Available online at ijci.wcci-international.org

International Journal of Curriculum and Instruction
12(Special Issue) (2020) 271–294

IJCI
International Journal of Curriculum and Instruction

A swot analysis to raise awareness about cyber security and proper use of social media: Istanbul sample

Nilgün TOSUN[a*], Murat ALTINÖZ[b], Emil ÇAY[c], Turan ÇİNKILIÇ[d], Sevinç GÜLSEÇEN[e], Tülay YILDIRIM[f], Muhammed Ali AYDIN[g], Bilgin METİN[h], Zerrin AYVAZ REİS[i], Nafiz ÜNLÜ[j]

[a*]*Assoc. Prof. Dr., Trakya University, Faculty of Education, Computer Education and Instructional Technologies Department, Edirne, TURKEY*

[b]*Istanbul Directorate of National Education, Provincial Deputy Director of National Education, İstanbul, TURKEY*

[c]*Halkalı ISE Multi-Program Anatolian High School, Information Technology Teacher, İstanbul, TURKEY*

[d]*TASEV Shoes and Saraciye M. and Technical Anatolian High School, Information Technology Teacher, İstanbul, TURKEY*

[e]*Prof. Dr., Istanbul University, Informatics Department, İstanbul, TURKEY*

[f]*Prof. Dr., Yıldız Technical University, Faculty of Electrical and Electronics, Department of Electronics and Communication Engineering, İstanbul, TURKEY*

[g]*Assoc. Prof. Dr., Istanbul University-Cerrahpaşa, Computer Engineering Department, İstanbul, TURKEY*

[h]*Assoc. Prof. Dr., Boğaziçi University, Department of Management Information Systems, İstanbul, TURKEY*

[i]*Assit. Prof. Dr., Istanbul University-Cerrahpaşa, Informatics Department, İstanbul, TURKEY*

[j]*Assist. Prof. Dr., Istanbul Technical University, Informatics Institute, İstanbul, TURKEY*

Abstract

Internet is a cyber-ambient where the number of users is increasing consistently as a result of wide opportunities those are provided and where access can be ensured with information technologies. Today, via internet and social media where the number of users reaches billions, the samples of committed cybercrimes and cyber-attacks are increasing throughout the world. For this reason, it is inevitable to raise awareness in the society about cyber security and social media use. Raising awareness also can be done by providing education for all sections of the society. It is aimed to bring the expert person who has knowledge and experiences to provide support about creating substructure of education about both cyber security and using social media, by considering potential of institution and organization, and these sharers hosted by Istanbul Provincial Directorate of National Education and it is aimed to make cooperations. In line with this aim, Cyber Security and Proper Use of Social Media Workshop was realized in Istanbul on 17-18 February 2018. In discussions made within the scope of the workshop, the participants made SWOT analyses on behalf of using social media properly and to raise awareness for cyber security. In that study, information will be given about these analyses performed for Istanbul province.

Keywords: Cyber security; social media; awareness; swot analysis

1. Introduction

Cyber security is considered as an important problem for many countries in recent years when internet and social media use are intensified. Increasing cyber wars those are considered as dangerous as the wars made by weapons, made countries take measures about this matter. It is clear that it will be effective by educating the individuals. As David Kevin Mitnick, a worldwide famous computer hacker, stated, human being is the most vulnerable ring of security chain. The base for creating a national cyber security, is to create an individual cyber security culture. Within the scope of efforts to create awareness for national and individual cyber security, some studies are performed in Turkey. One of them is Cyber Security and Proper Use of Social Media Workshop which is the subject of this statement. The purposes of that workshop realized in Istanbul on 17-18 February 2018, can be stated as follows; to raise awareness on out students about cyber security, to ensure that they are able to take basic level security measures, to provide opportunity for the student to make career planning in the field of cyber security by attracting attention about lack of experts in this field and effects of the cyber war that is experienced in the world, to provide education for preventing victimizations experienced on social media accounts, to clarify the students about cyber ethic and technology addiction, protecting personal privacy, cyber bullying, digital footprint, to increase readiness level for future occupations and social media expertize. Various institutions and organizations provided supports for the workshop:

1.Presidential Department of Corporate Communication

2.Ministry of National Education Head Council of Education and Morality

3.Ministry of National Education Directorate General for Innovation and Education Technologies

4. Boğaziçi University

5. Istanbul University

6. Istanbul University- Cerrahpaşa

7. Istanbul Technical University

8. Istanbul Medeniyet University

9. Trakya University

10. Yıldız Technical University

11.Public Prosecutor of Istanbul

12. Istanbul Police Headquarters Directorate of Anti-Cybercrimes

13. TÜBİTAK BİLGEM

14. HAVELSAN

15.Information and Communication Technologies Authority

16. Turkish Informatics Association

17. Informatics Innovation Association

18. BT Risk Data Security

19. GAIS Security

Within the scope of the workshop, the groups were created to discuss cyber security and proper use of social media. In each group; there were two moderators, 42 teachers from different branches from various types of schools, academicians those are experts in their fields, related Non-Governmental Organization (NGO) and invited representatives of Corporation. The groups performed below ones about cyber security and proper use of social media;

They presented current problems for Istanbul province (in terms of students, teachers and supervisors and parents),

They performed SWOT analyses to solve these problems,

They presented suggestions for solutions.

SWOT analysis is a method used commonly to determine and analyze resources of an organization and elements around that in four dimensions such as Strengths, Weaknesses, Opportunities and Threats (Samejima, Shimizu, Akiyoshi and Komoda, 2006). SWOT analyses should aim to ensure that skills and assets those perceived by the organization, are recognized and assessed by the sharers of the organization. The perspectives of the sharers should also be taken into consideration (Piercy & Giles, 1989; Wilson & Gilligan, 2005). For these reasons, in this workshop that was performed by focusing on Istanbul province, the sharers from education area and the sharers from cyber security area were brought together, about cyber security and proper use of social media, determining pushing forces and limiting factors, interpreting them and providing solutions were planned and realized.

2. Method

In this study, the data obtained from the participants of Cyber Security and Proper Use of Social Media Workshop held in Istanbul about cyber security were associated with a field literature review that was realized by the writers. Within the framework of the information obtained, the current situation involving the students, teachers, administrators and parents of the institutions that are dependent on the Ministry of National Education in Istanbul was tried to be revealed through a SWOT analysis. The study is important as it is the first SWOT analysis conducted on this subject in Istanbul. It is considered that the analysis made for Istanbul city, and the issues addressed and highlighted within the scope of the analysis are important for other cities too. It is hoped

that the information provided by this analysis will guide decision makers and implementers in establishing cyber security policies on individual, institutional and national.

3. SWOT Analyze Performed in the Workshop

3.1. Strengths

1) Having opportunity to reach parents of student in primary, secondary and high schools.
2) Importance of support from decision makers.
3) Existence of school-parent unions.
4) Importance and estimable religious values in internet ambient.
5) Measurement and assessment easiness about cyber awareness and being able to make central examinations.
6) Having sufficient documentation and material regarding the subject.
7) Sufficiency of human resources those can support the process.

