=249) güncelleme önerisini sitenin yapmasını beklediğini belirtmiştir.

**Tablo 1.**  
*Öğrencilerin Erişim ve Şifre Güvenliği Hakkındaki Farkındalıkları.*

Farkındalıklar		Hiçbir zaman	Nadiren	Arada sırada	Çoğu zaman	Her zaman
Bilgisayar ya da diğer elektronik cihazlarımı açarken başlangıçta şifre ile giriş yaparım.	f	216	312	497	500	504
	%	10.60	15.40	24.50	24.60	24.80
Bilgisayarın ya da diğer elektronik cihazlarımın başından kısa bir süreliğine de olsa ayrıldığımda oturumu kapatır ve tekrar şifre ile açarım.	f	217	400	470	467	475
	%	10.70	19.70	23.20	23.00	23.40
Kişisel bilgisayarımı, telefonumu vb. yi aile, arkadaş gibi yakınlarla paylaşır, ortak kullanırım.	f	152	357	500	462	558
	%	7.50	17.60	24.60	22.80	27.50
İnternet, e-posta, Facebook gibi hesaplarımın şifrelerini unutmamak için not defteri gibi bir yerlere yazarım.	f	306	429	512	359	423
	%	15.10	21.10	25.20	17.70	20.80
Şifrem başkasının eline geçtiğinde hesabımı geri alabilirim.	f	231	262	536	524	476
	%	11.40	12.90	26.40	25.80	23.50
Şifre isteyen tüm ortamlarda (bilgisayara giriş, e-posta, cep telefonu, Facebook gibi) aynı şifreyi kullanırım.	f	281	387	481	469	411
	%	13.80	19.10	23.70	23.10	20.30
En az sekiz karakterden oluşan şifreler kullanırım.	f	187	279	431	475	657
	%	9.20	13.80	21.20	23.40	32.40
Şifrelerimde; büyük ve küçük harfler ve harflerin yanı sıra, rakam ve "? , @ , ! , # , % , + , - , * , %" gibi özel karakterleri tercih ederim.	f	319	364	433	465	448
	%	15.70	17.90	31.30	22.90	22.10
Şifrelerim 1, 2, 3, 4 gibi ya da a, b, c, d gibi klavyedeki harf sırası, alfabedeki harf sırası gibi sıralı karakterler içerir.	f	467	292	483	406	381
	%	23.00	14.40	23.80	20.00	18.80
Şifrelerim ad, soyadı, doğum tarihi, doğum yeri, TC Kimlik No gibi kişisel bilgileri içerir.	f	441	347	395	508	338
	%	21.70	17.10	19.50	25.00	16.70

İkinci alt tema olan sosyal ağların güvenliği konusunda öğrencilerin farkındalıklarını belirlemeye yönelik olarak toplanmış olan verilere Tablo 2’de yer verilmiştir. Çalışmaya katılan öğrencilerin %91.80’i (f=1863) sosyal ağ kullandığını, %8.20’si (f=166) sosyal ağ kullanmadığını ifade etmiştir. Sosyal ağ kullananların öğrencilerin 1799’u sosyal ağ hesabı olduğu konusunda ebeveynlerinin haberi olduğunu, 34’ü ebeveynlerinin haberi olmadığını ve 30 tanesi de bu konudan tam emin olmadığını belirtmiştir. Tablo 2 incelendiğinde öğrencilerin %42.30’unun sosyal ağlarda kişisel bilgilerini paylaşmadığı, %58.00’inin sosyal ağlarda tanımadığı kişilerden gelen mesajları/istekleri engelleyebildiği, %60.10’unun sosyal ağlardaki paylaşımlarının güvenliğini sağlayabildiği, %57.90’ının rahatsız edici gönderi/iletilemlerle ilgili şikâyet oluşturabildiği ve %57.90’ının grupların/sayfaların gizlilik ayarlarını değiştirebildiği görülmektedir. Tablo 2 genel olarak değerlendirildiğinde öğrencilerin yarısından fazlasının sosyal ağ güvenliği konusundaki bilgi ve farkındalıkları yüksek olarak değerlendirilebilir. Bunun nedeni olarak da sosyal ağların öğrenciler arasında çok fazla kullanılıyor olması ve bu kullanıma bağlı olarak öğrencilerin bu konularda deneyim sahibi olmaları görülebilir.

**Tablo 2.**  
*Öğrencilerin Sosyal Ağ Güvenliği Konusundaki Farkındalıkları.*

Farkındalıklar		Hiçbir zaman	Nadiren	Arada sırada	Çoğu zaman	Her zaman
Sosyal ağlarda (Facebook, Twitter vb.) kişisel bilgilerimi (doğum tarihi, doğum yeri, cep telefonu, ev adresi, okulum gibi) paylaşıyorum.	f	340	518	434	408	329
	%	16.80	25.50	21.40	20.10	16.20
Sosyal ağlarda tanımadığım kişilerden gelen istenmeyen mesajları / gönderileri / bildirimleri / arkadaşlık isteklerini engellerim.	f	100	323	428	563	615
	%	4.90	15.90	21.10	27.70	30.30
Sosyal ağlarda paylaşacağım gönderilerin kimlerin görebileceğini güvenlik ayarlarından değiştiririm.	f	169	261	379	421	799
	%	8.30	12.90	18.70	20.70	39.40
Sosyal ağlarda beni rahatsız eden bir gönderi / ileti ile karşılaştığımda o gönderi için şikâyet oluştururum.	f	204	271	379	453	722
	%	10.10	13.40	18.70	22.30	35.60
Sosyal ağlarda oluşturduğum grupların / sayfaların gizlilik ayarlarını değiştiririm.	f	140	303	411	470	705
	%	6.90	14.90	20.30	23.20	34.70
Sosyal ağ hesabıma yeni bir cihaz ya da tarayıcıdan giriş yapıldığında sosyal ağın bana uyarı göndermesini sağlayabilirim.	f	164	306	510	419	630
	%	8.10	15.10	25.10	20.70	31.00

Üçüncü alt tema olan tehditler, korunma yolları, yazılım yükleme ve güncellemeye ilişkin öğrencilerin farkındalıklarını belirlemeye yönelik olarak toplanmış olan verilere Tablo 3’de yer verilmiştir.

