Secure Internet Use in Information Technologies and Software Course Textbooks at Primary and Secondary Schools

By Abdullatif Kaban[*]

Do we care about the security on the internet environment the way we do in the daily life safety of our children? In order to answer this question, this study aims to reveal what kind of education is provided at school about using secure internet. In accordance with this purpose, Information Technologies and Software Course textbooks at primary and secondary schools are examined applying document analysis method and analyzed by content analysis method. According to the findings, in the textbooks, the most frequently mentioned topics related to the use of secure internet are "protection of personal data", "security measures that can be taken" and "digital footprint"; and the most frequently mentioned topics related to the ethic are "internet ethics" and "respect for others". In this study on the use of secure internet, suggestions have been made about the precautions to be taken. The results are expected to provide information and resources to the researchers who work on secure internet use, educational institutions and teachers.

Keywords: Curriculum, Information technologies and software, Secure internet use, Primary school, Secondary school.

Introduction

Whether something is beneficial or harmful depends on how it is used. Any technology that is quite useful when used for good purposes, can become a very dangerous weapon when it gets into the hands of malicious people. Undoubtedly, the internet is a technology that facilitates our daily life especially for adults such as fast access to information, finding jobs, socializing and shopping (Colley & Maltby, 2008), but also it can be a threat for people of all ages such as theft of personal information, fraud and cyber bullying (Bilgin-Ülken & Kılınç, 2018). Unfortunately, today, the world of crime benefits from the blessings of the internet technology a lot more than the others. It is possible to see this in the news that we constantly encounter, such as phone scams, online games that lead children to suicide etc. According to the March 2019 data provided by the Turkish Statistical Institute, in Turkey, the number of mobile phone subscribers is nearly 81 million, and the number of internet subscribers is nearly 75 million (TÜİK, 2019). In order to reach the internet, children no longer have to hang out in internet cafes or chase their free time in the computer labs of schools, because of the accessibility of the internet in almost every pocket. Despite the various advantages it provides for education (e.g. computer-assisted learning, blended learning or ubiquitous

---
[*]Assistant Professor, Bayburt University, Turkey.

learning), it also introduces many dangers in educational and social environments. The decrease in academic achievement of students who spend a lot of time in social media (Gök, 2015) can be considered a trivial problem when compared to the other damages caused by the internet use. It should never be ignored that when children are left unattended while using the internet, some very serious problems are inevitable such as (a) technical damages (e.g. virus infection), (b) physical, social and psychological damages (e.g. dependence and being asocial), and (c) vital damages (e.g. pedophilia and exposure to malicious persons or harmful content) (Canbek & Sağıroğlu, 2007). Adults can protect themselves better than children from the various risks of the internet (Orhan & Akkoyunlu, 2004). At this point, this study seeks answers for the question "what are the ways to protect children from these dangers?"

There are two opposing views on secure internet use; one is completely restrictive and the other is completely libertarian. The restrictive view argues that a central authority should completely shut down the access of objectionable parts in order to protect children from the dangers they may encounter on the internet. The opposite view suggests that children must be left completely free to learn to use the internet correctly (Akbulut, 2013). Secure internet filters served by internet service providers may somehow procure security, but this is not enough for today's children who can access the internet at every opportunity and in any environment (Demirel, Yörük, & Özkan, 2012). In a study on the secure internet use of secondary school students (Beder & Ergün, 2015), it was emphasized that children should be provided with training on secure internet use. In order to protect children from the damages of the internet, both legal restrictions should be imposed and children should be made conscious in this sense (Çelen, Çelik, & Seferoğlu, 2011). Besides children, raising awareness activities should also include teachers, school administrators and parents (Mert, Bülbül, & Sağıroğlu, 2012). It is also known that the education level of parents positively affects the level of control on children's internet usage (Valcke, Bonte, De Wever, & Rots, 2010).

Aslan and Karakuş-Yılmaz (2017), listed activities aimed at raising awareness about safe internet use in Turkey as awareness seminars, awareness and promotional campaigns, printed and electronic publications, hotline, and technical and legal measures. Although a study conducted in 2014 (Kaşıkçı, Çağıltay, Karakuş, Kurşun, & Ogan, 2014) claimed that the parents don't have sufficient information to guide children about secure internet use, a later study by Tekin and Polat (2016) concluded that the parents are aware of the secure internet use. This shows that the measures taken by the government, school administrators and parents increase the level of awareness about the secure internet use. Especially when it is considered that primary school children have a more positive attitude towards programs that promote healthy attitudes than adolescent secondary school students (Hope, 2002), it would be a good choice to start awareness-raising activities at an early age.