Informing parents about cyber security and making warnings about students are easy in primary, secondary and high schools because school managements have communication with school-parent unions, teachers and parents consistently. This communication can be realized face to face and periodical meetings as well as electronic environments. Especially there are many Whatsapp groups those created by teachers and parents. Besides, social media accounts and web pages of schools are other environments used for electronic communication. Ministry of National Education Department of Information Technologies published School Internet Web pages Directives on 05.06.2018. With this directive, principles and rules those are required to follow about service application, management and publishing organizational internet web pages of state schools depending to Ministry of National Education and the organizations using meb.k12.tr domain name (Ministry of National Education Department of Information Technologies, 2018). There are organizational internet webpages those actively used by all schools in Istanbul as well as Turkey (For instance; Turgut Reis İlkokulu (Turgut Reis Primary Schools) official webpage http://silivriturgutreisio.meb.k12.tr/, Genç Osman İmam Hatip Ortaokulu (Genç Osman Religious Secondary School) official webpagehttp://gencosmaniho.meb.k12.tr/, Beşiktaş Anadolu Lisesi (Beşiktaş Anatolian High School) official webpagehttp://besiktasanadolu.meb.k12.tr/). It is aimed to ensure that new generation and many parents are social media user, to make and establish communication information exchange with students and parents via establishing organizational social media account by school managers and via establishing personal

social media accounts by teachers. Şehit Er Müslüm Zengin İlkokulu (Şehit Er Müslüm Zengin Primary School) Facebook account https://tr-tr.facebook.com/%C5%9Eehit-Er-M%C3%BCsl%C3%BCm-Zengin-ilkokulu-1435944160035148/, İstiklal Ortaokulu (İstiklal Secondary School) Instagram account https://www.instagram.com/istiklalilkortaokulu/, Pertevniyal Lisesi (Pertevniyal High School) Twitter account https://twitter.com/pertevniyal, can be given as examples for organizational social media accounts of schools.

Besides, it is also procedural easy to make coordination and cooperations between Ministry of National Education and all dependent departments. This situation is one of important factors empowering to take measures.

Another strenght is the subject of religious values. Religious values such as respect, love, empathy, moral and ethical those the society holds and the society has to hold, are valid and valuable also for internet environment. If new generation is education in an equipped way in terms of moral and cultural values, this education will have positive reflects also on internet environment. From this point of view, rules of good manners project was started in 2017 by Istanbul Provincial Directorate of National Education with the title of "A Kind Generation Will Raise From Istanbul". The purpose of this project is to give rules of good manners those are obtained by social learning from elders such as grandmother or grandfather, to students in school environment in today when these rules cannot be learnt due to family structure getting smaller, intense working lives of parents. The rules will not be given within the scope of a course, an environment will be created by teachers, these will be tried to be learnt by brainstorming and social learning (Güncel Eğitim, 2017).

As it was stated in Ministry of National Education's School-Parents Union's Regulation, "In order to realize integrity between school and parent, to ensure communication and cooperations between parent and school, to support education and training developing activities and to meet obligatory needs of school and education and training for the students having lack of financial opportunities, unions those have no legal entity are established within the bodies of schools" (Ministry of National Education Regulation, 2012). Due to the fact that school-parents unions those are operational in the school dependent on Ministry of National Education, are consistently and effectively in communication with parents, they can easily perform warnings about wrong behaviors and awareness and developments of both parents and students regarding cyber security. Besides, these unions have power to undertake an important task about ensuring participation in these activities for parents and to realize awareness activities for parents.

One of the important basic units of social culture is religious values. It can be said that loving people and respect are the common elements of almost all religions. If we love people, and respect their ideas, choices and preferences, we create a peaceful Living

environment. In case of a contrary situation, disorder, crime, injustice and violence occur in the society. For this reason, religious values in the lives of societies, are security and peace elements in material and nonmaterial aspects. These are also important factors in creating culture. Transferring these values from one generation to another has importance in terms of both existence of the society and culture and peace. But if digital environment behaviors are transferred to students by matching with religious values, it can be said that cybercrimes can be prevented in a big scale.

Another subject that is stressed as a strenght in SWOT analysis, is the easiness of preparing required measurement tools to determine and to assess cyber security awareness before and after training to be given. Also practicing these tools in central examinations for wide masses, is possible in the system of Ministry of National Education. Teachers have occupational knowledge and skill about measurement and assessment subjects. For this reason, it is predicted that there will be no problem about using measurement and assessment tools. Besides, there are many examination realized by Ministry of National Education centrally. Open Education Secondary School, Open Education High School, Open Education, Religious Vocational High School and Occupational Open Education High School examinations, Primary School and Secondary School Scholarship Examination, e-Examination for Motor Vehicle Drivers Trainees and central examinations can be given as examples (Ministry of National Education, 2019).

Existence of various resources to be used and developed to create cyber security awareness, was also stated amongst strengths. In the webpage of Education Informatics Network (EBA) that was developed by Ministry of National Education, contents those were developed by teachers, safe internet and social media use, informatics safety, personal safety are presented under various titles. To make the subjects permanents, animations, drawings, pictures and games are also used in addition to direct instruction (EBA, 2019a). Besides, there are web pages those were prepared for different age groups by Information and Communication Technologies Authority (BTK) (GüvenliÇocuk, 2019; Güvenli Web, 2019; İhbarweb, 2019; İnternet Yardım, 2019). It is also possible to encounter with webpages where these types of informing resources were given by anti-virus development companies (Eset, 2019; Kaspersky, 2019a). These webpages are updated consistently by experts, teachers, academicians, cyber security and informatics experts.

Existence of sufficient human resources those have knowledge and skill to have tasks in all activities, projects and works those were realized and to be realized about cyber security and proper use of social media, is amongst strengths. Today when cyber wars, cyber-attacks and hence cyber security come to the front, the number of teachers, academicians, informatics experts, psychologist, psychiatrist, nongovernmental organizations and police department employees those support to raise awareness of

children and youth for cyber security and to direct them to the occupations related with cyber security, cannot be underestimated.

3.2. Weaknesses

1) Low level of awareness of teachers about cyber security
2) Low level of absence of awareness of teacher about internet ethic knowledge.
3) Preferring weak passwords.
4) Using non-licensed softwares.
5) Lack of public service ads.
6) Making telephones used by others.
7) Shared internet use.
8) Lack of rules of good manners.
9) Not knowing /no paying attention for privacy of persons and personal information concepts.
10) Existence of e-mail accounts those are not used actively.
11) Keeping cyber awareness posts on school boards for a short time.
12) Not performing two factor authentication while entering into accounts.
13) Lack of keeping social media literacy and ethic subjects in teaching programs.
14) Lack of coordination and cooperations between organizations.
15) Lack of awareness and knowledge about rights and responsibilities in the scale of student- teacher- school manager- parent.
16) Low level of using social media platforms by teachers and student for educational purposes.
17) Insufficiency of auditing content in social media use.
18) Lack of definitions of occupations related with social media and education and directing.
19) Having no place in legislations about penalties in social media platforms those are correspondences of crimes made in real life (The content of current legislation is to prevent behaviors those are considered as crime in social media).