**Tablo 3.**  
*Öğrencilerin Tehditler, Korunma Yolları, Yazılım Yükleme ve Güncellemeye İlişkin Farkındalıkları.*

Farkındalıklar		Hiçbir zaman	Nadiren	Arada sırada	Çoğu zaman	Her zaman
Bilgisayar ya da diğer elektronik cihazlarıma (tablet, cep telefonu vb.) bulaşabilecek zararlı programların (virüs, casus yazılım, truva atı, solucan, spam gibi) neler olduğunu ve ne gibi zararlar verebileceğinin farkındayım.	f	121	310	451	494	653
	%	6.00	15.30	22.20	24.30	32.20
Zararlı programlardan koruma yazılımlarının (antivirüs, casus yazılım önleme gibi) neler olduğunu ve ne işe yaradıklarının farkındayım.	f	126	293	434	468	708
	%	6.20	14.40	21.40	23.10	34.90
Zararlı programlardan koruma yazılımlarını bilgisayarımın yükler ve etkin olarak kullanırım.	f	147	350	403	460	669
	%	7.20	17.20	19.90	22.70	33.00
Bilgisayarımın ya da diğer elektronik cihazlarıma zararlı yazılımların bulaşıp bulaşmadığını anlarım.	f	148	305	448	582	546
	%	7.30	15.00	22.10	28.70	26.90
İnternette bilgisayarımın ya da diğer elektronik cihazlarıma lisanslı olmayan (korsan) yazılımlar indirir ve yüklerim.	f	349	354	451	438	437
	%	17.20	17.40	22.20	21.60	21.50
İnternette yazılım, program vb. indirilecek sitenin güvenli olup olmadığını araştırırım.	f	250	332	438	480	529
	%	12.30	16.40	21.60	23.70	26.10

Tablo 3 incelendiğinde öğrencilerin %56.50’sinin bilgisayar/diğer elektronik cihazlara bulaşabilecek zararlı yazılımların farkında olduğu, %58.00’inin bununla ilgili önlem almak için kullanmaları gereken programların ne işe yaradığının farkında olduğu, %55.70’inin koruma yazılımlarını aktif olarak kullanabildiği ve %55.60’inin zararlı yazılımların bulaşıp bulaşmadığını anlayabildiği tespit edebilmiştir.

Tablo 3 genel olarak değerlendirildiğinde öğrencilerin yaklaşık yarısının tehditler ve korunma yolları konusundaki bilgi ve farkındalıkları yüksek olarak değerlendirilebilir. Diğer öğrencilerin ise bu konulardaki yeterlilik ve farkındalıkları açısından risk altında olduğu anlaşılmaktadır.

Tablo 3'teki bulgulara göre öğrencilerin %34.60'ının bilgisayar/diğer elektronik cihazlara korsan yazılımlar yüklediği, %49.80'inin internetten yazılım/ program indirdiği sitenin güvenli olup olmadığını araştırdığı tespit edilmiştir. Tablo 3'deki maddeler dışında öğrencilere antivirüs programlarını ne kadar sıklıkla güncelledikleri sorulmuştur. Öğrencilerin %17.20'si (f=348) güncelleme yapmadığını, %3.60'ı (f=73) her gün, %3.20'si (f=64) her hafta, %3.10'u (f=62) her ay, %3.30'u (f=67) altı ayda bir, %4.10'u (f=83) yılda bir ya da daha uzun sürede yaptığını ve %65.60'ı (f=1332) otomatik güncelleme yapıldığını belirtmiştir. Ayrıca öğrencilere dijital ortamdaki verileri ne kadar sıklıkla yedekledikleri sorulduğunda öğrencilerin %45.90'ı (f=931) yedekleme yapmadığını, %5.20'i (f=105) her gün, %7.30'u (f=148) her hafta, %14.20'si (f=288) her ay, %12.80'i (f=260) altı ayda bir, %14.60'ı (f=297) yılda bir ya da daha uzun sürede yaptığını belirtmiştir. Yazılım yükleme, güncelleme ve yedekleme teması genel olarak değerlendirildiğinde bu konularda bilgi ve farkındalığı yüksek olarak değerlendirilebilecek öğrenci sayısının yarının altında kaldığı söylenebilir. Bir diğer ifade ile öğrencilerin büyük çoğunluğunun bu konudaki yeterlilik ve farkındalıkları açısından risk altında olduğu anlaşılmaktadır.

Dördüncü alt tema olan e-posta güvenliği konusunda öğrencilerin farkındalıklarını belirlemeye yönelik olarak toplanmış olan verilere Tablo 4'de yer verilmiştir.


**Tablo 4.**  
*Öğrencilerin E-posta Güvenliği Hakkındaki Farkındalıkları.*

Farkındalıklar		Hiçbir zaman	Nadiren	Arada sırada	Çoğu zaman	Her zaman
Bir e-postayı birden fazla kişiye gönderirken alıcıların e-posta adreslerini gizlerim.	f	322	338	411	440	518
	%	15.90	16.70	20.30	21.70	25.50
İstemediğim e-postaları spam (istenmeyen e-posta) olarak işaretlerim.	f	198	227	464	510	630
	%	9.80	11.20	22.90	25.10	31.00
E-posta ile gelen bir eklentiye açmadan önce kaynağını kontrol edip, virüs taramasından geçiririm.	f	272	358	533	382	484
	%	13.40	17.60	26.30	18.80	23.90
Tanımadığım ve kaynağını bilmediğim kişilerden gelen e-postalara yanıt vermem.	f	204	287	422	432	684
	%	10.10	14.10	20.80	21.30	33.70
Tanımadığım ve kaynağını bilmediğim kişilerden gelen e-posta mesajı içerisindeki bağlantılara (linklere), dosyalara tıklamam, açmam.	f	158	336	420	496	619
	%	7.80	16.60	20.70	24.40	30.50
Bir e-postayı birden fazla kişiye gönderirken alıcıların e-posta adreslerini gizlerim.	f	322	338	411	440	518
	%	15.90	16.70	20.30	21.70	25.50

Tablo 4 incelendiğinde öğrencilerin %47.20'sinin çoklu e-posta gönderirken alıcıları adreslerini gizlediği, %56.10'unun istenmeyen postaları spam olarak işaretleyebildiği, %42.70'inin e-posta ekinde gelen dosyaları virüs taramasından geçirdiği, %55.00'inin tanımadığı kişilerden gelen e-postalara yanıt vermediğini ve %54.90'ının bu e-postalarda bulunan bağlantılara tıklamadıkları görülmektedir. Tablo 4 genel olarak değerlendirildiğinde öğrencilerin yaklaşık yarısının e-posta güvenliği konusundaki bilgi ve farkındalıklarının yüksek olarak değerlendirilebilir. Diğer öğrencilerin ise bu konulardaki yeterlilik ve farkındalıkları açısından risk altında olduğu anlaşılmaktadır.