It is possible to see many studies in the literature on the secure internet use. Yiğit and Seferoğlu (2019), found that the participants' cyber security behavior levels were sufficient in their study conducted at the university level. According to the study, cyber security behavior levels of the students of Department of

Computer and Instructional Technology Education and Department of Computer Programming were at a higher level than the others. When this finding is considered, it can be suggested that the topics related to secure internet use should be included in the curriculum of the other departments as well. In a study conducted at high school level (Aytaç & Erdem, 2019), students' awareness of secure computer and internet use was examined, and it was found that there was a strong negative relationship between the problems and threats faced by the students and their competencies. This means that the more we educate students on safe internet use, the more we can reduce the risks they may face. In their study on the opinions of students, teachers and parents about the risks that may be encountered on the internet, İlhan & Aydın (2019) emphasized that parents felt helpless due to the negative effects of the lifestyle the internet era created. So, there is a need to educate not only the children but also their parents on secure internet use. In a study conducted with the participation of the stakeholders of education (Moreno, Egan, Bare, Young, & Cox, 2013), the views revealed that the most appropriate age for the start of the secure internet use trainings was 7 and that the most responsible stakeholder on this was the parents.

It is possible to extend the list of studies mentioned here. However, when the studies were examined, it was seen that their main focus was to describe the current situation, and to put forward suggestions. The common proposal of all studies is that it is necessary to protect children from these harmful aspects of the internet in the best possible way. In Turkey, there are legal regulations within the scope of various articles of the Turkish Criminal Code No. 5237 and Law No. 5651 entitled Regulation of Publications on the internet and Suppression of Crimes Committed by means of Such Publication (Gökçearslan, 2016). A test on how effective they are can be the subject of a separate study. In addition to legal regulations, web filters used by the Information and Communication Authority since 2011 protect both children and families from many dangers. In this regard, both informative and awareness-raising efforts are being conducted at different levels by websites (Güvenli Çocuk, 2019; 2019; Güvenli Web, 2019; Güvenli İnternet, 2019) for children and families.

In the education part of providing children with internet security, the students are educated in primary and secondary schools on the use of secure internet with various learning outcomes included in the curriculum. The weekly timetable for primary school determined by the Board of Education affiliated to the Ministry of National Education has been put into practice as of the 2018-2019 academic year (MEB, 2018a). According to this timetable, while Information Technologies and Software courses are not a part of the curriculum for the first four years of primary school, they are compulsory in the 5th and 6th grades and are in the elective course list in the 7th and 8th grades. It is a need to examine the books used in the Information Technologies courses either compulsory or elective in curriculum, in terms of safe internet usage and education. As mentioned above, although there are many kinds of dangers and risks that children may encounter on the internet, there are many methods to deal with them and measures that can be taken. The question is which of these measures and methods are included in the curriculum, and to what extent.

In the literature, it is possible to find many studies investigating whether students use the internet safely. However, there are not many studies to reveal what kind of trainings are given regarding secure internet use. Education is the desired and permanent change of behavior of the individual. Is the information about the secure internet use given in the books sufficient to change the student's behavior in a permanent and desired way? This study is important in terms of revealing the trainings on secure internet use in primary and secondary schools. Determining the current situation will make it easier for curriculum developers to identify missing or wrong aspects and will provide a general perspective to these people. In this study, it is aimed to reveal the current situation by examining the books used in Information Technologies and Software courses in the curriculum of primary and secondary schools in terms of secure internet use. The results are expected to raise awareness about the importance of using safe internet for children and provide ideas for the future researches on this subject.

Methodology

In this qualitative study, document analysis method is employed. Document analysis is carried out in the form of examination and analysis of various written or visual materials containing information related to the research questions of the study such as books, magazines, newspapers, archives and letters (Cansız-Aktaş, 2015) in cases where direct observation or interview is not possible (Yıldırım & Şimşek, 2005). Since the research questions are directly related to the examination of the Information Technologies and Software Course textbooks which are deemed suitable for use in primary and secondary schools for 5 years starting from 2018 by the Ministry of National Education, the data were collected by document analysis method. The research topic being safe internet use within the scope of informatics courses, these books have been selected as main data source.

Information Technologies and Software Course, planned to be taught in primary schools, offers a different structure from the classroom level. A theme-based structure is presented for grades 1 through 4 in primary school. The levels indicated in the themes don't represent the classes but the level of skill that the students must acquire. Different levels can be taught in different classes according to the individual skills of the teacher and the readiness of the students (MEB, 2018b). The web page of the Ministry of National Education was used for downloading the Information Technologies and Software course books. However, 7th and 8th grade textbooks couldn't be accessed from the web page of the Ministry of National Education because all textbooks are sent to schools for free by Ministry of National Education; but the ones for the elective courses (7th and 8th grades) are sent upon request and none of the schools applied held a hard or online copy. The books reviewed are given in Table 1.

Table 1. Textbooks examined in the scope of the study

Level	Book Title
Level 1	Information Technologies and Software Course 1st Level Activity Book
Level 2	Information Technologies and Software Course 2nd Level Activity Book
Level 3	Information Technologies and Software Course 3rd Level Activity Book
Level 4	Information Technologies and Software Course 4th Level Activity Book
5th Grade	5th Grade Information Technologies and Software Course Student Materials
6th Grade	6th Grade Information Technologies and Software Course Student Materials

The data obtained from the Information Technologies and Software course textbooks used in primary and secondary schools were analyzed by content analysis method. Each book has been reviewed one by one and each page covering the secure internet use was discussed. While examining the books, terms related to *secure internet use* were coded and the codes under the same topic were grouped and categories were obtained.