According to statement from teachers taking place in workshop groups, there are complaints from students in Ministry of National Education regarding that teachers reveal weakness about cyber security. A part of teachers have behaviors those are wrong and calling danger such as interesting with their personal mobile phones for a long time during courses, opening computers taking place in teachers' lounge for use of students without auditing, leaving from these computers by not making safe exit from personal accounts those are entered with passwords, not coding Private files and folders. These behaviors may cause harm for organization or teachers by having benefit from security gaps of some students. In addition that social media use increases, unauthorized shares for photograph and video shots in classroom and school by teachers and students come to

the agenda. Against this situation, Ministry of National Education published a public mandate in 2017 to prevent negative results. These statements were given in Social Media Public Mandate (Ministry of National Education Law Services General Directorate, 2017); " Information is received by out Ministry regarding that images of activity, actions and situations those are performed during courses and free times in schools, are taken by students, teachers and managers in our schools and organizations, voices are recorded or video shots are taken; and these ones are uploaded on internet web pages later and shared in social media environments. Informing shall be ensured regarding that sharing all types of voice, text, image and video records on internet or on different digital or pressed environment regarding persons by students having education and all personnel of Ministry of National Education working in schools or organizations by province, district, school or organization managers, are conflicting with the Constitution, international contracts and the Law numbered 1739; and these actions are regulated as crime in Turkish Criminal Law and required measure to prevent these situations will be taken. Besides, required legal proceedings will be initiated within the frame of related legislation regarding the ones those are determined as they upload and share all types of voice, image and video records those will have negative effects on psychological and social aspects of these persons, on general network environments and the Ministry will be informed about the results." In addition that this and similar legal regulations, it is an important subject to support teachers about cyber security with in-service trainings. Besides, it is required to place cyber security subjects sufficiently in course contents of Faculties of Educational Sciences. When course contents of faculty of educational sciences those were updated n 2018, are examined; it has been seen that cyber security subject was given in basic level in Internet Ethic and Security course that is given in Computer and Instructional Technologies Education Department. In Informatics Technologies course given in other departments, safe internet use takes place just as a sub-title subject (The Council of Higher Education, 2018). It is required to ensure that cyber security subjects those covering required information and skills for teacher candidates, are placed in syllabus with more details and for a longer period.

Lack of knowledge regarding creating a strong password, is also another important factor in cyber security gaps. The password is an important weapon ensuring our safety in internet environment. It is required to stress this fact for the users. Besides, we should learn how to use lineaments, retina and fingerprint those we have naturally, as passwords. We should prefer two stages password entries in case on entering internet web pages. If we cannot produce password, we should take assistance from professional web pages those were prepared about this matter.

Using licensed operating system and anti-virus in the devices we use to enter to internet, is an important measure to be taken again various cyber threat. Individuals generally avoid using licensed software due to high cots. This situation causes cyber

security for both individuals and corporations. Some education institutions are taking steps about removing this problem with collective license contracts.

Istanbul has wide opportunities about delivering public service ads to wide masses. On vehicles and areas those are used by millions of people every day such as bus, minibus, metro bus, metro, tram, marine transportation, airports and stops, public service ads can be used for awareness of cyber security. One part of the workshop participants addressed insufficiency of these public service ads.

One part of the teachers who participated the workshop, mentioned that the students share their personal mobile phones or internet connections with their friends. Mutual used mobile phones and internet connections are amongst important factors threating personal cyber security. Measures such as avoiding mutual uses expect very needed conditions, not to share passwords in case of using mutually, preventing to reach applications and files with passwords, should be taken. If password is shared, it should be changed immediately.

Many businesses offer free publicly available internet connection services under the name of customer satisfaction. The biggest threat for such connections is the ability of a hacker to positioning himself/herself between you and the port. In other words, instead of communicating directly with the access point, you send your information to a hacker who is forwarding them to another location. Hackers can easily distribute malicious softwares using a publicly available unencrypted connection (Kaspersky, 2019b). Use of such links should be avoided unless it is very necessary.

Internet ethics and rules are a set of rules those should be followed while using various sites and social networks. The use of internet without knowing these ethical rules and internet ethics, brings a large number of cybercrime, criminals and victims. Ethical rules and internet ethics are important topic of cyber security training. The ability of children and young people to have sufficient and accurate information about internet ethics and rules can be related with providing rules of good manners. Individuals who grown up rich in terms of human, cultural, global and religious values will use these acquisitions into behavior in every real and virtual environment. In this sense, it is important to have Rules of Good Manners course in the curriculum. In some schools, it is covered in the scope of Guidance course. Some schools, with the participation of non-governmental organizations and experts invited to the schools, teach rules of good manners. The Character Education project in the light of values initiated by the Uşak National Education Directorate in 2015 can be given as an example to these studies. Within the scope of this project, it is aimed to explain one of our national and spiritual values every month (and to keep them alive in schools (Uşak Directorate of National Education, 2015). Since 2011, Antalya Directorate of National Education has been carrying out values education activities supported by workshops, projects and in-school and out-of-school practices (Antalya Directorate of National Education, 2017). With such practices, it will

be ensured that children and youth learn both the rules of good manners and their traditional values and carry what they have learned into cyber space.

Another important weakness is that especially children and youth cannot be aware of personal information and private information concepts. They sometimes share their personal or private information and sometimes others' personal or private information with everyone on internet. These shares both constitute a crime factor and give opportunity to swindlers and cyber bullies. In addition, all internet shares, comments and likes, called digital footprints, may come across children and youth as a negative factor in business and academic career planning. According to recent researches, 29% of university admissions officers search candidates on Google and 31% of them visit students' social media profiles. In employments, it is stated that the candidates are frequently consulted on the internet to evaluate how they look at Google (ekoruma, 2018). Therefore, the concepts of personal information and privacy should be thought to children and youth and the effects of positive digital footprint should absolutely be explained.

An important situation that is seen from time to time, is to use inactive e-mail accounts for illegal or unethical works as a result that this e-mail address is out of the use of that individual without his/her knowledge and being used by another person. For example, Microsoft closes accounts those are not used actively for more than 5 years. Closed account names can be used to open new accounts (Kayhan_N, 2018). Individuals should be informed about this.

According to the teachers those participated to the workshop, posters and banners about cyber security those hang on school boards are collected in a short period. It is not possible for students, parents and teachers to benefit from these visuals sufficiently. However, these boards can be used for multi-purpose. Successful students can be announced on these boards. Colorful and impressive shares can be done to raise awareness on any subject. Such shares are both interesting and can create funny learning environments (Red17, 2017). Teachers should be encouraged to use the boards more effectively in schools, and in some cases parents should be directed to these boards. The most important task in this regard belongs to the school administrators.

It is recommended to use two-stage authentication entries for access to environments with a high level of private information such as social networks and e-mail accounts. Against any password theft, the user is warned by sms as a guarantee and it is ensured to log in with another instant password. The purpose of sending an instant password is to ensure that the person who will log into the system is the right person. Individuals do not use this staged entry because they sometimes do not know and sometimes it takes time. In entries to virtual environments such as Facebook, Twitter, Instagram, LinkedIn, Snapchat, Reddit, Pinterest, Tumblr, Slack, Dropbox, Evernote, Pay Pal, IFTTT, LastPass, Yahoo, Apple, Microsoft, Amazon, Dashlane, Wordpress, GoDaddy, Sony

Playstation those have millions and even billions of users, it is possible to use two-stage authentication (Griffith, 2019).