Beşinci alt tema olan internet ve ağ güvenliği konusunda öğrencilerin farkındalıklarını belirlemeye yönelik olarak toplanmış olan verilere Tablo 5'de yer verilmiştir.

**Tablo 5.**  
*Öğrencilerin İnternet ve Ağ Güvenliği Hakkındaki Farkındalıkları.*

Farkındalıklar		Hiçbir zaman	Nadiren	Arada sırada	Çoğu zaman	Her zaman
Modem şifremi düzenli olarak değiştiririm.	f	254	437	492	441	405
	%	12.50	21.50	24.20	21.70	20.00
Modemimin şifresini arkadaşlarımla/komşularımla paylaşıyor ya da onların benimle paylaştıkları şifreleri kullanırım.	f	287	400	454	548	340
	%	14.10	19.70	22.40	27.00	16.80
Bilgisayarım ya da diğer elektronik cihazlarımla yalnızca bildiğim ve güvendiğim kablosuz internet bağlantılarına bağlanırım.	f	156	319	484	529	541
	%	7.70	15.70	23.90	26.10	26.70
İnternette güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini alırım.	f	237	269	492	509	522
	%	11.70	13.30	24.20	25.10	25.70
İnternet sayfalarında gezinti yaparken çıkan mesajları okumadan “evet” veya “tamam” gibi seçeneklere tıklarım.	f	254	380	492	467	436
	%	12.50	18.70	24.20	23.00	21.50
https ve  simgesi olan siteleri kullanmayı tercih ederim.	f	225	289	507	429	579
	%	11.10	14.20	25.00	21.10	28.50
İnternette indirdiğim ya da arkadaşımından aldığım video, müzik, film gibi dosya veya programları virüs taraması yaparak kullanırım.	f	219	428	434	518	430
	%	10.80	21.10	21.40	25.50	21.20
İnternette ya da ağ üzerinden dosya paylaşımında bulunduğumda, paylaşılan dosyaları açmadan önce virüs taraması yaptırım.	f	240	409	477	464	439
	%	11.80	20.20	23.50	22.90	21.60

Tablo 5 incelendiğinde öğrencilerin %41.70'inin modem şifresini düzenli olarak değiştirdiği, %33.80'inin bu şifreyi başkalarıyla paylaşmadığı ve %52.80'inin yalnızca bildiği kablosuz internet bağlantılarına bağlandığı görülmüştür. Tablo 5'teki bulgulara göre öğrencilerin %50.80'inin internet alışverişlerinde güvenlik tedbirleri aldığı, %31.20'sinin gezinti esnasında karşısına gelen alakasız mesajlara tıklamadığı, %28.50'inin https özelliğindeki web sitelerini kullanmayı tercih ettiği, %49.60'ı internette indirdikleri film/müzik/video gibi dosya ve programları virüs taramasından geçirdiği ve %44.50'inin dosya paylaşımı aracılığıyla aldığı dosyaları virüs taramasından geçirdiği görülmüştür.

Tablo 5 genel olarak değerlendirildiğinde internet ve ağ güvenliği konusundaki bilgi ve farkındalığı yüksek olarak değerlendirilebilecek öğrenci sayısının yarının altında kaldığı söylenebilir. Bir diğer ifade ile öğrencilerin büyük çoğunluğunun bu konudaki yeterlilik ve farkındalıkları açısından risk altında olduğu anlaşılmaktadır.

Altıncı alt temada kullanıcı farkındalıkları konusunda öğrencilerin farkındalıklarını belirlemeye yönelik olarak toplanmış olan verilere Tablo 6'da yer verilmiştir.

Tablo 6 incelendiğinde öğrencilerin %57.50'inin birey olarak üzerine düşen sorumlulukların farkında olduğu, %53.60'ının güvenli bilgisayar ve internet kullanımıyla ilgili sorun yaşadıklarında nereye ve nasıl başvuracaklarını bildikleri, %48.70'inin siber suçları ve bu suçların kapsamını bildiği, %44.60'ının güvenli bilgisayar ve internet kullanımıyla ilgili bilgilendirici politika ve uygulamaları takip ettiği anlaşılmaktadır. Ayrıca, öğrencilerin güvenli bilgisayar ve internet kullanımıyla ilgili yaşadıkları sorunlarda bu durumu çoğunlukla; %44.30'unun ailesiyle, %41.70'i öğretmenleriyle, %48.70'i ise arkadaşlarıyla paylaştıklarını belirtmektedir. Yine, %41.60'ının kullandıkları cihazların aileleri tarafından kontrol edildiği, %47'sinin de aileleri tarafından bilgilendirildiği görülmektedir. Tablo 6 genel olarak değerlendirildiğinde büyük çoğunluğunun kullanıcı farkındalığının düşük olduğu değerlendirilebilir.