Table 2. Number of Learning Outcomes in Curriculum

Level	Theme	Topic	Outcomes
Level 1	Ethics and Security		3
Level 2	Ethics and Security		3
Level 3	Ethics and Security		3
Level 4	Ethics and Security		3
5th Grade	Ethics and Security	Ethical Values	4
		Digital Citizenship	3
		Privacy and Security	2
6th Grade	Ethics and Security	Ethical Values	7
		Digital Citizenship	2
		Privacy and Security	6
7th Grade	Ethics and Security	Ethical Values	2
		Privacy and Security	4
8th Grade	Information Technologies	Privacy and Security	3

Findings

In this part of the research, the Information Technologies and Software Course textbooks examined in terms of the secure internet use are discussed separately and the findings related to the text and images in each book are presented on a book-by-book basis. The list of behaviors to be gained by students in these courses are given in the Information Technologies and Software Course Curriculum for primary and secondary schools published by the Ministry of National Education in 2018 (MEB, 2018b; MEB, 2018c; MEB, 2018d). When these programs were examined, it was seen that the learning outcomes related to the secure internet use are generally given under the theme of "ethics and security". The units where "secure internet use" topics are handled in Information Technologies and Software Courses and the number of learning outcomes to be given in these units, obtained from the education programs offered by the Ministry

of National Education are given in Table 2. The findings obtained from the books taught in Information Technologies and Software Courses are presented below for each book one by one.

Information Technologies and Software Course 1ˢᵗ Level Activity Book

The learning outcomes related to the use of secure internet in Information Technologies and Software Courses are generally given in the theme of Ethics and Security. In the Ethics and Security theme of the 1ˢᵗ Level Activity Book, no learning outcomes were found regarding the use of secure internet. The book includes learning outcomes which are about ethics and about secure use of the computer as an electronic device.

Information Technologies and Software Course 2ⁿᵈ Level Activity Book

In the Information Technologies and Software Course 2ⁿᵈ Level Activity Book, there are 2 learning outcomes related to the confidentiality and security of personal information in addition to one gain related to the secure use of computer and computer labs. Through activities "Everything about Me" and "Attention! Top Secret!", it is aimed to teach students what personal information is and to raise awareness that this information is so valuable that it should be protected while using the internet. Screenshots of the activities in the book and translations of some texts are given in Figure 1. When we have a closer look at Figure 1, it becomes obvious that the text and drawings given in the book are suitable for primary school level.

Figure 1. "Everything about Me" and "Attention! Top Secret!" Activities

	In this table, 4 children named Mete, Aslı, Kaan and Ela are asked for their personal information. The answer "Söylemem" means "I don't/won't say". Except from that, the children answer their personal information correctly. In the activity, the students are asked 3 open-ended questions according to the information provided in the table: 1- Who has given personal information that should not be given? 2- Who has not given any personal information? 3- Which information should not be given except this information?
	ATTENTION! TOP SECRET! • Do not share your personal information with people you do not know on the Internet! • Do not accept messages, friendship requests or files from people you do not know on the Internet! • Inform an elder family member about the situations that make you worry, upset, or scared! • Check the reliability of the website you enter, whether the person you are communicating with is real or not, with help from an elder family member!

