RedFame

Journal of Education and Training Studies
Vol. 6, No. 11a; November 2018
ISSN 2324-805X E-ISSN 2324-8068
Published by Redfame Publishing
URL: http://jets.redfame.com

Social Networks as a Learning and Teaching Environment and Security in Social Networks

Nilgün Tosun

Correspondence: Nilgün Tosun, Assoc. Prof. Dr., Trakya University, Faculty of Education, CEIT Department, Edirne, Turkey.

Received: October 18, 2018 Accepted: October 27, 2018 Online Published: November 29, 2018

doi:10.11114/jets.v6i11a.3817 URL: https://doi.org/10.11114/jets.v6i11a.3817

Abstract

Technology is in a constantly evolving and changing structure since the existence of mankind. Because of this dynamic structure, technology fulfills a number of functions such as facilitating people's lives, time, profit from work, profit from cost, making life more enjoyable. At the same time, technology is used in all areas of life, and it also causes changes and transformations in these areas. Education is one of these areas, perhaps the most important, that technology affects. The hunter society, written with nails, made an important step with the paper's invention, and the written documents were moved from the stones to the books. The invention of computers and the internet has also opened an important milestone in human history and education. In the beginning, the course contents loaded on storage units such as floppy disks, CDs, DVDs were used by the students and teachers, computers were included in the education systems. During periods when we have not yet met with the internet, computer-assisted education has found a large place in many educational institutions and in the curriculum of education level. The development of information Technologies led to widespread use of the internet over time, and shortly thereafter examples of use in education began to increase. Computer-assisted education has also led to the rapid transition of education through internet-supported education, along with the different demands of the network society's individuals. Users are not satisfied with the internet environments where only reading authority is available, and more and more active and interacting requests have come to the agenda. Beyond reading, social networks that make it possible to comment, create content, upload/share/view images, upload video/audio files, and make video, text and voice calls have become popular for users. Social networking platforms where users interact with the environment or with other users in the environment have been attracted by the diversity of user profiles, the usage rates and durations, and the easy and versatility of accessibility. Because of these features, studies on the use of social networks in the field of education to support learning and teaching have also been accelerated and diversified. Social networks can also contain some security issues because they are huge platforms where billions of users are together. Having information about security issues as little as possible, what to do when they are encountered is important for the continuity of learning and teaching. The aim of this study is to demonstrate the importance of social networks, education, learning and teaching influences, possible security threats to be encountered in social networks, and measures to be taken. It is hoped that working in this context will shed light on the work of learners, teachers and decision makers on the subject.

Keywords: social networks, learning, teaching, security in social networks

1. Introduction

The constant and rapid change of technology causes a number of changes in the areas it influences as well. Education is one of those areas where technology has an influence on. Many new technological products directly influence the way that individuals learn and teach, their environment, their speed and time. The person who once wrote with nails in stone tablets has begun to learn and teach on virtual platforms with the wide possibilities that the Internet provides today. Among these virtual platforms that are used for learning and teaching purposes, social networks are widely used. Thanks to the facilities such as easy and free membership, sharing of all kinds of media, comments and likes feature, private messaging, and so on, social networks continue to become ever-increasing virtual platforms. According to the January 2018 figures of the Digital in 2018 report, the number of active social network users in the world is 3 billion 196 million. With 2 billion 167 million users, Facebook is the most used social network in the world. Following this, Youtube ranks second with 1½ billion users and Whatsapp third with 1 billion 300 million users. The number of users on Twitter, however, is 330 million Global Digital Report (2018). In social networks where the number of users is so high, there is undoubtedly a remarkable degree of sharing and movement traffic. According to the 2018 figures of Cumulus Media company, within 1 minute,

there are 973 thousand entries on Facebook, 481 thousand tweets on Twitter, 4.3 million videos watched on YouTube, 2.4 million snaps on Snapchat, 25,000 GIFs on Messenger and 38 million messages sent on Whatsapp. This data and more can be seen in Figure 1.

Figure 1. This is WhatHappens in an Internet Minute 2018 (Descardins, 2018)

Safety is crucial for schools that have a traditional educational environment. According to Bucher and Manning (2005), a safe school is where students, teachers, administrators and other employees live in peace all around the school, one group is not superior to the other groups, and students, teachers, administrators, other employees, parents and visitors interact positively. Because of these schools, students are successful. In safe schools, students can freely increase their knowledge in peace and develop their skills.