**Tablo 6.**  
*Öğrencilerin Kullanıcı Farkındalıkları ve Sosyal Mühendislik Hakkındaki Farkındalıkları.*

Farkındalıklar		Hiçbir zaman	Nadiren	Arada sırada	Çoğu zaman	Her zaman
Güvenli bilgisayar ve internet kullanımının ne anlama geldiğinin farkındayım.	f	149	311	524	479	566
	%	7.30	15.30	25.80	23.60	27.90
Güvenli bilgisayar ve internet kullanımının sağlanması konusunda birey olarak üzerime düşen sorumlulukların farkındayım.	f	155	233	474	596	571
	%	7.60	11.50	23.40	29.40	28.10
Güvenli bilgisayar ve internet kullanımımı tehdit eden bir olay ile karşılaştığımda kimlere ve nereye başvurmam gerektiğinin farkındayım.	f	130	329	483	545	542
	%	6.40	16.20	23.80	26.90	26.70
Siber suçların tam olarak neler olduğunun ve neleri kapsadığının farkındayım.	f	216	352	473	473	515
	%	10.60	17.30	23.30	23.30	25.40
İnternette müzik, program gibi telif hakkı içeren dosyaları paylaşmamam gerektiğinin farkındayım.	f	138	326	406	549	610
	%	6.80	16.10	20.00	27.10	30.10
İnternette müzik, program gibi telif hakkı içeren dosyaları indirmemem gerektiğinin farkındayım.	f	152	337	515	413	612
	%	7.50	16.60	25.40	20.40	30.20
Güvenli bilgisayar ve internet kullanımının sağlanması konusundaki Milli Eğitim Bakanlığının ve devletin politikalarını/uygulamalarını takip ederim.	f	279	376	468	431	475
	%	13.80	18.50	23.10	21.20	23.40
İnternette karşılaştığım güvenli bilgisayar ve internet kullanımı ile ilgili olumsuz durumları aileme anlatırım.	f	200	419	511	426	473
	%	9.90	20.70	25.20	21.00	23.30
İnternette karşılaştığım güvenli bilgisayar ve internet kullanımı ile ilgili olumsuz durumları öğretmenlerime anlatırım.	f	326	407	451	446	399
	%	16.10	20.10	22.20	22.00	19.70
İnternette karşılaştığım güvenli bilgisayar ve internet kullanımı ile ilgili olumsuz durumları arkadaşlarıma anlatırım.	f	179	384	478	442	546
	%	8.80	18.90	23.60	21.80	26.90
Ailem bilgisayarım ve telefon gibi diğer elektronik cihazlarımı kontrol eder.	f	289	382	515	405	438
	%	14.20	18.80	25.40	20.00	21.60
Ailem bilgisayar ve diğer elektronik cihazları kullanırken güvenli bilgisayar ve internet kullanımı konusunda beni bilgilendirir.	f	252	408	415	514	440
	%	12.40	20.10	20.50	25.30	21.70

### Tartışma, Sonuç ve Öneriler

Araştırma bulguları temalar bazında genel olarak değerlendirildiğinde erişim ve şifre güvenliği, sosyal ağ güvenliği, tehditler, korunma yolları, yazılım yükleme ve güncelleme, e-posta güvenliği, internet ve ağ güvenliği, kullanıcı farkındalıkları ve sosyal mühendislik temalarının tamamında verilerin “hiçbir zaman”, “nadiren”, “arada sırada”, “çoğu zaman”, “her zaman” gözeneklerine yaklaşık olarak eşit oranlı bir şekilde dağıldığı görülmektedir. Bu durum güvenli bilgisayar ve internet kullanımı farkındalığı yüksek olarak niteleyebileceğimiz öğrenci sayısının genel olarak az olduğunu göstermektedir. Araştırma bulgularını destekler nitelikte Kaşıkçı et al. (2014) tarafından gerçekleştirilen araştırmada da Türkiye’deki çocukların %83.40’ı “İnternet hakkında çok şey bilirim” demekle birlikte, çocukların aslında internet okuryazarlığı ile ilgili farkındalıklarının az olduğu ifade edilmiştir. Kaşıkçı et al. (2014) tarafından gerçekleştirilen araştırma sonucuyla kıyaslandığında günümüz öğrencilerinin günlük internet kullanım ortalamalarının yükseldiği anlaşılmaktadır. Ayrıca Kaşıkçı et al. (2014) tarafından gerçekleştirilen araştırma kapsamında internet erişimi için kendi bilgisayarını kullanan öğrencilerin oranının Türkiye’de %40.20 olduğu tespit edilmiş ve bu orana rağmen ebeveynler çocuklarının internet kullanımlarını



denetleyebilmede güçlük yaşadıklarını ifade etmişlerdir. Avrupa çevrimiçi çocuklar araştırma projesi sonuçlarına göre, ebeveynlerin %70.00'i internette yaptıklarıyla alakalı olarak çocuklarıyla konuşmakta ve %58'i ise interneti kullanırken onların yakınında bulunmaktadır (Kaşıkçı et al., 2014). Bu araştırmanın örneklemini oluşturan öğrencilerin %95.00'inin kişisel bilgisayar ya da mobil cihaza sahip oldukları göz önüne alındığında ise ebeveynlerin denetiminin daha da güçleşebileceği sonucuna varılabilir. Çünkü özellikle taşınabilir bilgisayar ya da mobil cihaza sahip olan öğrenciler evin herhangi bir yerinden ya da ev dışı ortamlarda da internete bağlanabileceklerdir. Söz konusu bu durumun getirmiş olduğu risklerin bir diğer önemli boyutu ise araştırmadan elde edilen bulgulara göre, öğrencilerin büyük çoğunluğunun güvenli bilgisayar ve internet kullanımı ile ilgili yaşadıkları olayları ebeveynleri ile paylaşmadıklarıdır. Bu durumda öğrencilerin bilgisayar ve internet kullanımları ile ilgili ebeveyn farkındalık durumlarının çok az düştüğü söylenebilir.