The fact not having a course on the proper use of social media in it is one of the major disadvantages of educating children and youth about the subject. According to the workshop participants, this situation has an important place among our weaknesses. In the Turkish National Education System; Information Technologies and Software courses are thought as elective courses at primary school level. In this course, cyber security issues are quite superficial and are grouped under a few titles (EBA, 2018a; EBA, 2018b; EBA, 2018c; EBA, 2018d).The same course is thought as a compulsory course in the 5th and 6th grades of secondary school. In the two units of the course, some subjects of cyber security are tried to be explained (EBA, 2018e; EBA, 2018f). Computer Science course is thought as compulsory in some high schools and elective in others. This course is divided into units as Setup 1 (EBA, 2017) and Setup 2 (MEB, 2017), in the first setup, Ethical, Security and Society subjects take place. In primary, secondary and high school levels, it is inevitable that the courses which have the knowledge and skill acquisitions under the name of Cyber Security or another should be included in obligatory programs. In some countries, initiatives have started about this matter. For example, in Israel, in collaboration with the Ministry of Education and the army, it has been decided that cyber security issues are thought in 20 high schools throughout the country (Cyber Bulletin, 2015). The UK has developed a digital training program called Cyber Discovery Program with a budget of £ 20 million to increase the interest in cyber security among young people. Within the scope of the program prepared for online and offline problems faced by young people aged between 15 and 18, young people receive training against fictional hackers (Cyber Bulletin, 2017a). At Purdue University Northwest in the USA, a half-million-dollar was funded for the students for the preparation of a curriculum about cyber-security. With this allowance, the authorities stated that they will raise the awareness of high school students about cyber security and encourage them to think about a career in this field (Cyber Bulletin, 2017b).

There are institutions and organizations in Turkey operating about cyber security and cyber security training. Information Technologies And Communications Authority (BTK), Cyber Security Council dependent to BTK, Telecommunications Communication Presidency (TİB), National Cyber Events Intervention Center (USOM) dependent to TİB, Digital Turkey Platform, Turkish Armed Forces Cyber Defense Center Presidency, Police Department for Anti-Cybercrimes, HAVELSAN, ASELSAN, Istanbul Metropolitan Municipality Art and Occupation Training Courses (İSMEK) and Public Education Centres (HEM) and TÜBİTAK BİLGEM Cyber Security Institution, Information Technologies and Internet Security Association (BTİDER) can be mentioned amongst the most wellknown institutions with their works about cyber security and trainings. Besides, Istanbul Commerce University, Istanbul University- Cerrahpaşa, Istanbul City University, Marmara University, Kadir Has University and Bahçeşehir University are

some of the universities in Istanbul and those have undergraduate and postgraduate programs about cyber security. In 2019, Ministry of National Education and Presidency Defense Industry Department signed Occupational and Technical Education Development Cooperation Protocol. With this protocol, it is aimed to train teachers and to improve capacity in many subjects and areas including cyber security (Akşam, 2019). On the other hand, BTK Academy provided certificated educations to 1872 students within the scope of Summer Technology Camp in 2019 on digital issues, including cyber security (BTK, 2019). The Secure Internet Truck, which was launched in cooperation with BTK and BTİDER, visited some schools in Istanbul in 2018 and tried to inform the students (BTİDER, 2018). Turkcell, one of Turkey's leading communications companies, organized trainings in order to raise new cyber security experts for Turkey in last 3 years. In 2019, 24 students received cyber security trainings for 10 days (Sabah, 2019). According to the participants of the workshop, there is not enough coordination and cooperation between these institutions and Ministry of National Education to realize cyber security education and awareness activities. The coordination and cooperation of the people, institutions and organizations that use IT systems and infrastructures will increase the impact of cyber power. International cooperation and coordinated action are also needed to detect and counter attack in cyberspace (Şenol, 2017).

In social media, there are problems especially sharing personal and private information. These shares can be done not only by children and young people but also school managers, teachers and parents. After some complaints, Ministry of National Education tries to prevent unauthorized and improper shares with Social Media Use in schools with public mandate named Law Services General Directorate. Having shortcomings about sharing private and personal information of other people and individuals, unauthorized shares and penal sanctions, was stated amongst weaknesses by the participants of the workshop.

Another important subject that was pointed by the teachers participated to the workshop, was that not to use social media for education purposes. It was stated that teachers need to be educated and directed about this matter. Using social media for education purposes can be a tool to make social media be used by students together with teachers with correct aim and positive targets.

In social media platforms, inappropriate, illegal and dangerous content can be complained. But not everyone knows how to do it or ignores, or passes over. In this case, it is emphasized that the content shared on social media should be controlled by a system supported by a filtering or artificial intelligence technology.

Social media platforms, which have been on the agenda with their multi-purpose usage in recent years, have also led to the emergence of some professional fields. Social media expertise, social media activity expertise, social media legal consultancy, blogger, seo expertise, Google Adwords account management are some of them. In order to raise

qualified manpower needed for these new and agenda occupational groups, schools that will provide gradual education starting from an early age should be established. Because Turkey and Istanbul have more than this human potential. In order to promote and encourage these professions, informing children, young people and families, getting support from guidance counselors, and attracting attention with effective visuals such as public service ads can be mentioned. The teachers participating in the workshop pointed out that these professions were not promoted sufficiently.

3.3. Opportunities

1) Easiness for accessing internet and social media throughout the country.
2) Having individuals using social media intensively.
3) Being able to follow developments in the world regarding cyber security as the country.
4) Demonstrating threats in internet.
5) Raising awareness by pointing out material loss.
6) Bitcoin owners having need for protecting their assets.
7) Existence of potential power of Z generation.
8) Having students who have interest and skill for informatics technologies.
9) Existence of occupation and business areas related with social media and cyber security.
10) Need for protecting game accounts and YouTube channel accounts.
11) Reaching a wide mass by loading content related with cyber security on EBA an Ministry of National Education Informatics System (MEBBİS).

According to Hootsuite and WeAreSocial companies' January 2019 survey results, in Turkey with a population of 82.44 million and the number of active internet users is 59.36 million. 56 million of these people access internet with mobile devices. 84% of active internet users access the internet every day regularly. According to the same report, the number of active social media users in Turkey is 52 million. 44 million of these people connect to social media with mobile devices. The average daily use of social media in Turkey was determined as 2 hours 46 minutes. Additionally, the average number of social media accounts per capita is 9.7 (Dateportal, 2019). These figures show that internet and social media usage in Turkey is carried out at higher rates. Intensiveuse of internet and social media, creates an important opportunity for Turkey to follow developments about cyber security in the world and Turkey. Besides, it may be easier to inform individuals about dangers and threats that may be encountered in internet environment by using the power of internet and social media. This can be seen as an important opportunity for individuals to raise awareness on cyber security and to provide training on this subject.