Information Technologies and Software Course 3ʳᵈ Level Activity Book

Information Technologies and Software Course 3ʳᵈ Level Activity Book, which has 3 learning outcomes related to the secure internet use, includes topics such as respect for others, protection of personal information and generating secure password. In addition, topics related to the conscious use of the internet are mentioned such as the use of the search engine and research on the internet. Event cards, posters related to the learning outcomes and translations of some texts are shown in Figure 2. In the activity titled "I use the internet consciously", the rights and responsibilities of internet usage are mentioned. In another activity titled "Don't Touch My Personal Information", the importance of personal information is emphasized and given examples of what problems will arise if they are not protected. In the "My Secure Password" activity, it has been tried to provide information about how passwords, which are very important in social media, online shopping and internet banking transactions should be created.
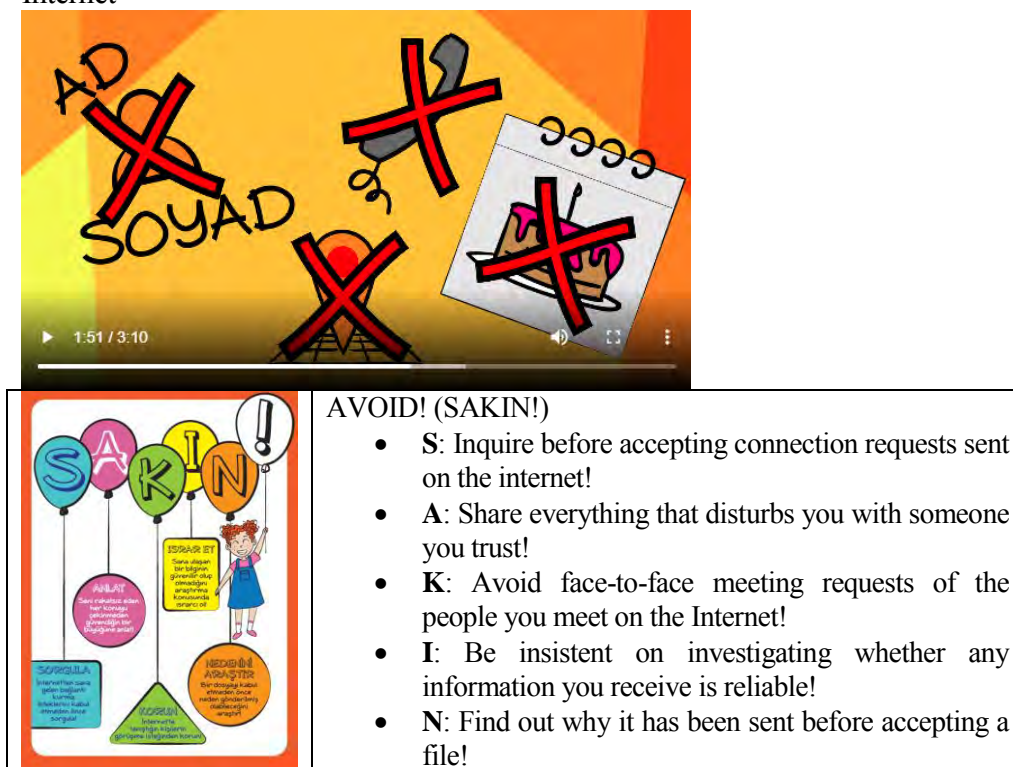
Figure 2. "I use the Internet Consciously", "Don't Touch My Personal Information" and "My Secure Password" Activities

	CONSCIOUS INTERNET USER
	1. Always respect the rights of others. Before sharing a photo or information, be sure to obtain the consent of the person in the photo or the person who posted the information. 2. Review before expressing your feelings and thoughts. 3. Always use a gentle and positive language on the Internet. 4. Use your time efficiently on the Internet. 5. Share information you are sure is correct. 6. Share topics that can contribute to the Internet world and the topics you are an expert. Etc.
	The activity titled "Don't Touch My Personal Information" is a role play activity depicting the sharing of personal information in public places.
	MY SECURE PASSWORD • We need to make sure it contains at least 8 digits. • We should be make sure that our password has at least one Uppercase / lowercase (A, a, B, b,… Z, z), number (0, 1, 2,…, 9), punctuation mark (. , ; : etc.), and special character (% / & etc.). • In all cases, do not use the same password. We must generate different passwords for different situations. • PERSONAL INFORMATION: We should not include our personal information while generating a password.

Information Technologies and Software Course 4th Level Activity Book

The results of the analysis of the Information Technologies and Software Course 4th Level Activity Book which includes the topics of information ethics, digital footprint and internet security, indicate that 2 learning outcomes related to secure internet use are emphasized. These learning outcomes are "Realizes that transactions and user information on the internet are recorded" and "Realizes that the identities used on the internet may be fake". Screen shots of the video and activity in the book and translations of some texts are given in Figure 3.

Figure 3. Animation of "Digital Footprint" and poster of "Stay Safe on the Internet"

AVOID! (SAKIN!)
- **S**: Inquire before accepting connection requests sent on the internet!
- **A**: Share everything that disturbs you with someone you trust!
- **K**: Avoid face-to-face meeting requests of the people you meet on the Internet!
- **I**: Be insistent on investigating whether any information you receive is reliable!
- **N**: Find out why it has been sent before accepting a file!

The Information Technologies and Software Course Level 4 Teacher's Guide book has two activities related to this topic; one is an animated movie about digital footprint, and the other is a game activity. The animation (Figure 3) fits the student levels well in representing the fact that all the information used for signing in on the internet is recorded somewhere and it isn't possible to delete them. The "Stay Safe on the Internet" poster aims to teach the students that the people encountered on the internet can harm them by using fake identities. In this poster, students are taught that they should be careful before opening messages and other content sent by people they don't know.

5th Grade Information Technologies and Software Course Student Materials

In the 5th Grade Information Technologies and Software Course Student Materials textbook, there are 4 learning outcomes related to Ethical Values, 3 related to Digital Citizenship, and 2 related to Privacy and Security. The activities in the book are designed to make sure that students gain responsibilities related to digital citizenship in terms of secure internet use; and their ability to protect personal data is measured by "Digital Footprint" test. Within the scope of the course, it is aimed to develop awareness of respecting the rights of others and coping with digital bullying.