Ebeveynler doğal olarak çocuklarının sanal dünyayı nasıl kullandıkları ve sanal dünyada nasıl hareket ettikleri konusunda endişeye sahiptirler. Neyin güvenli ve uygun olduğunu çocukları ile birlikte karar vermelerini sağlamak için ise yeterli bilgiye sahip olmaları gereklidir (ENISA, 2011). Fakat bilgi güvenliği konusunda yeterli farkındalığa sahip olmayan aileler hem kendilerine hem de çocuklarına yardım etmek konusunda oldukça yetersiz kalacaktır. Bu sorunun çözülmesinde ise politika yapıcılardan okullara kadar birçok kuruma görev düşmektedir. Politika yapıcılar, ebeveynlere bilgi güvenliği konusunda farkındalık yaratacak olan ortamları ve yeni politikaları sunmalıdırlar. Yeni ortamlar ise politika yapıcılar ve okulların işbirliği içinde eğitimler aracılığıyla yürütebilirler. Farkındalık eğitiminde amaç, güvenlik konusuna basitçe dikkat çekmektir (Wilson & Hash, 2003). Farkındalık yaratmak uzun soluklu ve çok zaman alıcı bir iş olmadığı için öğrenciler, ebeveynler ve tüm ortak paydada yer alan kişiler rahatlıkla bu konuda eğitilebilirler. Bu verilere ek olarak, öğrencilerin günlük internet kullanımları da büyük oranda öğrencilerin bilgi güvenlik farkındalıklarını etkilediği görülmektedir. Avrupa çevrimiçi çocuklar projesinde de benzer şekilde Türkiye'de çocukların yaklaşık %25.00'ini İnternet'in aşırı kullanımından kaynaklı olarak çevrim içi risklere maruz kaldıkları, bu oranın Avrupa çapında %33.00 olduğu belirtilmiştir (EU Kids Online, 2011).Türkiye İstatistik Kurumu 2015 verilerine göre Türkiye genelinde İnternet erişim imkânına sahip hanelerin oranı 2015 yılı Nisan ayında %69.50'dir ve 16-74 yaş grubu bireylerin %87.10'u interneti evde kullanmaktadır. Günlük internet kullanımı eğer bilgi güvenliği farkındalığını etkiliyor ise ev içinde ebeveynlerin öğrencileri internet kullanım sürecinde kontrol altında tutmaları gereklidir. Bu konuda ise alınabilecek önlemlerden bazılarını aşağıda yer verilmiştir (ENISA,2011):

- Çocukların bilgisayarlarına filtreleme ya da ebeveyn kontrolü sağlayacak programlar kurmak.
- Sanal dünyadaki şifrelerini arkadaşları ile paylaşmama konusunda çocukları eğitmek.
- Genç kullanıcıların sanal dünya aktivitelerinin içinde yer almak.
- Çocukları genel olarak teknoloji kullanımı sorumlulukları konusunda eğitmek.

Fakat bu önlemlerin hayata geçirilebilmesi için ebeveynlerin bilgi güvenliği konusunda farkındalığa ve yeterli bilgiye sahip olmaları gereklidir.

Araştırma kapsamında, öğrencilerin sosyal ağ farkındalığı teması altında verdikleri cevaplara bakıldığında; kişisel bilgileri paylaşmama, istenmeyen kişilerden gelen mesajları ve uygulamaları engelleyebilme, profilinin/sayfalarının güvenlik ayarlarını değiştirebilme gibi işlemleri yapan/yapabilen öğrenci sayısının ortalamanın üstünde olduğu ve diğer temalara göre bilgi ve farkındalıklarının bu temada daha yüksek olduğu görülmektedir. Avrupa çevrimiçi çocuklar projesinde, 9-16 yaş aralığında yer alan çocukların %59.00'unun herhangi bir sosyal paylaşım sitesinde profile sahip oldukları ve sosyal paylaşım sitesini kullanan çocukların %26.00'sinin herkese açık profile sahip oldukları belirlenmiştir (EU Kids Online, 2011). Ayrıca, sosyal ağlarda güvenliğin sağlanması üzerine yapılan bazı araştırmalarda da gençlerin sosyal ağ kullanma konusunda yeterli güvenlik bilgisine sahip olmadıkları sonucuna ulaşılmıştır (Kaşıkçı et al., 2014; Lawler & Molluzzo, 2010). Aradaki bu farkın nedeni ise öğrencilerin büyük çoğunluğunun sosyal ağları kullanıyor olması ve bu kullanım deneyiminin getirmiş olduğu bilgi ve farkındalıktaki artışa bağlı olabilir.

Çocuk ve gençlerin, bilgisayar ve internet kullanımı esnasında karşılaştıkları teknik sorunlar arasında; çocukların bilgisayara virüs bulaştırması, casus yazılımların girmesine müsaade etmesi, bilgisayarı bozması, bunun sonucu olarak var olan belge ve dosyaların kaybedilmesi ve bazı yazılım ayarlarının bozulması gösterilmektedir (Canbek & Sağıroğlu, 2007). Araştırmada da, öğrenciler tehditler ve korunma yolları güvenliği teması altında verdiği cevaplarda; zararlı yazılım ve virüslerin verebileceği zararların, zararlı programlardan koruma yazılımlarının farkında olma, bu programları kullanma, zararlı yazılımların bilgisayara bulaşıp bulaşmadığı fark edebilme ile ilgili farkındalığı yüksek olan öğrenci sayısının yüksek olduğu görülmektedir. Yıldırım ve Varol (2013) tarafından yapılan araştırmada ise birçok kullanıcının antivirüs programı kullanmadıkları belirlenmiştir. Benzer şekilde, Tekerek ve Tekerek'in (2013) araştırmasında da, kötücül yazılım denetlemesi yapma, belge koruma, kişisel bilgisayar güvenliği, güvenlik duvarı ve filtreleme yazılımları kullanımı gibi konularda öğrencilerin farkındalıklarının düşük olduğu görülmüştür. Ayrıca öğrenciler, güvenli bilgisayar ve internet kullanımı konusunda yeterli bilgiye sahip olmadıklarını belirtmişlerdir. Öte yandan, istenmeyen iletileri önleme ve antivirüs programı kullanma oranı Avrupa'da %72.00 iken, Türkiye'de bu oran %46.00 olarak bulunmuştur (Kaşıkçı et al., 2014). Bu araştırma sonucuna göre ise öğrencilerin antivirüs programı kullanım oranlarının yükseldiği görülmektedir. Bu yükselişin nedenleri arasında öğrencilerin bireysel olarak bilgisayar ve mobil cihazlara sahip olup kullanmaları sonucu bu cihazları daha da benimsemeleri ve buradaki kişisel bilgilerini koruma niyetleri görülebilir. Bir başka ifade ile öğrenciler ebeveynleri vb. ile ortak kullanılan BİT araçlarında daha az kişisel bilgi bulundurabileceğinden dolayı buradaki verilerin korunmasını çok fazla önemsemiyor; buna rağmen bireysel BİT araçlarındaki verilerin korunmasını ise daha fazla önemsiyor olabilirler.