With the cooperation between BtcTurk which is Turkey's first and the world's 4th crypto currency exchange and Istanbul University Statistics Research and Application Center, a research that is named Understanding Bitcoin, was conducted. According to the data obtained from individuals and corporate participants between the ages of 15-55, 25% of the participants answered that Bitcoin is an investment instrument. According to the research, while interest in Bitcoin continues to increase, Bitcoin goes before the stock and government bond in the future (Köse, 2019). Bitcoin, which is not subjected to the regulation, is not centered and solely aroused by computer skills, has opened a new door for cyber attackers. Bitcoin which is followed with attention by international finance environments with its market values exceeding 1 billion dollar, has been started to be subjected robberies consisting very big amounts. Attackers those deceive Bitcoin owners with sociale engineering tactics, ensured that the users reset their passwords by entering into e-mail accounts. The attackers, who also took digital wallets, received approximately $ 1.2 million dollars. Since Bitcoin transactions cannot be undone transactions and users cannot officially document this situation, it is not possible to return the stolen money to the original owners (Trendmicro, 2019). Bitcoin owners, who are the target of such a serious threat and danger and whose usage rate is increasing, will feel the need to protect their assets and to take precautions. This can be transformed into an opportunity to create cyber security awareness.

According to official data, as of May 2019, 3 million 175 thousand 285 students have education in pre-school, primary and secondary education in Istanbul (Governorship of Istanbul, 2019). These figures indicate the existence of a very serious Z generation in Istanbul. One of the most important characteristics of Z generation is that they see themselves as experts and competent in use of information technologies (Fernández, F.J., & Fernández, M.J., 2016). Social networks are also their main and natural communication platform. They can do multiple works at the same time. They decide quickly (Nagy & Székely, 2012). All of these characteristics will make it easier for decision makers and educators for Z-generation cyber security education. Delivering cyber security contents to this generation, which spends some of its time on the internet and social networks during the day, will not be difficult. Another advantage of Z generation potential in Istanbul is that these children and young people can contribute to meet the needs of educated and equipped individuals in the field of cyber security.

Nowadays when concepts such as artificial intelligence, robotic and internet of object are heard oftenly and studies are performed about this field, it is indicated that cyber security expertise, information security engineering, cyber security analyst and security management expertise occupations will be amongst the most favorite occupations in near future (Indigo, 2018). Besides, social media research expertise, distance education consultancy, forensic IT expertise, site acceleration engineering, ethical break team

volunteering, intelligence analyst, digital finance analyst and virtual service expertise will be amongst the occupations to be needed in the field of cyber security (Koyuncuoğlu, 2017). Z generation in Istanbul and the potential of talented students in the use of information technologies can be seen as important factors and opportunities for ensuring adequate employment in these important occupational areas of the future.

In January 2019 research of Hootsuite and WeAreSocial companies, the most used social media in Turkey was determined as YouTube with 92 % rate (Dateportal, 2019). Around 2 billion people visit Youtube every month. The number of videos watched in a day is 5 billion. The video duration is 300 hours per minute. The most famous Youtuber earned about $ 180 million (Yıldız, 2019). Given the financial benefit of being a Youtuber by opening a channel, the tendencies of young people and children in this direction can be considered usual. Considering this fact, many YouTube channel began to be opened in Turkey. Some of the channel owners are children. For the most popular YouTube channels in 2018 established by children, Oyuncak Avı (Toy Hunt) (5 million followers), Prenses Elif (Princess Elif) (4 million followers), Oyuncak Oynuyorum (I Play with Toys) (3 million followers), Ceylin H (1.250 million followers) and Prince Yankı (520) million followers) can be given as examples (Fulin, 2018). In addition to the security of the channel owner's personal data and content, cyber security of channel subscribers can be considered as issues that need to be raised frequently as the number of channels increases. Channel owners, who do not want to lose their followers and data, will surely make attempts about cyber security. Similarly, there will be a need for online gamers to protect their personal information and the security of the devices to which they connect to internet. It can be said that having a YouTube channel and playing online games have an important place for raising cyber security awareness and spreading to large masses.

EBA is a social education platform which is online, provided free for use of teachers, students, students of Faculty of Educational Sciences and academicians by Ministry of National Education Innovation and Education Technologies General Directorate. With this platform, it is aimed to support the use of effective materials through information technologies and to ensure the integration of technology into education. EBA has been actively used since 2012 (EBA, 2019b). On the other hand, MEBBİS was opened for use in 2007 and it is a system providing easiness to students and parents and providing technology-based and rapid transactions instead of unnecessary and long-term written documents. This system allows all the necessary procedures to be carried out in the process from the time a student enrolls in a school until graduation (Hürriyet, 2018). Due to the fact that both sites provide service for many students, teachers and academician, educational content, banners, announcements etc. shares regarding cyber security can be delivered to wide masses quickly. These sites can be considered as opportunity for cyber security.

3.4. Threats

1) Existence of fake mobile accounts.
2) Unconsciously uploading mobile applications.
3) Harmful softwares.
4) Social media use in early ages.
5) Sharing personal information unconsciously on sociale media.
6) Cyber threats on internet.
7) Corporations collecting personal information unconsciously or purposely.
8) Wrong use of Whatsapp by parents.
9) Encouraging using internet in late hours.
10) Having no password policy.
11) Not oftenly auditing internet cafes.
12) Access easiness for contents consisting sexual, violence and hatred elements for individuals those should not reach
13) Hiding negativities experienced on internet and sociale media due to pressure from the society, not sharing this kind of things with related persons and organizations.
14) Not perceiving that social media experiences are equal to the ones in real live.

One of the most important factors posing a threat to internet platforms and social media is fake accounts. Fraud and cyber bullying incidents are frequently encountered with these accounts. There are many websites that provide information on how to determine whether an account is a fake account (Computer Hope, 2018; Dodaro, 2018; Richards, 2018). Users should be informed about whether an account is a fake account.

According to January 2019 data of 2019 report of Digital that is published by WeAreSocial and Hootsuite companies, mobile application were downloaded for 2.8 billion times in total in Turkey and the amount of money spent on mobile applications is calculated as 360 billion dollars (Bayrak, 2019). Some of mobile applications those attract attention that much and used, unfortunately consist of some harmful codes those were developed for password and data robbery. Some mobile applications, on the other hand, demand interesting access and usage rights such as answering via access to contact list, images and messages. It is unfortunate that many of material and nonmaterial damages are accompanied by approving the areas in which these requests are written without being read carefully or approving them without being aware of the dangers. For this reason, mobile applications have been mentioned as a threat by many of the workshop participants.

The case that individuals start to use social media in very early ages, was considered amongst weaknesses. Social media research conducted by TotallyAwesome in 2018 demonstrates that in Indonesia, Malaysia, Singapore, Thailand and Vietnam, 90% of children aged 4-12 use social media platforms such as Facebook, Instagram and YouTube. In a study conducted by Cyber Security Malaysia with more than 8,000 primary and secondary school students in 2017, it was determined that almost half of the students aged between 7 and 9 had social media accounts. This ratio was found as 67% for children between ages of 10 and 12 (Thomas, 2019). In a study conducted in Turkey, it was determined that beginning to use social media ages interval was founds as 7-9 (Habertürk, 2013). In another study conducted with children between the ages of 6-15 in 2019, the age of starting to use the internet was found as 9 years. In the same study, it was determined that the rate of internet use among children aged 6-15 was 70% (Habertürk, 2019). Internet and social media, which are used unconsciously without sufficient education yet, can cause cyber security weaknesses by children. In particular, preparing an environment for cyber bullying, virtual exchanges and sharing of information without consent of parents are important threats to risk cyber security.