Some of the social networks, some of which have billions, some of which have millions of users, are used as formal or informal learning environments. The use of social networks in formal learning environments remain lower than in informal learning (Chen and Bryer, 2012). One of the most prominent examples of the use of social networks formally is the pages that educational institutions start on social networks. In these pages, institutions can share general information about the institution, also academic and administrative announcements, news, and allow their followers' comments and shares. It is possible to see the official pages of many educational institutions that take into account the advantage of the high number of users on social networks as Facebook, Twitter and Instagram. According to the report of BoomSocial (2018), one of the most important institutions calculating social network statistics, Oxford University with 3.568.220 followers and Cambridge University with 2.105.586 followers are ranked as the top two of the most active educational institutions in the world. Another example of the formal use of social networks in education is the course management system such as Blackboard, Sakai, and Moodle, and the limited use of some social networking features integrated into these systems (Chen and Bryer, 2012). MOOCs, which we have heard frequently in recent years, have also social networking features. Anyone can register to these platforms and get training in the field they want. In MOOCs, although the content of the course is shared in almost all formats for students, with tools such as forums, blogs and in-system messaging, learner-teacher and learner-learner interactions are maximized. UDEMY, Coursera, Edx and Khan Academy are just a few of the best known MOOCs in the world.

Informal use of social networks in education is more common. One of the best examples of such use is the social networking groups or communities. Generally, there may be communities where people who are interested in the same subject come together and share, or a group opened by a faculty member for his/her course. In some social networks, it is possible to access, upload and comment on videos that teach how to do or to give theoretical information. In social networks on video sharing, there are also private channels for individuals or institutions. There are also social networking sites with visual archives, such as photographs or pictures, and most of which are shared with users for free. Some of the social networks allow especially competent and experienced people in the business sector to come together and share with those who are employees or future employees in that field. It is also possible to see the examples of many instructors and administrators of educational institutions who provide information and update information to their followers through their social network accounts.

The security of social networks is also as important as the security of schools as traditional educational settings. Considering the number of users and environment traffic, security problems are likely to occur in social networks. Hence, in addition to how to implement learning and teaching in social networks, issues regarding the provision of individual, institutional and environmental security are on the agenda. If individuals know the possible threats they may face in social networks, what precautions they should take against them, and what they need to do when they encounter

a threat, and if relevant institutions take the necessary precautions and train their stakeholders on this matter, social networks can turn into safe learning and teaching environments.

Based on this fact, the information to be presented in this study is thought to be enlightening for decision makers and administrators in the field of education, as well as learners and researchers.

2. Method

This research is a descriptive study in the screening model, which aims to provide information on the importance of social networks as a learning and teaching environment, the risks that may be encountered in these environments, the precautions to be taken against these risks, and things to do when the danger is encountered.

The following questions were asked in the study:

- How is the use of social networks as a learning and teaching environment realized? What are the positive reflections?
- What are the dangerous situations that can be encountered in social networks?
- What precautions should be taken for dangerous situations that may be encountered in social networks?
- What should be done when a dangerous situation is encountered in social networks?

In order to respond to the research questions, a review of literature was conducted about the subject. The data obtained are mainly from electronic sources. For this purpose, related journals, e-books, thesis, blogs, articles, bulletins, reports and interviews were referred. Ultimate attention is paid for resources to be recent and as a result, all sources that were utilized were picked from the last 5 years. Key phrases of literature review are as follows; social network using in education, learning in social networks, teaching in social networks, and security in social networks.

Social Networks as a Learning and Teaching Environment

Social networks are preferred and used by many people because they are open and free platforms without distinction of personal characteristics such as age, gender, nationality, religious belief, marital status and education level. While everyone's or organization's purpose of using social networks can be different, it is possible to benefit from social networks for all types of education whether it is traditional or remote, formal or informal.