E-posta, anlık mesajlaşma gibi iletişim platformları çocukların su istimal edilmesine açık ortamlardır (Bilgin, 2007; akt. Çelen, Çelik, & Seferoğlu, 2011). Gençlerin sahip olduğu bireysel bilgisayar ve internet erişim olanaklarının artması ile okul içinde ve dışında öğrencilerin sık sık çevrimiçi ortamlardan etkileşime girmesiyle bu süreçler içinde çeşitli istismarlarla karşılaşma olasılıkları yüksektir. Bu nedenlerden dolayı da öğrencilerin bu konuda yeterli farkındalığa sahip olmaları önem teşkil etmektedir. Araştırmada, öğrencilerin e-posta güvenliği farkındalıklarını belirlemeye yönelik olarak sorulan sorulara göre öğrencilerin yaklaşık yarısı; toplu e-postalarda alıcı isimlerini gizlediklerini, istemeyen e-postaları spam olarak işaretlediklerini, ekli dosyaları açmadan önce virüs taramasından geçirdiklerini, tanınmadığı kişilerden gelen e-postalar içerisindeki linkleri açmadıklarını söylemişlerdir. Dördüncü alt tema olan şifre güvenliğine yönelik olarak öğrencilerin büyük bir kısmı; şifrelerini unutmamak için not defterine kayıt ettiğini, bazı ortamlarda aynı şifreyi kullandıklarını, güvenilir ve elde edilmesi zor olan şifreler oluşturmadıkları ve hesabı çalındığında nasıl geri alabileceğini bilmediklerini dile getirmektedir. Genel olarak değerlendirildiğinde öğrencilerin e-posta kullanma farkındalıklarının, güvenli şifre oluşturma konusundaki farkındalıklarına göre daha yüksek olduğu söylenebilir. Ancak güvenli şifre oluşturma güvenli e-posta kullanımının ön koşulu olarak değerlendirildiğinde öğrencilerin bu açıdan da risk altında olduğu görülmektedir. Tekerek ve Tekerek (2013) tarafından ilköğretim ve lise düzeyinde öğrenim gören öğrenciler üzerinde yapılan araştırmada ise güvenli şifre kullanımı farkındalıklarının düşük olduğu; Mert, Bülbül ve Sağıroğlu (2012) tarafından sekizinci sınıf öğrencileri ile gerçekleştirdikleri araştırmada da öğrencilerin %30.00'unun şifrelerinde sadece küçük harf, %17.00'sinin sadece sayı, %17.00'sinin sadece büyük harf ile sayı veya sadece küçük harf ile sayı ve büyük harf, küçük harf, sayı, özel karakter kullananların oranının ise %1.00 olduğu belirlenmiştir. Kruger, Drevin ve Steyn (2010) tarafından gerçekleştirilen bir çalışmada ise katılımcıların yarısının güçlü şifrenin ne demek olduğunu bilmedikleri ortaya koyulmuştur. E-posta ve şifre güvenliği açısından öğrencilerin farkındalık durumlarının bu araştırma sonuçlarına benzer seviyede olduğu söylenebilir.

Genel olarak değerlendirildiğinde ise öğrencilerin büyük çoğunluğunun sosyal ağ güvenliği ile tehditler ve korunma yolları temasına yönelik bilgi ve farkındalıklarının yüksek olduğu görülmüştür. Öğrencilerin yaklaşık yarısının erişim ve şifre güvenliği ile e-posta güvenliği temalarına yönelik bilgi ve farkındalıkları diğer temalara oranla nispeten biraz daha yüksek olarak nitelenebileceği ancak öğrencilerin büyük çoğunluğunun; tehditler, korunma yolları, yazılım yükleme ve güncelleme, internet ve ağ güvenliği, kullanıcı farkındalığı ve sosyal mühendislik temalarına yönelik farkındalıklarının ise düşük olduğu söylenebilir. Genel olarak temaların değerlendirilmesi sürecinde "hiçbir zaman" ile "nadiren";

“çoğu zaman” ile “her zaman” gözenekleri birlikte yorumlanarak değerlendirilmiştir. Ancak güvenli bilgisayar ve internet kullanımı gibi hassas bir konuda olması gerekenin en ideali olduğu, bir diğer ifade ile gözeneklerin en uç noktaları değerlendirilmeye alındığında ise bu oranın yarı yarıya düşebileceği göz önüne alınmalıdır. Özetle, ucuzlayan bilgisayar ve internet teknolojileri ile birlikte günümüz gençliğinin bireysel teknoloji erişim imkânlarına sahip olduğu ancak öğrencilerin altı tema altındaki güvenli bilgisayar ve internet kullanımı konularındaki farkındalık düzeylerinin genel olarak düşük kaldığı söylenebilir.

Her ne kadar okullarda güvenli bilgisayar ve internet kullanımını sağlamak adına internet filtreleme programları ve bilişim teknolojileri derslerinde güvenli bilgisayar ve internet kullanımı ile ilgili kazanımlar olsa da bunun bilgi ve farkındalığın oluşmasında yetersiz kaldığı görülmektedir. Ayrıca, okullarda bilişim derslerinin müfredatının değişmesiyle beraber güvenli BİT kullanım eğitimlerine ağırlık verileceği belirtilmesine rağmen bunun da etkin uygulanamadığı anlaşılmaktadır. Gelecek araştırmalarda okul internet filtreleme programlarının kullanımları ile ilgili öğrenci, öğretmen ve yönetici görüşleri incelenebilir. Okullarda Bilişim Teknolojisi derslerinde verilmekte olan güvenli bilgisayar ve internet kullanımı eğitimlerine yönelik müfredat çalışmaları yapılabilir. Yapılan araştırmalarda Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümlerinde okuyan öğretmen adaylarının kendilerini güvenli bilgisayar ve internet kullanımını sağlama konusunda yeterli bilgi ve beceriye sahip oldukları ifade edilmekle birlikte (Kurtoğlu Erden, 2014); öğretmen adayları arasında e-demokrasi kültürünün geliştirilmesi ve çevrimiçi politik uygulamalara katılım düzeyinin artırılması için diğer bölümlerdeki öğretmen adaylarına da hizmet öncesi eğitim sürecinde internet erişimi, BİT okuryazarlık durumu, teknik altyapı, vatandaş grupları ile ilgili etik ve yasal konular, gizlilik ve güvenlik konularındaki farkındalıklarının artırılması önerilmektedir (Yıldız & Seferoğlu, 2014).