Another important cyber threat is that companies and institutions share their personal data with third parties without obtaining approval from individuals. These unauthorized shares threaten the personal safety of individuals and cause many unnecessary and tiresome advertisements and e-mails. Privacy Act that was entered into force in 2016 in Turkey, it was tried to minimize cyber threats. Every internet user and commercial company should be informed about the law.

Together with that social media becomes widespread, Whatsapp that is used much in Turkey, is a preferred virtual communication channel in teachers-parents, parents-parents communication. This information is statements of teachers and school administrators participated to the workshop. According to statements of the same participants, some parents share in groups at any time of the day and do not hesitate to share the data they are not sure. It is stated that there are many examples where personal and private information and visuals are shared. Such shares are extremely wrong in terms of both internet ethics and individual cyber security.

Some internet service providers make campaigns reducing usage fees after midnight in order to ease internet traffic. Since May 1, 2017, data use and downloading processes between 02:00 am and 08:00 am, have not been assessed within the scope of Fair Usage Quota, thanks to this, it has been provided that the users use internet more easily in nights (Hürriyet, 2017). Some telecommunication companies also have such campaigns (Turktelekom, 2019). Children and youth using internet until late hours with the attraction of this situation, can be target for cyber bullies and swindlers. Additionally, this situation provides easiness for entering dangerous games working with directives

after midnight such as MaviBalina (Blue Whale) and Mariam. For this reason, after-midnight internet use campaigns can have threating element features.

According to statements made by the participants of the workshop, many internet users around do not have a healthy password policy. Password policy is important not only for access to websites, but also for wearable technologies and internet of things that are becoming an important part of life. These policies are an important part of individual and corporate cyber security. According to the participants of the workshop, observing the students and their environment, passwords that are easy to remember are preferred. These passwords can also be broken easily. Writing passwords as note on papers those can be reaches easily by everyone and taking as note on mobile phones, are also one of the most common mistakes. Using the same password for all the accounts is also another serious mistake. For the ones having trouble to create strong passwords and to remember them, password manager softwares can be benefited (Çavuş, 2018). Sometimes, it is also seen that passwords can be shared with aclose friend, date or spouse. In addition to the passwords such as retina, face, fingerprint and voice those we have naturally, some sites use pattern passwords to enter (Şahin, 2017), it was stated that 40% of Android mobile phone owners use pattern password. According to a research made by Visa Europe in England, fingerprint scanning is the most attractive authentication method for Z generation. DNA samples and body chips are less interested (Visa, 2016). Setting up password policies individually or as a corporation has become easier with technological advances. It is possible to be protected against many cyber threats with a strong password policy.

There are more than 23 thousand internet cafes operating in Turkey and a big part of them are registered in Istanbul (Internetcafedestek, 2014). With the decision taken by BTK, even though internet cafe operating was determined by the rules, especially existence of internet cafes being operated by not being registered and insufficiency of audits are amongst important cyber security threats those attention was paid by the teachers participated to the workshop. Not following the rule for age restriction for entering into cafe, using improper programs and sites by young aged ones, not making security camera records, not using software filters or licensed anti-virus, are amongst problems in internet cafes. The participants stated opinions about making audits more oftenly.

One of the most important threats to social media security is the ease of access to inappropriate content. Since there is no age restriction in opening a social media account and there is no obligation to provide accurate personal information, the shares can be seen as uncensored and unfiltered. This situation can negatively affect children and youth psychologically and sociologically. As a measure, families can use paid or unpaid parental filters. These filter programs can be run on PC or mobile devices (dr.fone, 2019; Güvenli Web, 2017). It is important to inform parents and encourage them to use filter

programs. For this purpose, activities can be organized in parent meetings and in school-parent unions. Posters can be hung on the boards. Public service ads can be used.

Another important threat is that the negativities experienced in the internet and social media are not shared with the related authorities. Cyber bullying has an important place among these negativities and is especially emphasized in this workshop because the most of cyber bullying cases are encountered at the children at end of primary school period and at the beginning of secondary school period (KidsHelpLine, 2019). In particular, cyber bullying cases in social media are oftenly hided from relatives of cyber victims. As well as children and youth, it is obligatory that parents and teachers should be informed about measure, complaint, legal rights and responsibilities against cyber bullying cases. Lack of information is also considered as an important threat to ensure social media security.

This phenomenon is really common in children and youth and it is absolutely wrong: "This is social media, virtual world. I write whatever I like to, I share whatever I like to, none of their business. Who will see, who will know. I am free in here." This wrong opinion, unfortunately causes that children and youth commit a cybercrime and leads them to be victimized. It should absolutely be thought that internet and social media are public spaces, it is same as real life that we have legal responsibilities against individuals in public place in real life and there are crimes and penalties for crimes in social media. In New Media and Ethic Workshop result statement that was realized in 2017, these sentences attract attention: "The existence of a part thinking that making shares in social media those are not ordered, go beyond the limit, is freedom, democratic right, freedom of speech and additionally, the case that this part is becoming dominant; are very serious problems in terms of community health care and education of youth generation (TARMER Çalıştayları 1, 2017). When both these determinations and statements of the participants of the workshop are taken into consideration, it can be said that shares and behaviors of children and young people on social media and internet platforms must be gained through education and kept under control.

4. Conclusions

As a result of the Cyber Security and Proper Use of Social Media Workshop, which was held with the participants working on the proper use of social media and cyber security; the problems that were experienced in Istanbul center were put forward. The factors that may be effective in the formation and elimination of these problems were determined by SWOT analysis. In the light of this analysis, the participants proposed solutions for available problems. All the data produced within the workshop were presented to the relevant managers as a report. It is thought that obtained data is important to raise awareness of students, teachers, parents and school administrators about cyber security. It is also expected that this data will be motivational to take effective steps such as

taking place in international business unions, establishing cyber security high schools and having more cooperations with universities and NGOs and opening obligatory courses and updating curriculum of decision makers.

Acknowledgements

We thank Assoc. Prof. Dr. Özcan Erkan AKGÜN, Medeniyet University, for his contribution to the data collection process.