Figure 4. "Digital Citizenship" and "Privacy and Security" Events

- If I Am a Good Digital Citizen (İyi Bir Dijital Yurttaşsam)
- DIGITAL FOOTPRINT TEST (DİJİTAL AYAK İZİ TESTİ)
  1. Do you go online every day?
  2. How many hours do you stay online?
  3. Do you also connect to the internet on your mobile phone?
  4. Do you share songs on the Internet? Etc.
- Hidden Like a Secret (Sır Gibi Saklı): The steps of converting the word "Samsunlu" into S@m5U#1u as a password areexplained.
- How do I recognize cyber traps? (Siber Tuzakları Nasıl Anlarım?)
  5. Be wary of websites that request credentials on the Internet.
  6. Avoid free gifts, programs and contests that says you will win. Etc.

Sample pages from the 5th Grade Information Technologies and Software Course Student Materials textbook and translations of some texts have been shown in Figure 4. In addition to the topics of digital citizenship and digital footprint, the activities in the book also teach students how a strong password can be generated and the dangers that may be encountered on the internet.

6th Grade Information Technologies and Software Course Student Materials

The results of the analysis of the 6th Grade Information Technologies and Software Course Student Materials textbook which covers Ethical Values, Digital Citizenship and Privacy and Security topics indicate that a total of 15 learning outcomes are included in the Ethics and Security theme. In these learning outcomes, methods related to the secure internet use such as protection from cyber

bullying, protection from information criminals, protection of personal information and protection from harmful software are mentioned.

Figure 5, which provides sample pages about secure internet use and translations of some texts, lists the behaviors that should and should not be done in relation to digital bullying and secure websites use, presents a poster which includes information about the protection of personal information and malicious software. The visuals and texts are appropriate for the level of the target audience.

Figure 5. Sample Pages from the 6th Grade Student Materials Textbook

	DON'T BE A BULLY! • Don't save and share personal conversations • Don't send offensive and too many messages! **DON'T BE SCARED!** • Don't answer the bullies, block them. • Share with an adult you trust right away. • Keep the message or email sent to you
	I LOVE MY CYBER MIND! On unsafe websites; • Don't be a member! • Don't shop! • Don't click on the links! • Don't believe the news right away! • Don't download! Remember that you will never be completely safe on the Internet!
	WHAT ARE THE THREATS TO INFORMATION SECURITY? • Distortions during writing, reading, and transporting information. • Physical damages 　Etc. **HOW TO PROVIDE INFORMATION SECURITY?** • Security software. • Make a backup. 　Etc.
	DANGEROUS SOFTWARE TEAM • I'm a virus! I reproduce, I live in other programs, I infect. I slow down the computer, I can corrupt information. • I'm an antivirus! I recognize malicious software, if I find it on your computer, I delete it. If I cannot delete it, I will quarantine. I follow new viruses. I block unauthorized access. I try to speed up the system.

7th and 8th Information Technologies and Software Course Textbooks

As the 7th and 8th grade Information Technologies and Software Course textbooks couldn't be accessed from the web page of the Ministry of National Education, they are not included in the analysis. However, 7th and 8th grade learning outcomes related to the use of secure internet in the Education Program (MEB, 2018d) published by the Ministry of National Education are accessed. The analysis suggests that the learning outcomes in the curriculum are under the themes of Ethics and Security of 7th grade and Information Technologies of 8th grade. In the 7th Grade Curriculum, there are 2 learning outcomes in Ethical Values, 4 learning outcomes in Privacy and Security; and in the 8th Grade Curriculum, 3 learning outcomes in Privacy and Security are included. In the learning outcomes related to the secure internet use, the factors that threaten information security, measuring the security levels of various environments, measures that could be taken against the dangers and the topics to be considered in online shopping are mentioned.

Summary of Findings

Table 3 shows a summary of the findings obtained through the analysis of the 1st - 4th levels, 5th and 6th grades Information Technologies and Software student material textbooks in the form of categories and codes. Although the data of the first 6 books were obtained by examining the document itself, the data of the 7th and 8th grades were obtained only from the learning outcomes without examining the textbooks.

Table 3. The Distribution of the Topics of Safe Internet Use by Books

Categories	Codes	Levels				Grades				f
		1	2	3	4	5	6	7	8	
Ethic	Internet ethics	X			X	X	X	X		5
	Respect for others	X		X	X	X	X			5
	Violation of Ethics					X	X			2
	Copyright						X			1
	IT Crimes						X			1
	Intellectual property							X		1
Digital Citizenship	Practices					X				1
	The effects of information sharing					X	X			2
	Appropriate game selection						X			1
Security	Computer security	X	X							2
	Protection of personal information		X	X	X	X	X	X	X	7
	Generating a strong password			X		X				2
	Digital Footprint				X	X	X			3
	Cyber Bullying					X	X			2
	Malware and antivirus						X		X	2
	Security precautions			X	X	X	X	X	X	6
	Online shopping					X	X		X	3
Total		*3*	*2*	*4*	*5*	*11*	*13*	*4*	*4*	*46*

Although the findings obtained from the books examined within the scope of the study were presented above on a book-by-book basis, when the Table 3 prepared to reveal a general picture is examined, it is obvious that "Protection of personal information" is the most commonly mentioned topic. This is followed by "Security measures" under the security category. The codes of "Internet ethics" and "Respect for others" in the category of ethics are the most commonly mentioned topics of this category. The other subjects are distributed in a balanced way to levels and grades.