Kaya ve Tuna'ya (2010) göre eğitim durumu ne olursa olsun çocuklarına yeterince zaman ayırmayan, BİT'in güvenli kullanımı konusunda çocuklarını bilinçli şekilde yönlendiremeyen ve bu konularda yeterli bilgiye sahip olmayan ebeveynlerin çocuklarının, bu teknolojilerle daha fazla vakit geçirerek istenmeyen davranış biçimlerini bilinçsizce geliştirmeleri olasıdır. Bu nedenle bu konuda kamuyu bilinçlendirmeye yönelik eğitimlerin de verilmesi önemlidir. TÜBİTAK BİLGEM tarafından hazırlanmış Bilgimi Koruyorum E-Öğrenme Projesi kapsamında hazırlanan web ortamı güvenli bilgisayar ve internet kullanımı farkındalığı oluşturmak adına hazırlanmış iyi örneklerden birisi olup, bunun yaygın etkisinin oluşturulması adına Bilişim Teknolojileri derslerinde ve halk eğitim merkezi gibi kurslarda bu kaynaklara olan farkındalık artırılabilir. Yine öğretmen, okul idaresi, ebeveyn ve öğrencilere yönelik konuyla ilgili çeşitli kamu spotları oluşturularak farkındalıkları artırılabilir. Okullarda ebeveynlerle toplantılar yapılarak güvenli bilgisayar ve internet kullanımı konusunda ebeveynlere düşen sorumluluklar konusunda veliler aydınlatılabilir.

### **Sınırlılıklar ve Gelecek Araştırmalar İçin Öneriler**

Betimsel tarama yöntemine göre yürütülen bu araştırmanın bir takım sınırlılıkları bulunmaktadır. Öncelikle araştırmanın verileri araştırmacılar tarafından geliştirilen bir anket aracılığıyla elde edilmiştir. Gelecek çalışmalarda nicel yöntemlerin yanı sıra nitel yöntemler kullanılarak da daha derinlemesine araştırmaların yapılması yararlı olacaktır. Ayrıca anket maddeleri öğrencilerin güvenli bilgisayar ve internet kullanımı ile ilgili sık gösterilen davranış durumları dikkate alınarak hazırlanmıştır. Ancak konunun kapsamlı bir konu olduğu dikkate alındığında belirtilen temalar dışında yeni temalar altında ve daha kapsamlı maddeler içerecek şekilde ölçme araçları ile kullanıcı farkındalıkları ölçülebilir. Araştırmanın bir diğer sınırlılığı ise örneklemin Bartın ili merkezindeki liselerde öğrenim görmekte olan ve çoğunlukla 15-18 yaş aralığındaki öğrencilerle sınırlı olmasıdır. Bir diğer ifade ile araştırma sonuçlarının yalnızca lise öğrencilerinin güvenli bilgisayar ve internet kullanım farkındalıklarını temsil etme yeterliliğine sahip olduğu söylenebilir. Gelecek araştırmalarda farklı yaş ve öğrenim gruplarındaki öğrenciler üzerinde ve sosyo-ekonomik olarak daha farklı bölgelerde de çalışmalar gerçekleştirilmesi yararlı olacaktır. Öğrencilerden farklı olarak eğitim yöneticileri, öğretmenler, ebeveynler ve bu konuda çalışan politika

geliştiriciler üzerinde de çalışmalar gerçekleştirilebilir. Güvenli bilgisayar ve internet kullanım farkındalığının kültürel bir olgu olduğu ve bu kültürün oluşmasında ailenin önemli bir rolünün göz önüne alındığında bu konuda ebeveynler üzerinde derinlemesine çalışmalar yapmakta yarar vardır.

#### **Teşekkür ve Bilgilendirme**

Bu çalışma Bartın Üniversitesi Bilimsel Araştırmalar Proje Birimi tarafından desteklenmiştir (Proje No: 2014-SOS-A-004).

## References

- Alhejaili, H. (2013). *Usefulness of teaching security awareness for middle school students*. Unpublished master's thesis, Rochester Institute of Technology.
- Al-Jerbie, S.I., & Jali, M.Z. (2014). A second look at the information security awareness among secondary school students. In *The International Conference on Information Security and Cyber Forensics (InfoSec2014)* (pg. 88-97). The Society of Digital Information and Wireless Communication.
- Arachchilage, N.A.G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304-312.
- Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48, 51-61.
- Berrier, T. (2007). *Sixth-, seventh-, and eighth-grade students' experiences with the internet and their internet safety knowledge*. Unpublished doctorate dissertation, East Tennessee State University.
- Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, 9(3), 165-174.
- Chen, Y. (2014). *Protect children online safety on social media and mobile platforms*. Unpublished doctorate dissertation, The Pennsylvania State University.
- Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719 - 731.
- Chou, C., & Peng, H. (2011). Promoting awareness of internet safety in Taiwan in-service teacher education: A ten-year experience. *The Internet and Higher Education*, 14(1), 44-53.
- Cole, A. (2014). *The digital world: are our children ready*. Unpublished master's thesis, Utica College.
- Çakır, H., Hava, K., Gülen, Ş. B., & Özudoğru, G. (2015). Öğretmen adaylarının sosyal ağ sitelerinde güvenlik farkındalıklarının incelenmesi. *International Journal of Human Sciences*, 12(1), 887-902.
- Çelen, K. F., Çelik, A., & Seferoğlu, S. S. (2011). Çocukların internet kullanımları ve onları bekleyen çevrim-içi riskler. *Akademik Bilişim'11 - XIII. Akademik Bilişim Konferansı Bildirileri*, 2-4 Şubat 2011 İnönü Üniversitesi, Malatya.
- Daniel, J. (2012). *Sampling essentials: Practical guidelines for making sampling choices*. Thousand Oaks, CA: SAGE Publications.
- Deisman, W. W. (2008). *Securing cyberspace: neo-liberalism, risk and child safety*. Unpublished doctorate dissertation, Carleton University.
- Demirel, M., Yörük, M., & Özkan, O. (2013). Çocuklar için güvenli internet: Güvenli internet hizmeti ve ebeveyn görüşleri üzerine bir araştırma. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 4(7), 54-68.
- EuKidsOnline METU. (2011). *EU Kids Online Projesi, Türkiye araştırma grubu, ODTÜ*. Retrieved 29 June, 2015, from <http://eukidsonline.metu.edu.tr>
- European Network and Information Security Agency (ENISA) (2011). *Network Information Security in Education*. Retrieved 10 February, 2016, from <https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/nis-brokerage-1/NetworkInformationSecurityinEducation.pdf>
- Field, A. (2005). *Discovering statistics using SPSS*. London: Sage Publications.
- Gökmen, Ö. F., & Akgün, Ö. E. (2015). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği bilgilerinin çeşitli değişkenlere göre incelenmesi. *Çukurova Üniversitesi Eğitim Fakültesi Dergisi*, 44(1), 61-84.
- Gökmen, Ö. F., & Akgün, Ö. E. (2016). Öğretmen adaylarının bilişim suçlarına yönelik deneyimleri ve bilişim güvenliği ders içeriğine yönelik görüşleri. *Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 13(33), 178-193.