The use of social networks for learning and teaching purposes has been pursued for a while through different examples. One example is the social network groups. Sefton-Green (2004) states that by becoming a member of communities or groups in social networks, many people perform self and informal learning, and play the role of both a learner and a teacher in such platforms. In their study, Trinder, Guiller, Margaryan, Littlejohn, and Nicol (2008) determined that students create communities through social networks such as Myspace, Bebo, Youtube, Wikipedia and Flickr, by this means that they are in more communication, they can share and they can even prepare course materials with each other. Some companies try to identify the best performances by communicating with their employees, educating them and using the gamification approach through social networks such as Linkedin and Youtube (Bersin, 2011). Considering the fact that a significant part of the learning takes shape by visualizing, managers and employers prepare short videos about an information or skill that needed to be learnt about work or lessons. They publish these videos on YouTube for employees / learners to access and learn. Youtube also includes millions of videos that are personally published and explain how to do an application (Arshavskiy, 2014). Another example is Youtube EDU. YouTube EDU, a YouTube application with high quality educational content, contains videos that can be used in a classroom environment. Youtube for Schools is a platform that allows schools to access content only in YouTube EDU by limiting non-educational content on YouTube. As for YouTube/Teachers, it is a platform which provides information about how teachers can use YouTube in the classroom (Arslan, 2015). Skype has just released a version that can only be used in education. This version of Skype can be accessed from education.skype.com. In this platform, lessons are given, common lessons and speech classes can be created (Kazancı and Dönmez, 2013). Twitter, however, is used for instant information updates and feedback (Arshavskiy, 2014). Linkedin is one of the most used social networking platforms in informal education. Linkedin is a platform that brings together professionals and fellows and allows people to connect with each other. The informal tips, important information or techniques provided by many professionals in the field are more than what is given in the classroom (Arshavskiy, 2014). With Flicker, known as a photo sharing platform, students can gain many skills, such as digital literacy, visual arts, and language skills. Creating a virtual museum tour, teaching the words, teaching the use of digital cameras, brain storming about digital storytelling and painting, are some examples of using Flicker class activities inside or outside the classroom (Gülbahar, Kalelioğlu and Madran, 2010). In many blogs, students can keep multimedia records, and can add pictures, audio and video into written texts. At certain times, discussion hours can be arranged and students can be allowed to comment on each other's blogs (Kist, 2012).

There are many studies in the literature about the use of social networks as a learning and teaching environment and

their positive reflections. Most of these studies have investigated the effects of Facebook, Twitter, Youtube and Edmodo social networks on learning and teaching on secondary school, high school, undergraduate and graduate students. According to the results of this research, students participated in all activities that required and did not require cooperation within the course plan. It was reported that academic success and motivation increase in the students. Students also expressed positive views on the use of social networks in mobile learning. In some studies, it was observed that in social networks, university students discussed university-related issues as well as were actively involved in various university communities. There is also research that reveals that Facebook is more interesting to students than the classroom environment and that students are more actively involved in social networking discussions, and that Facebook offers a rich learning environment and process, with teachers sharing lesson materials and for other reasons. Some of the important results obtained from these studies are that social networks help students develop written communication skills and support the increase of vocabulary in mother tongue and foreign language, that social networks enable communication between learners and teachers more effectively and quickly and provide a broad source of information. In some studies, students also expressed satisfaction with sending their assignments via social networks, taking an exam, answering survey questions, and receiving feedback quickly. They stated that they were happy to be able to access the course materials and to communicate with their teachers and friends wherever and whenever they wanted, as well as to get help from social networks to prepare for their exams and their homework or projects. Some other research shows that social networks support informal learning (Alcantar, Ballesteros, Torres, Padilla, and Barajas, 2016; Alkan and Bardakçı, 2017; Al-Mukhaini, Al-Qayoudhi, and Al-Badi, 2014; Asberg, 2013; Buzzetto-More, 2012; Chvanova, Khramova, Pitsik, and Hramov, 2016; Clothey, 2016; Dere, Yücel, and Yalçınalp, 2016; Dhanhani, Mizouni, Otrok, and Rubaie, 2015; James, 2014; Klimova and Poulova, 2015; Komninou, 2018; Lavy, 2015; Messner, 2009; Mora, Pont, Casado, and Iglesias, 2015; Moolenaar and Daly, 2012; Pettenati and Ranieri, 2006; Rivero, 2011; Sánchez-Gómez, Iglesias-Rodríguez, and García-Peñalvo, 2017; Schachter, 2011; Simonova and Poulova, 2015; Wang, Chen and Liang, 2011).