When the findings on the basis of books are examined, it becomes clear that the books with the highest frequency in terms of ethical and security topics are 6th and 5th grade textbooks, respectively. In the textbooks of 1st and 2nd levels, besides ethics, only the secure use of the computer as an electronic device is mentioned. There is a balanced distribution in the other textbooks.

Conclusions

A qualified and rich learning experience can only be ensured through a well-organized education process. For this reason, the goals and gains to be achieved must be supported by a rich content and a qualified learning experience (Bulut & Dursun, 2019). The aim of this study is to reveal the current situation by examining the textbooks used in Information Technologies and Software Course in the curriculum of primary and secondary schools in terms of secure internet use. For this purpose, Information Technologies and Software Course textbooks were downloaded from the web page of the Ministry of National Education and "Ethics and Security" themes were examined through content analysis method. The results of the analysis can be summarized below.

The topic of *protection of personal information* is mentioned in almost all the textbooks. Nowadays, having the knowledge of secure use of the internet, which has entered every home and pocket, concerns children as well as adults. It is generally known that children use computers at home or parents' mobile phones for playing games or watching videos (Kaşıkçı et al. 2014). With subliminal messages placed in games, codes running in the background that allow remote control, advertisements placed between games and videos (Tarı, Taşdemir, Özcan, & Tarı, 2018), children can easily be distracted. It is essential to repeatedly remind students of what level of information should be protected and should not be randomly shared on the internet. Perhaps this will enable them to become conscious of the possible dangers.

Security measures is also one of the most commonly mentioned topics in the security category. In most of the textbooks, this topic is placed with the topics of internet ethics and respect for others. Measures to be taken regarding the use of secure internet include instructions about personal information shouldn't be shared with strangers and/or unsafe sites; strong passwords should be set for user accounts, reliable and current software should be used against malicious software. These suggestions are parallel to the ones made by Yavanoğlu, Sağıroğlu and Çolak (2012).

Internet ethics and respect to others are the most common topics under the category of ethics. While mentioning the possible harms of sharing personal information on the internet, the textbooks handles both the topics of not harming others and not being harmed by them. There are recommendations to children who are at risk of encountering malicious people on the internet at all times on how to deal with these problems.

Other topics related to secure internet use appear to be distributed balanced in the books. These topics can be listed as transactions related to digital citizenship, violation of ethics, IT crimes, intellectual property, digital footprint, cyber bullying and online shopping. Given that the most persistent risk among children are bullying and cyberbullying (92%), hate speech (88%) and sexual content (75%) (Dinh, Farrugia, O'Neill, Vandoninck, & Velicu, 2016), it can be concluded that the trainings and measures to be taken should be increased.

Discussion and Suggestions

Every precaution should be taken to protect children from the dangers they may face both in the real world and the virtual one. All stakeholders have various duties to protect children from risks that may arise from the internet (Gökçearslan & Seferoğlu, 2016). Measures should be taken at the government, ministerial, school, family and individual levels; and continuous activities should be organized to pay enough attention. Measures taken by the government include making internet service providers implement various filters (Wishart, 2004) and enacting various laws to punish cybercrimes. The Ministry of National Education aims to enable students to acquire secure internet use behaviors by the ethical and security themes included in the curriculum. Computer course, which was among the elective courses before, is now included in the curriculum as a compulsory course in the 5th and 6th grades under the name of Information Technologies and Software. It is considered necessary to be among the compulsory courses in both primary school and 7th and 8th grades because of the importance it holds. Measures to be taken by families can be listed as restricting the internet against harmful content by using a family profile, using the internet with children, positioning the computer to be used by children in a place where everyone can see the screen and informing children about the dangers they may encounter (Greenfield, 2004). Spending more than 40 hours a week on the internet is a sign of addiction (Soule, Shell, & Kleen, 2003). Parents should control the amount of time children spend in front of a computer screen.

Television, with the highest rate of use by children in terms of media use (Aslan, Turgut, Göksu, & Aktı-Aslan, 2019), should make broadcasts that will mediate awareness raising activities for children on secure internet use. In domestic and national cartoons broadcasted on children's channels, these subjects should be handled. Producers can also shoot a documentary film containing the damages that may arise when enough attention is not paid to cyber security. The evolution of the technology, while easing our lives from many perspectives, will keep gradually increasing the factors threatening our kids/future. In this respect,

high school and university curricula should be carefully examined and the current situation should be put forward regarding the secure internet use keeping the precautions up to date. The scope of training and awareness-raising activities on secure internet use and IT crimes should be extended to be more inclusive for the family, teachers and school administrators.