References

Akşam (2019). MEB ile SSB arasında Meslekî ve Teknik Eğitimi Geliştirme İş Birliği Protokolü imzalandı. Access address: https://www.aksam.com.tr/ekonomi/meb-ile-ssb-arasinda-meslek-c3r-ve-teknik-egitimi-gelistirme-is-birligi-protokolu-imzalandi/haber-826075

Antalya Milli Eğitim Müdürlüğü (2017). Antalya'da Değerler Eğitimi. Access address: http://nydurucpl.meb.k12.tr/meb_iys_dosyalar/07/14/869676/dosyalar/2017_10/23120046_DeYerler_EYitimi_KitapYY.pdf?CHK=f95134668340c5232bffebb46208c5c7

Bayrak, H. (2019). 2019 Türkiye İnternet Kullanım ve Sosyal Medya İstatistikleri. Access address: https://dijilopedi.com/2019-turkiye-internet-kullanim-ve-sosyal-medya-istatistikleri/

BTİDER (2018). Güvenli İnternet Tırı İstanbul Eyüp Asım'ın Nesli İmam Hatip Ortaokulu'nda. Access address: https://www.btider.org.tr/etkinlikicerik/guevenli-internet-tiri-istanbul-eyuep-asim-in-nesli-imam-hatip-ortaokulu-nda

BTK (2019). "Yaz Teknoloji Kampı" Sertifika Töreni Yapıldı. Access address: https://www.btk.gov.tr/haberler/yaz-teknoloji-kampi-sertifika-toreni-yapildi

Child Mind Institue (2019). How to Help Kids Deal With Cyberbullying. Access address: https://childmind.org/article/help-kids-deal-cyberbullying/

Computer Hope (2018). How do you know if an account is real or fake? Access address: https://www.computerhope.com/issues/ch001850.htm

Çavuş, N. (2018). En Başarılı ve Kullanışlı 6 Şifre Yöneticisi Program. Access address: https://www.webtekno.com/en-basarili-ve-kullanisli-6-sifre-yoneticisi-programi-h44549.html

Dalil, R. E. (2018). Protecting Children from Cyberbullying. Access address: https://www.unicef.org/egypt/protecting-children-cyberbullying.

Dateportal (2019). Digital 2019 Turkey. Access address: https://datareportal.com/reports/digital-2019-turkey?rq=Turkey

Dodaro, M. (2018). 9 Tips to Help Spot a Fake LinkedIn Profile. Access address: https://www.socialmediatoday.com/news/9-tips-to-help-spot-a-fake-linkedin-profile/515631/

dr.fone (2019). Windows ve Mac için 10 İyi Ebeveyn Denetimleri Yazılım. Access address: http://global.drfone.biz/tr/parental-controls/parental-control-software.html

EBA (2019a). Siber Güvenlik İçerikleri. Access address: http://www.eba.gov.tr/siber-guvenlik?fbclid=IwAR3eLUSqXk_kI_drNLqRDIqf_M4pRYLNDTblk2hWKdkJ5vrN9CJIkmq3Mas

EBA (2019b). Eğitim Bilişim Ağı (EBA). Access address: http://www.eba.gov.tr/hakkimizda

EBA (2018a). Bilişim Teknolojileri ve Yazılım Dersi 1. Seviye Etkinlik Kitabı (2018-2019). Access address: http://www.eba.gov.tr/ekitap?icerik-id=7324

EBA (2018b). Bilişim Teknolojileri ve Yazılım Dersi 2. Seviye Etkinlik Kitabı (2018-2019). Access address: http://www.eba.gov.tr/ekitap?icerik-id=7328

EBA (2018c). Bilişim Teknolojileri ve Yazılım Dersi 3. Seviye Etkinlik Kitabı (2018-2019). Access address: http://www.eba.gov.tr/ekitap?icerik-id=7343

EBA (2018d). Bilişim Teknolojileri ve Yazılım Dersi 4. Seviye Etkinlik Kitabı (2018-2019). Access address: http://www.eba.gov.tr/ekitap?icerik-id=7346

EBA (2018e). 5. Sınıf Bilişim Teknolojileri ve Yazılım Dersi Öğretmen Rehberi. Access address: http://www.eba.gov.tr/ekitap?icerik-id=6674

EBA (2018f). 6. Sınıf Bilişim Teknolojileri ve Yazılım Dersi Öğretmen Rehberi. Access address: http://www.eba.gov.tr/ekitap?icerik-id=6696

EBA (2017). Ortaöğretim Bilgisayar Bilimi Ders Kitabı – Kur 1. Access address: http://www.eba.gov.tr/ekitap?icerik-id=4370

ekoruma (2018). İnternetin Çocuklara Zararları ve Çocuklar İçin Online İtibar Yönetimi. Access address: https://ekoruma.net/internetin-cocuklara-zararlari-ve-cocuklar-icin-online-itibar-yonetimi/

Eset (2019). Çocuklar Güvende. Access address: https://cocuklarguvende.net/

Fernández, F.J., & Fernández, M.J. (2016). Generation Z's Tea - chers and their Digital Skills, *Comunicar*, 46, 97-105.

Fulin (2018). Türkiye'nin Fazla Göz Önünde Olmasa da En Çok Takip Edilen 14 İlginç YouTube Kanalı. Access address: https://onedio.com/haber/turkiye-nin-fazla-goz-onunde-olmasa-da-en-cok-takip-edilen-14-ilginc-youtube-kanali-849318

Güncel Eğitim (2017). İstanbul'daki okullarda adab-ı muaşeret dersi verilecek. Access address: http://www.guncelegitim.com/haber/11067-istanbuldaki-okullarda-adab-i-muaseret-egitimi-verilecek.html

Güvenli Çocuk (2019). Güvenli Çocuk. Access address: http://www.guvenlicocuk.org.tr/

Güvenli Web (2019). Güvenli Web. Access address: https://www.guvenliweb.org.tr/

Güvenli Web (2017). Ebeveyn Denetim Araçları. Access address: https://www.guvenliweb.org.tr/dokuman-detay/ebeveyn-denetim-araclari

Griffith, E. (2019). Two-Factor Authentication: Who Has It and How to Set It Up. Access address: https://www.pcmag.com/feature/358289/two-factor-authentication-who-has-it-and-how-to-set-it-up

Habertürk (2013). Sosyal medya çocukların elinde! Access address: https://www.haberturk.com/medya/haber/898522-sosyal-medya-cocuklarin-elinde

Habertürk (2019). 6-15 yaş arası çocuklarda internet kullanımı yüzde 70'leri aştı. Access address: https://www.haberturk.com/samsun-haberleri/68236354-6-15-yas-arasi-cocuklarda-internet-kullanimi-yuzde-70leri-asticocuklarda-teknoloji

Hürriyet (2017). Geceleri kota yok! 1 Mayıs'ta başlıyor... Access address: http://www.hurriyet.com.tr/ekonomi/geceleri-kota-yok-1-mayista-basliyor-40421345

Hürriyet (2018). MEBBİS nedir? MEBBİS öğretmen girişi nasıl yapılır? Access address: https://www.msn.com/tr-tr/haber/gundem/mebbis-nedir-mebbis-%C3%B6%C4%9Fretmen-giri%C5%9Fi-nas%C4%B1l-yap%C4%B1l%C4%B1r/ar-AAAFnR1

İhbarweb (2019). BTK İnternet Bilgi İhbar Merkezi. Access address:https://www.ihbarweb.org.tr/

Indigo (2018). Siber Güvenlik Uzmanlığı: Gelecekte en çok ihtiyaç duyulacak meslek. Access address: https://indigodergisi.com/2018/07/siber-guvenlik-uzmanligi/

Internetcafedestek (2014). En fazla internet kafenin bulunduğu şehir Bartın. Access address: http://internetcafedestek.com/internet-cafe-destek-haberler/item/71-en-fazla-internet-kafenin-bulundugu-sehir-bart-n/71-en-fazla-internet-kafenin-bulundugu-sehir-bart-n.html

İnternet Yardım (2019). İnternet Yardım Merkezi. Access address: https://www.internetyardim.org.tr/