This and many other studies in the literature reveal the benefits of using social networks as a learning and teaching environment. Social networks are likely to continue to be part of education for a long time, because of the increase in the number of social networks and users, easy access to social networks, and that social networking requires no special training. For this reason, security in social networks is a matter of importance.

Dangers Threatening Security in Social Networks

In addition to its many advantages and benefits, social networks also contain some potential dangers. It is important for social network users to know these risks and their scopes in order to take security precautions. Possible threats that may be encountered in social networks are as follow:

*Fake Accounts:*This is one of the most common threats in social networks. Fake account holders sometimes use credentials that do not actually exist. After they have been in contact with the target for some time and earned their trust, they are in demand for financial gain. Such as asking for debts, phone credits, bank account numbers, or credit card information. Some of those who open accounts with counterfeit information can use attractive photographs to propose a meeting with the target person. In this way, they may cause physical or material damage to the target person. Sometimes, a fake account is opened using the credentials of a recognized and famous person. Shares are made on behalf of this person or material requests from followers are made. People can also open fake accounts to get the information they can not access with their real identity. False accounts can sometimes be used to organize and initiate illegal acts. Feeling more free and acting comfortably, sexual harassment and cyber bullying can be listed among the reasons for opening fake accounts (Altındağ, 2015). Being able to follow the old lover or a friend who is not liked or in good terms with, hiding from family or relatives, making extra use of internet games, and expressing political opinion more easily are among the reasons for opening a fake social network account (Şahin, 2016). Fake accounts, also called bots in recent years, are often mentioned. Boat followers are fake followers, which look like real followers, created by computer software and driven by a system (wmaracı, 2018). One of the most effective ways to show a target group that a social network account is popular or safe is to increase the number of followers and likes with bot accounts. According to Dailyworld, there are 270 million fake accounts on Facebook (Dailyworld, 2017). Menczer (2018) also stated that between 9% and 15% of Twitter users can be fakes. Studies are also being conducted to determine fake accounts. Israeli and American researchers have developed a method to identify fake accounts on many social networking platforms, including Facebook and Twitter (Leichman, 2018).

Theft of Accounts: This is one of the most common social networking threats done for many reasons. Social network account hijackers can share inappropriate or illegal content through the stolen account. They can also communicate with the people in the friends list and ask them for money, credits or some private information (Lena, 2016). Account theft can be done with the feeling of enmity or harm, as well as by those who have made it into a habit or profession.

Social Malware: Briefly known as socware. With these softwares, it is aimed to capture private information such as social networking or e-mail password, bank account number, credit card, identity or home address. Any kind of information can be accessed with a link sent via the captured account of one of the friends list. Sometimes they can infiltrate devices and access the information they want, through applications loaded with fake award promises, surveys or contests (ISTR20, 2015; Rahman, 2012; Talay, 2017). Facelikertrojan is one of the most frequently heard names among malicious software in recent times. Faceliker is placed in a web browser via a website visited by a person. Then, it hacks the likes in the person's Facebook account. In other words, people like some content and pages without realizing it. In this way, developers of Faceliker bring accounts that they want to be popular or look trustworthy into the forefront (Cimpanu, 2017; EPN, 2017). Another group of malicious software that is often seen on social networks is a type of software called scareware. By convincing people of a dangerous situation that does not really exist (such as virus infection, system crashes, seizure of social network accounts), this software creates panic and then directs people to buy software that will help to get rid of this dangerous situation (Dadar, 2016; Norton Team, 2015). Another type of malicious software is Clickjacking. It is also called Likejacking. These malicious codes spread via the like buttons, especially on Facebook, become active when the button is clicked. That is, without knowing it, the operation of unknown malware is ensured (Demir, 2016). The malicious software that is running can remotely control the microphone and camera of the device connected to Facebook (OWASP, 2017).

Phishing: This is a term coined by the combination of the words Password and Fishing. It can be expressed as password catch by the fishing line or as phishing (Taş, 2018). In the case of phishing as a social engineering product, people are phished according to their interests, or the data obtained from the navigation points on the web pages they visit. Victims will be directed to fraudulent sites by clicking on links containing interesting messages or suggestions that people would not want to miss (Sırt, 2017). For example; "You have won the gift certificate from the X company.", "X company's bestselling product is almost sold out, last two products.", "You will miss free vacation if you do not participate in the survey", "Your account will be deleted if you do not change your Internet banking password." The target person is first directed to a fake web site with such messages. When the link is clicked, a form is displayed on the screen where some personal information need to be entered. For many people, when the ordinary information starts to be entered into this form, the target person is phished (Hoelscher, 2016). The most common method for phishing in social media is to open a fake Facebook page of about 60%. In addition, 71% of personal cyber attacks start with a phishing. Twitter's Direct Message feature is one of the most popular methods for phishing. (Eren, 2018). These are very important and remarkable rates and data.