<div align="center">References</div>

Akbulut, Y. (2013). Çocuk ve ergenlerde bilgisayar ve İnternet Kullanımının gelişimsel sonuçları [Developmental implications of computer and Internet use among children and adolescents]. *Trakya University Journal of Education, 3*(2), 53-68.

Aslan, A., & Karakuş-Yılmaz, T. (2017). Türkiye'de güvenli İnternet kullanımına yönelik gerçekleştirilen uygulamalar [Practices developed towards safer Internet use in Turkey]. *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, 53*, 121-143.

Aslan, A., Turgut, Y. E., Göksu, İ., & Aktı-Aslan, S. (2019). Çocukların medya okuryazarlık düzeylerinin ve kullanım alışkanlıklarının demografik değişkenler açısından incelenmesi [Examining children's media literacy levels and usage habits in terms of demographic variables]. *Gazi Üniversitesi Gazi Eğitim Fakültesi Dergisi, 39*(2), 793-815.

Aytaç, T., & Erdem, M. (2019). Examining high school students' safe computer and internet usage awareness. *European Journal of Education Studies, 6*(1), 295-311.

Beder, A., & Ergün, E. (2015). Ortaokul öğrencilerinin güvenli İnternet kullanım durumlarının belirlenmesi [Assessment of secondary school students' safe Internet usage]. *Eğitim Bilimleri ve Uygulama, 14*(27), 23-41.

Bilgin-Ülken, F., & Kılınç, F. (2018). Çocukların çevrimiçi ortamda karşılaştıkları risk türleri ile aracılık uygulamaları arasindaki ilişki [The relationship between the risk types that the children come across on online platforms and parental mediation]. *İnsan ve Toplum Bilimleri Araştırmaları Dergisi, 7*(1), 124-145.

Bulut, A., & Dursun, F. (2019). Aktif öğrenme modelinin eleştirel düşünme eğilimleri üzerindeki etkisinin belirlenmesine yönelik öğrenci ve öğretmen görüşleri [Student and teacher opinions on determining the effect of active learning model on critical thinking trends]. *Gümüşhane University Journal of Social Sciences Institute, 10*(3), 610-626.

Canbek, G., & Sağıroğlu, Ş. (2007). Çocukların ve gençlerin bilgisayar ve İnternet güvenliği [Computer and Internet security for children and teenagers]. *Journal of Polytechnic, 10*(1), 33-39.

Cansız-Aktaş, M. (2015). *Kuramdan Uygulamaya Eğitimde Bilimsel Araştırma Yöntemleri [Scientific Research Methods in Education from Theory to Practice].* Metin, M. (Ed.) Nitel veri toplama araçları. Ankara: Pegem Akademi.

Colley, A., & Maltby, J. (2008). Impact of the Internet on our lives: Male and female personal perspectives. *Computers in Human Behavior, 24*(5), 2005-2013.

Çelen, F. K., Çelik, A., & Seferoğlu, S. S. (2011). Çocukların İnternet kullanımları ve onları bekleyen çevrim-içi riskler [Children's Internet usage and online risks they face]. *Akademik Bilişim'11 - XIII. Akademik Bilişim Konferansı*, (pp. 645-652). Malatya.

Demirel, M., Yörük, M., & Özkan, O. (2012). Çocuklar için güvenli İnternet: Güvenli İnternet hizmeti ve ebeveyn görüşleri üzerine bir araştırma [Safe Internet for children: A study on safe Internet service and parental views]. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 4*(7), 54-68.

Dinh, T., Farrugia, L., O'Neill, B., Vandoninck, S., & Velicu, A. (2016). *Internet safety helplines: Exploratory study first findings.* Retrieved 11 11, 2019, from https://bit.ly/3aVGAVZ.

Gök, T. (2015). The positive and negative effects of digital technologies on students' learning. *ICEMST 2015: International Conference on Education in Mathematics, Science & Technology* (pp. 173-177). The Eurasia Proceedings of Educational & Social Sciences (EPESS).

Gökçearslan, Ş. (2016). *Bilişim suçları ve etik [IT crimes and ethics]*. S. Şahin (Ed.), *Eğitimde Bilişim Teknolojileri I-II.* Ankara: Pegem Akademi.

Gökçearslan, Ş., & Seferoğlu, S. S. (2016). Ortaokul öğrencilerinin İnternet kullanım biçimleri: Riskli davranışlar ve fırsatlar [The use of the Internet among middle school students: Risky behaviors and opportunities]. *Kastamonu Eğitim Dergisi, 24*(1), 383-404.

Greenfield, P. M. (2004). Inadvertent exposure to pornography on the Internet: Implications of peer-to-peer file-sharing networks for child development and families. *Journal of Applied Developmental Psychology, 25*(6), 741-750.

Güvenli Çocuk. (2019). *Siber Çocuk [Cyber Boy].* Retrieved 11 10, 2019, from https://bit.ly/33sjzr5.