- Güldüren, C., & Keser, H. (2015). Bilgi güvenliği farkındalık ölçeği geliştirme çalışması. *Kastamonu Eğitim Dergisi*, 23(3), 1167-1184.
- Harris, M. (2010). *The shaping of managers' security objectives through information security awareness training*. Unpublished doctorate dissertation, Virginia Commonwealth University.
- Harshman, K. L. (2014). *Assessing effectiveness of age-appropriate curriculum on internet safety education and cyberbullying prevention*. Unpublished doctorate dissertation, Grand Canyon University.
- Karaođlan Yılmaz, F. G., Yılmaz, R., & Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışları ve bilgi güvenliği eğitimine genel bir bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi*, 3(1), 176-199.
- Kaşıkcı, D. N., Çağıltay, K., Karakuş, T., Kurşun, E., & Ogan, C. (2014). Türkiye ve avrupa'daki çocukların internet alışkanlıkları ve güvenli internet kullanımı. *Eğitim ve Bilim*, 39(171), 230-243.
- Kaya, K., & Tuna, M. (2010). Popüler kültürün ilköğretim çağındaki çocukların aile içi ilişkileri üzerindeki etkisi. *SDÜ Fen Edebiyat Fakültesi Sosyal Bilimler Dergisi*, 21, 237-256.
- Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, 18(5), 316-327.
- Kurtođlu Erden, M. (2014). *Bilgisayar ve öğretim teknolojileri eğitimi bölümü lisans programının mezun yeterlik algılarına göre değerlendirilmesi*. Unpublished doctorate dissertation, Hacettepe University.
- Küçükali, M., & Bülbül, H. İ. (2015). Fatih projesi kapsamında internetin bilinçli ve güvenli kullanımının artırılması. *TÜBAV Bilim Dergisi*, 8(2), 1-17.
- Kritzinger, E., & Smith, E. (2008). Information security management: an information security retrieval and awareness model for industry. *Computers & Security*, 27(5-6), 224 -231.
- Lawler, J. P., & Molluzzo, J. C. (2010). A study of the perceptions of students on privacy and security on social networking sites (SNS) on the internet. *Journal of Information Systems Applied Research*, 3(12), 3-18.
- Leach, J. (2003). Improving user security behaviour. *Computers & Security*, 22(8), 685-692.
- Mert, M., Bülbül, H. İ., & Sağırođlu, Ş. (2012). Milli eğitim bakanlığına bađlı okullarda güvenli internet kullanımı. *Türk Bilim Araştırma Vakfı Bilim Dergisi*, 5(4), 1-12.
- Murray, D. L. (2014). *A survey of the practices and perceptions of students in one catholic high school on the use of the internet regarding safety, cyberbullying, and sexting*. Unpublished doctorate dissertation, The University of San Francisco.
- Ngoqo, B., & Flowerday, S. V. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *Computers & Security*, 53, 132-142.
- Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28(8), 816-826.
- Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, 48, 199-207.
- Tamjidyamcholo, A., Baba, M. S. B., Shuib, N. L. M., & Rohani, V. A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. *Computers & Security*, 43, 19-34.
- Tekerek, M., & Tekerek, A. (2013). A research on students' information security awareness. *Turkish Journal of Education*, 2(3), DOI: 10.19128/turje.181065
- Tsim, S.J. (2006). *Internet safety education: information retention among middle school aged children*. Master thesis, San Jose State University.

- TÜBİTAK-BİLGEM. (2011). *Bilgimi koruyorum e-öğrenme projesi*. Retrieved 29 June, 2015, from <http://www.bilgimikoruyorum.org.tr>
- Valcke, M., Schellens, T., Van Keer, H., & Gerarts, M. (2007). Primary school children's safe and unsafe use of the internet at home and at school: An exploratory study. *Computers in Human Behavior, 23*(6), 2838-2850.
- Van Bruggen, D.C. (2014). *Studying the impact of security awareness efforts on user behavior*. Unpublished doctorate dissertation, University of Notre Dame.
- Vicks, M. E. (2013). *An examination of internet filtering and safety policy trends and issues in south carolina's k-12 public schools*. Unpublished doctorate dissertation, Nova Southeastern University.
- Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special Publication, 800*(50), 1-39.
- Wishart, J. (2004). Internet safety in emerging educational contexts. *Computers & Education, 43*(1), 193-204.
- Yan, Z. (2009). Differences in high school and college students' basic knowledge and perceived education of Internet safety: Do high school students really benefit from the children's internet protection act? *Journal of Applied Developmental Psychology, 30*(3), 209-217.
- Yenilmez, Y., & Seferoğlu, S. S. (2013). Sanal zorbalık ve öğretmenlerin farkındalık durumlarına bir bakış. *Eğitim ve Bilim, 38*(169), 420-432.
- Yıldırım, N., & Varol, A. (2013). Sosyal ağlarda güvenlik: Bitlis Eren ve Fırat Üniversitelerinde gerçekleştirilen bir alan çalışması. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 7*(7), 285-292.
- Yıldız, H., & Seferoğlu, S. S. (2014). Sayısal uçurum ve demokrasi bilincine bakış: İlköğretim öğrencilerinin görüşleri. *Eğitim ve Bilim, 39*(171), 86-98.