Cyber Bullying: This occurs when an individual or group is intentionally and continuously trying to harm others by using information and communication technologies such as the Internet and mobile phones (Tokunaga, 2010). The target that cyber bullies can reach the most easily and can conclude their bullying is children and youngsters. Cyber bullies seduce their targets by interest, compassion, kindness and even gifts. They know the latest music and hobbies that attract children. They listen to children's problems and share their feelings. They try to break the shyness of young people by slowly incorporating sexual content into chats or by showing explicit content about sex. They can share humiliating videos on social networks. They can reveal secrets or confidential information. They can replace the victim and then write hateful or sexual comments on the victim's friends' shares or on their walls. They can act like a victim's friend, so they can gain trust and then attack the victim (Microsoft, 2018). Data from numerous studies also indicate that social media is now the favored medium for cyber bullies. 40% of cyber bullying occurs in social network sites (Cyberbully411, 2018). Cyber bullying often occurs on Facebook or through text messages (Cook, 2018).

Similar Name Fraud: Also known as make-up. They are attacks aimed at harming users by buying names similar to the names of websites used by companies. This is an attack method that attempts to steal a user's identity information by providing a web address extension similar to the actual one - with one or more characters being different (Khanse, 2016; Siberg üvenlik, 2016). For example; tweetter.com, twiitter.com, twiteer.com, twiter.com, facebok.com, yuutube.com, and so on. For make-up, the proximity feature of the neighboring letters on the keyboard is sometimes used. As in the case of Facenook.com.

Common Friends Feature: Some social networks feature the common friends feature. Through this feature, the attacker first reaches out to the friends of the person whom s/he is friends with. Then, through indirect friendships to reach the target, the attacker can access to the victim's all of the social network friends (Mashable, 2014).

Photos with GPS Features: Many people take photos and videos with smartphones or digital cameras. Some information is recorded into the captured images without the knowledge of the user. For example; whether the flash is used, lens distance, resolution, shutter speed, diaphragm, camera brand and model. This information, called EXIF, includes the geographical location information, which is also called Global Positioning System (GPS). When shared images are opened with appropriate photo editing programs, location of the person or that the person is outside home /

work can be clearly identified (Mediatrend, 2015). This can lead to problems of theft or undesired people finding your place.

Mobile Applications: According to the Digital in 2018 report January 2018 figures, the number of active users connecting to the Internet with mobile devices worldwide is 3 billion 722 million. According to the 2017 figures of the same report, the number of mobile applications downloaded worldwide is 175 billion (Global Digital Report, 2018). In the mobile applications market, where material is provided at a fairly high rate, applications that are particularly from unknown resources are a danger for users. These applications often use interesting titles such as "See which celebrity you look like", "Who searched your name in a social network", "What name they recorded you with". Before installation, there are options for users such as "Sign up with my Facebook information" or "Sign up with my email address & phone number", which aim to steal personal information. Once the user accepts one of these options, the information stealing begins (Hürriyet, 2018).

Deepfake: It means to process a photograph and mount it to a pornographic video (Sözcü, 2018). These videos are often of a sexual or humiliating nature; this is because it is used for harm or slander (Talwar, 2018). Close-up photographs shared on social networks are sufficient materials for deepfake.