Güvenli Web. (2019b). *Ebeveyn Denetim Araçları [Parental Control Tools].* Retrieved 11 10, 2019, from https://bit.ly/3b02IhO

Güvenli İnternet. (2019). *Güvenli İnternet Hizmeti: Güvenli İnternet Hizmeti Nedir?* [*Secure Internet Service: What is Secure Internet Service?*]. Retrieved 11 10, 2019, from https://bit.ly/2xHQOeg.

Hope, J. (2002). Internet safety: Issues for New Zealand primary schools. *Proceedings NetSafe: Society, Safety and the Internet,* (pp. 59-68).

İlhan, V., & Aydın, H. (2019). Okul topluluğu üyelerinin İnternet ve mobil iletişim teknolojileri ile etkileşimin olası riskleri üzerine düşünceleri [Thoughts of members of the school community on the possible risks of interaction with Internet and mobile communication technologies]. *The Journal of International Social Research, 12*(64), 755-772.

Kaşıkçı, D. N., Çağıltay, K., Karakuş, T., Kurşun, E., & Ogan, C. (2014). Türkiye ve Avrupa'daki çocukların İnternet alışkanlıkları ve güvenli İnternet kullanımı [Internet habits and safe Internet use of children in Turkey and Europe]. *Education and Science, 39*(171), 230-243.

MEB. (2018a). *İlköğretim Kurumları (İlkokul-Ortaokul) Haftalık Ders Çizelgesi (2018-2019 Eğitim Öğretim Yılında Uygulanacak).* Ankara: Milli Eğitim Bakanlığı. Retrieved 11 11, 2019, from http://ttkb.meb.gov.tr/meb_iys_dosyalar/2018_10/08141710_ilkogretimkurumlari_hdc.rar

MEB. (2018b). *Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı (İlkokul 1, 2, 3 ve 4. Sınıflar).* Ankara.

MEB. (2018c). *Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı (Ortaokul 5 ve 6. Sınıflar).* Ankara.

MEB. (2018d). *Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı (Ortaokul ve İmam Hatip Ortaokulu 7 ve 8. Sınıflar).* Ankara.

Mert, M., Bülbül, H. İ., & Sağıroğlu, Ş. (2012). Milli Eğitim Bakanlığına Bağlı Okullarda Güvenli İnternet Kullanımı [Using of Security Internet in Schools of Ministry of Education]. *TÜBAV Bilim Dergisi, 5*(4), 1-12.

Moreno, M., Egan, K., Bare, K., Young, H., & Cox, E. (2013). Internet safety education for youth: Stakeholder perspectives. *BMC Public Health, 13*(1:543).

Orhan, F., & Akkoyunlu, B. (2004). İlköğretim öğrencilerinin İnternet kullanımları üzerine bir çalışma [A study on the use of Internet by primary school students]. *Hacettepe Üniversitesi E¤itim Fakültesi Dergisi, 26*, 107-116.

Soule, L. C., Shell, L., & Kleen, B. (2003). Exploring Internet addiction: demographic characteristics and stereotypes of heavy Internet users. *Journal of Computer Information Systems, 44*(1), 64-73.

Tarı, M., Taşdemir, Ş., Özcan, C., & Tarı, A. (2018). Kırsal kesimdeki ilköğretim öğrencilerinin internet kullanımlarının TÜİK verileriyle karşılaştırılması ve güvenlik incelemesi [Internet usage of elementary school students in rural area comparison with TUIK Data and security review]. *International Journal of Multidisciplinary Studies and Innovative Technologies, 2*(1), 21-25.

Tekin, A., & Polat, E. (2016). Ortaokul öğrenci velilerinin güvenli İnternet kullanımı farkındalığı [Secondary school students' parents' safe Internet usage awareness]. *Journal of Instructional Technologies & Teacher Education, 5*(2), 80-92.

TÜİK. (2019). *Sabit telefon, cep telefonu ve internet abone sayısı* [*Number of fixed phones, mobile phones and internet subscribers*]. TÜİK, Ulaştırma ve Altyapı Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu. Retrieved 11 7, 2019, from http://www.tuik.gov.tr/PreIstatistikTablo. do?istab_id =1580

Valcke, M., Bonte, S., De Wever, B., & Rots, I. (2010). Internet parenting styles and the impact on internet use of primary school children. *Computers & Education, 55*, 454-464.

Wishart, J. (2004). Internet safety in emerging educational contexts. *Computers & Education, 43*, 193-204.

Yavanoğlu, U., Sağıroğlu, Ş., & Çolak, İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler [Information security threats and taking privacy precausions in social networks]. *Journal of Polytechnic, 15*(1), 15-27.

Yiğit, M. F., & Seferoğlu, S. S. (2019). Öğrencilerin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve çeşitli diğer değişkenlere göre incelenmesi [Investigating students' cyber security behaviors in relation to big five personality traits and other various variables]. *Mersin University Journal of the Faculty of Education, 15*(1), 186-215.

Yıldırım, A., & Şimşek, H. (2005). *Sosyal bilimlerde nitel araştırma yöntemleri* [*Qualitative research methods in the social sciences*]. Ankara: Seçkin Yayıncılık.