İstanbul Valiliği (2019). Millî Eğitim Bakanlığı İstanbul Eğitim İstatistikleri Açıklandı. Access address: http://istanbul.gov.tr/milli-egitim-bakanligi-istanbul-egitim-istatistikleri-aciklandi

Kaspersky (2019a). Ebeveynler için İnternet Güvenliği İpuçları. Access address: https://www.kaspersky.com.tr/resource-center/preemptive-safety/internet-safety-tips-for-parents

Kaspersky (2019b). Herkese Açık Wi-Fi Güvenlik Risklerini Önleme. Access address:https://www.kaspersky.com.tr/resource-center/preemptive-safety/public-wifi-risks

Kayhan_N (2018). Microsoft temsilcisi. Access address: https://answers.microsoft.com/tr-tr/outlook_com/forum/all/e-mail-%C5%9Fifremi-unuttum/fd9bc43e-914d-491b-8e40-631becf80691

KidsHelpLine (2019). Cyberbullying. Access address: https://kidshelpline.com.au/parents/issues/cyberbullying

Koyuncuoğlu, H. (2017). İnternetteki geleceğimiz onlara emanet! İşte geleceğin siber meslekleri. Access address: https://www.cnnturk.com/ekonomi/sirketler/internetteki-gelecegimiz-onlara-emanet-iste-gelecegin-siber-meslekleri?page=1

Köse (2019). Türkiye'nin Bitcoin araştırması yayınlandı: İşte sonuçlar. Access address: https://uzmancoin.com/bitcoin-arastirmasi-turkiye/

MEB (2017). Ortaöğretim Bilgisayar Bilimi Ders Kitabı – Kur 2. Access address: http://mufredat.meb.gov.tr/ProgramDetay.aspx?PID=335

MEB (2019). Merkezi Sistem Sınavları. Access address: http://www.meb.gov.tr/meb_sinavindex.php

MEB Bilgi İşlem Daire Başkanlığı (2018). Okul İnternet Siteleri Yönergesi. Access address: http://mevzuat.meb.gov.tr/dosyalar/1958.pdf

MEB Hukuk Hizmetleri Genel Müdürlüğü (2017). Okullarda Sosyal Medyanın Kullanılması. Access address: http://mevzuat.meb.gov.tr/dosyalar/1833.pdf

MEB Mevzuat (2012). Millî Eğitim Bakanlığı Okul-Aile Birliği Yönetmeliği. Access address: http://mevzuat.meb.gov.tr/dosyalar/1532.pdf

Nagy, Á., & Székely, L. (2012). The basis and the structure of the tertiary socialisation field and the "Youth-Affairs" as an autonomous area. *Acta Technologica Dubnicae*, 2(2), 1-18.

Piercy, N., & Giles,W. (1989). Making SWOT analysis work. *Marketing Intelligence & Planning*, 7, 5–7.

Red17 (2017). The Importance of a Good Notice Board in the Classroom. Access address: https://www.red17.co.uk/blog/notice-boards-in-the-classroom/

Richards, P. (2018). When someone makes fake social media profiles is it possible to find out who they really are? Access address: https://www.quora.com/When-someone-makes-fake-social-media-profiles-is-it-possible-to-find-out-who-they-really-are

Sabah (2019).Türkiye'nin yeni nesil siber güvenlik uzmanları Cyber Camp'ta yetişiyor. Access address: https://www.sabah.com.tr/ekonomi/2019/01/31/turkiyenin-yeni-nesil-siber-guvenlik-uzmanlari-cyber-campta-yetisiyor

Samejima, M., Shimizu,Y., Akiyoshi, M., & Komoda, N. (2006). SWOT analysis support tool for verification of business strategy. In IEEE international conference on computational cybernetics, 1–4.

Shariff, S. (2015). Defining the lines on cyberbullying: navigating a balance between child protection, privacy, autonomy and informed policy. Access address: https://www.unicef-irc.org/article/839-defining-the-lines-on-cyberbullying-navigating-a-balance-between-child-protection.html

Siber Bülten (2015). İsrail'de siber güvenlik lise müfredatına girdi. Access address: https://siberbulten.com/uncategorized/israilde-siber-guvenlik-lise-mufredatina-girdi/

Siber Bülten (2017a). İngiltere'den siber eğitim için 1.9 milyar sterlinlik bütçe. Access address: https://siberbulten.com/uluslararasi-iliskiler/ingiltere/ingiltereden-siber-egitim-icin-2-milyar-sterlinlik-butce/

Siber Bülten (2017b). Siber müfredat için yarım milyon dolar. Access address: https://siberbulten.com/uluslararasi-iliskiler/abd/lise-ogrencilerine-siber-guvenlik-mufredati-hazirlanmasi-icin-yarim-milyon-dolarlik-butce-ayrildi/

Şahin, Y. E. (2017). Android telefonlardaki desen kilidi beş denemede kolayca kırılabiliyor. Access address: https://www.gzt.com/bilim-teknoloji/android-telefonlardaki-desen-kilidi-bes-denemede-kolayca-kirilabiliyor-2601690

Şenol, M. (2017). Türkiye'de siber saldırılara karşı caydırıcılık. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* Cilt:3, No:2, 1-9.

TARMER Çalıştayları 1 (2017). Yeni Medya ve Etik. Access address: https://www.aydin.edu.tr/tr-tr/arastirma/arastirmamerkezleri/tarmer/PublishingImages/Pages/yayinlar/SOSYAL%20MEDYA%20VE%20ET%C4%B0K%20K%C4%B0TABI.pdf

Thomas, J. (2019). Children and social media. Access address: https://theaseanpost.com/article/children-and-social-media.

Trendmicro (2019). Bitcoin Güvenli mi ve Nasıl Korunmalı? Access address: https://www.trendmicro.com.tr/newsroom/pr/bitcoin-guvenli-mi-ve-nasil-korunmali/index.html

Turktelekom (2019). Selfy'den Bol İnternetli Geceler Kampanyası. Access address: https://bireysel.turktelekom.com.tr/mobil/web/kampanyalar/sayfalar/faturali/selfy-bol-internetli-geceler-kampanyasi-faturali.aspx

Uşak Milli Eğitim Müdürlüğü (2015). Değerler Işığında Karakter Eğitimi Projesi. Access address: https://usak.meb.gov.tr/www/degerler-isiginda-karakter-egitimi-projesi/icerik/4360

Wilson, R. M., & Gilligan, C. (2005). Strategic marketing management: Planning, implementation and control. Routledge.

Visa (2016). Z Kuşağı şifre girmek yerine parmak iziyle ödeme yapmak istiyor. Access address: https://www.visa.com.tr/visa-hakkinda/basin-odasi/z-kusagi-sifre-girmek-yerine-parmak-iziyle-oedeme-yapmak-istiyor-1235031?returnUrl=/visa-hakkinda/basin-odasi/listing?tag=inovasyon

Yıldız, B. (2019). Youtube İstatistikleri. Access address: https://www.brandingturkiye.com/youtube-istatistikleri-guncel/

YÖK (2018). Yeni Öğretmen Yetiştirme Lisans Programları. Access address: https://www.yok.gov.tr/kurumsal/idari-birimler/egitim-ogretim-dairesi/yeni-ogretmen-yetistirme-lisans-programlari