Social Network Diseases: Social networks are platforms that serve various purposes in this age, which are housed in a large number of vehicles used by people of all ages, genders, professions, religions, languages and nations. The January 2018 data of the Digital in 2018 report shows the average daily use of social networking in 40 countries. According to this figure, where the users are between the ages of 16-64, the Philippines ranks first with 3 hours 57 minutes, which is followed by Brazil with 3 hours 39 minutes and Indonesia with 3 hours 23 minutes. Japan is in the last place with 48 minutes (Global Digital Report, 2018). Social networks, which take up a long time of users, lead to many health problems unless adequate measures are taken. Social network addiction is one of the most common health problems. If you have started to use social networks as a means of escape from problems, if you feel uncomfortable when you do not get into social networks, if you are trying to create an opportunity to enter, if you spend more time on social networks than you think, if the feelings of happiness, sadness and jealousy that you experience in your real relationships in everyday life have begun to emerge through relationships with these social networks, if the time spent to go to work, go out, meet with friends is left to social networks, and if they are starting to threaten your business and your relationships, then you can be called a social network addict (Erol, 2014). Another social network disease is called FOMO (Fear Of Missing Out). The most prominent features of the FOMO are the inability to resist the desire to be informed about what friends are doing on the social media, the need to constantly follow friends, feeling nervous and anxious if this is not done, and the anxiety of missing out the developments in the social network (Rodrigues, 2018; Şahin, 2018). The continuous checking and counting of 'likes' in social media is known as Like Addiction (O'Connor, 2014). Another social network disease is Photolurking. It is a disease that manifests itself through the time spent looking at people's photos for hours on any social networking platform and doing it constantly (Öztürk, 2017). Facebook Depression is expressed as a disease in which people become more susceptible to depression after sharing their frustrations via the Facebook social network (Fottrell, 2014). The inability of individuals who read and write continuous short texts on smartphones or tablets to improve their reading and writing skills is, on the other hand, known as Hidden Illiteracy disease. These people are different from those who have never attended and have not learned to read and write, in that they may read a text but not understand what they read, figure out the numbers, but may not solve the problem. Hidden illiterate people are those with diploma who know how to read and write but can not use these skills effectively in everyday life (Güneş, 2015). Hikikomori's disease is defined as a person's ability to develop communication addiction in the virtual world with the computer screen and to close himself / herself in the social environment. It is also called withdrawal or reclusion disease (Çetiner, 2015). Among the indications of this disease is the delay and neglect of all the responsibilities of one's life, and the beginning of meeting the basic physiological needs in the face of the computer.

Native Language Corruption: Some languages, including English, have begun to show corruption on social networks for a number of reasons, including fast and short writing habits, desire to share too many feelings and thoughts in little time, and pretension. Over time, a unique language of communication has begun to form in social network correspondence. Among the features of this language are the use of emoji instead of writing a word / sentence, failing to follow spelling and punctuation, abbreviating words / sentences (writing pls instead of please, bt instead of but, 4u instead of for you, gf instead of girlfriend). Unfortunately, this language occasionally manifests itself in written communications such as test papers, petitions, homework, and e-mails. This is a sign of both corruption of the native language and one of the important factors in the formation of occasional written communication problems between digital natives and digital immigrants.

Violation of Privacy: A person's private life, information, photograph, video or document is shared with everyone in the social network without the permission of the person. The seizure and recording of this information, photographs, videos

and the document without the owner's permission is also considered as a violation of the confidentiality of private life (Aslan, 2017; Demir, 2018).

Violation of Confidentiality of Communication: This occurs when records of written, verbal or visual communication between individuals are shared by one party on social networks without the permission of the other party (Tan, 2015; Yılmaz, 2015).

Measures to be Taken to Protect Against Hazardous Situations in Social Networks

Measures that can be taken for possible dangerous situations in social networks can be listed as follow:

- For social networks, passwords that are very strong and not used for another account should be generated. Passwords should be changed at regular intervals. They should never be saved anywhere.
- A two-step verification system should be used to access social network accounts.
- Social network addresses should be typed manually into the browser's address line, auto-completion should not be used.
- Devices connected to social networks must use licensed antivirus programs. This program should be kept constantly up to date.
- Devices that access social networks must use a licensed operating system and the operating system should be updated periodically.
- Devices connected to social networks should be backed up periodically.
- All devices connected to social networks should use a boot-up password.
- All devices connected to social networks should use a different screen password in addition to the boot-up password.
- Instead of unencrypted Wi-Fi to connect to social networks, personal or corporate, encrypted network connections should be used.
- If public computers or devices are to be used to access social networks, the No button should be clicked when "Do you want to save your password for the next login?"message appears on the screen.
- If a public computer or device is used to login to social networks, the "Secure Log Out" button must be used at the exit from the social network site.
- Taking into account the remote controllability with spyware, the webcam of the desktop computers should be disabled at times when not in use. The camera of the mobile devices should be covered with a dark band.
- Those who use nicknames instead of real names, or those you do not actually recognize, should be deleted from your friends list.
- One should be familiar with the privacy, security, and data-using policies of social networks.
- The privacy and security settings of social networks should be known and applied to personal accounts.
- For use as evidence of cyber bullying, interview recording programs should be used.
- Before installing applications developed for mobile devices, you should be sure which device and personal data access permissions are granted.
- You should be informed about social networking etiquette, use social networks by following it, and expect this from others.
- Inorder to avoid social network addiction, one should participate in social, cultural, artistic or sporting activities based on personal interests and skills.
- In order to spend quality time with their children, parents should make an internet and social network use agreement with their children and hang it up at a place where everyone can see at home (Güvenli Web, 2017).
- One should be informed about what acts are criminal in social networks.
- One should be informed about legal rights and what should be done in the face of criminal behavior encountered in social networks.
- Promotional messages sent via social networks should not be accepted without confirmation from the internet.
- Close-up photographs as well as photographs in perspective that will help determine the address where the photo was taken should not be shared on social networks.

Things To Do When Social Network Based Threats

Despite the current measures, one of the basic actions to be taken in case of any dangerous situation in social networks is to learn the complaints processes on social network platforms and follow these steps. Detailed information about the social network complaints process is usually found in the Help / Help Center / Complaint links on the social networking homepage. In addition to complaints to social networks, applications must be made to the relevant government agencies and organizations. For this reason, one should be informed about the process of notice and legal complaints. This is because most of the threats that are encountered in social networks are defined as crime in law and they bear penal sanctions. These processes can involve different institutions in each country. Particularly in cyber bullying cases, correspondence and sharing should never be erased, it should be recorded and used as evidence in the legal process. In addition, in a suspicious case, one can also benefit from the software to detect if a social network account is fake. Some of these are; Anywho, AllAreaCodes, Facebook Graph Search, GeoSocial Footprint, Hoverme, Identify, Linkedin, Muck Rack, Numberway, Person Finder, Pipl.com, Rapportive, Spokeo, WebMii, and WHOIS (Uzun, 2016).

3. Conclusions and Recommendations

In this research; how social networks might be used as a learning and teaching environment is tried to be explained with examples. Dangers arising from social networks, things to do against these dangers, and security methods were mentioned.

Using of social networks as a learning and teaching environment was the subject of many studies in the process of the integration of information technologies to education. Studies examined the integration of different social networks to education from different aspects, such as, effect on academic success, communication, interaction, motivation, attendance and co-operative study. As a result of the studies that are conducted on the subject of using Facebook in the Extensive Disease Management class, DiVall and Kirwin (2012) determined that students' access to class notices, online discussions, and recommended links related to classes significantly increased. In the same study, it was clarified that the highest access rate to the Facebook page was during midterm and final weeks. In the study, where Sorte and Rathod (2016) examined the effect of social networks on informal learning, they formed a Facebook group and invited their students to join in. In this group, class materials were shared and students' questions were answered. At the end of the study, it was determined that there was a significant increase in student's academic success and a significant increase in rates of passive students' interaction and questions asked by them. Delello, Mcwhorter, and Camp (2015) carried out a study in which utilization dynamics of social networks as a learning tool in university education were examined. They examined the influence of Pinterest, Facebook, Twitter, Youtube, LinkedIn, Second Life, and Skype on learning. The students stated that they were happy while they were learning in social networks, that they were better focused, and that learning with social networks was positively interesting to them. Moreover, these platforms paved the way for students to share information with each other easily, and to connect with their peers globally as well. The students stated that the classes in which social networks were utilized made more sense. Dunlap and Lowenthal (2009) examined the effects when a microblog example, Twitter, was involved in the education environment in another study. With Twitter, an environment which was qualified to support the formal education but still was an independent learning environment was established. According to the results of the study, it was suggested that Twitter shares improved the sense of a social being and collaborative abilities in students, and enabled them to interact in time. Another study conducted by Junco, Heiberger, and Loken (2010) that evaluated Twitter as the subject of the study, they analyzed the influence of Twitter on students' attendance and their grades. In the study, it was observed that the attendance rates of students who utilized Twitter increased, and the interaction between their peers and faculty members. There are studies in the literature about blogs and wikis which are accepted as social networks. For instance; Ebner, Lienhardt, Rohs, and Meyer (2010) determined that the students demonstrated positive attitudes and behaviors about the subject of utilizing a microblog for collaboration and informal learning in an academic environment; furthermore, they stated that they were happy when they utilized these social networks in a study in which they examined the effects of microblog utilization on students in informal learning. The authors of the study also emphasized the importance of the utilization of microblogs in situations such as supporting collaboration, feedback, learning through informal communication.

Studies show that social networks are utilized mostly for informal education. The lower rates of formal utilization may be due to the security and validity issues that may be experienced in the evaluation of learning in publicly available social networks. In these circumstances; the utilization of safe online examination software or hardware, or carrying examinations out on more reliable and institutional platforms other than social networks can be considered as solutions. In this circumstance, there will be a need for relevant legal regulations. Additionally, security problems arising from social networks being available to anyone such as stating real identity information not being obligatory during the process of signing up, attending classes and taking examinations on behalf of others, deleting course materials, deleting/altering legal data will be brought into question. Institutes will be required to fulfill their responsibilities such as providing the necessary software and hardware in the context of security and providing training for students and teachers about the subject of security.

Social networks are virtual platforms that involve millions or even billions of individuals from all ages. In these platforms, as well as in real life, dangerous and malicious people exist. We have information about these people and their threats in real life and we take necessary precautions. We should take the same measures for social networking platforms as well. Both physical and electronic environment security of schools and courses, which are traditional learning and teaching environments, are essential for quality and effective education. Taking into account the fact that social networks are often used as learning and teaching platforms, providing the security of these platforms is one of the current issues that need to be addressed. For this reason, research is emphasized on the risks, threats, and security measures in social network environments (Cabaj, Domingos, Kotulski and Respício, 2018; Carlson, Djupsund and Strandberg, 2013; Çakır, Hava, Gülen and Özüdoğru, 2015; Forkner, 2016; Fox, 2012;Gaff, 2014; Hegel JR., 2011; Hiatt and Choi, 2016; Kelly, 2011; Kroll, 2011; Lenhart, 2013; McBride, MSN, RN, CPN, CPON and CCRN, 2011; Pedersen, 2013; Schaik, Jansen, Onibokun, Camp, and Kusev, 2018; Shillair, Cotten, Tsai, Alhabash, LaRose, and Rifon, 2015; Stroud, 2010; Tenenbaum and Zottola, 2011; Zernetska, 2017). In addition to individual work, there are also initiatives that require international co-operation in order to raise awareness about the safe use of social networks and the Internet. COP (Child Online Protection), INHOPE (International Association of Internet Hotlines), and INSAFE (European Safer Internet Network) are the most common of these initiatives. INSAFE is a large European network in which 30 national secure internet centers operate together, including the European Union countries, Norway, Iceland and Russia (Insafe Network, 2018).

It is extremely important that individual, national and international research and studies continue. This is because the more information and experience people have on social networking dangers, the measures to be taken against them, and the legal rights, social networks will become more secure as educational platforms.

To this end, the following recommendations can be made for decision makers, administrators, teachers, learners and parents:

- Since they keep the information of a large number of students, parents and employees in electronic form, educational institutions have the responsibility for the protection of this information. For this reason, they need to formulate security strategies and measures against phishing attacks that may come from social networks or other Internet tools.
- Regular trainings should be given to teachers who teach at every level of school, university lecturers, and institution managers about safe use of social networks.
- Under the general heading of safe social networking, courses should be opened for students at all levels.
- Educational institutions should also organize training programs for parents, as well as teacher and student trainings.
- Teachers should be trained on the use of social networks for teaching purposes, effective methods and applications.
- Countries should establish long-term social networking and cyber security policies and necessary steps should be taken in this framework.
- Internationally secure social networking strategies should be developed and cooperation between countries should be promoted.
- In the safe use of social networks, community members other than managers, teachers, students and parents should also be trained.
- In all work on the safe use of social networks, schools, universities, non-governmental organizations and related technology companies should be in constant collaboration.
- Using social networks with children, being friends with them on social networks, or guiding children to social activities can help families with the fight against cyber bullying.
- On public transport, stops and advertising boards, effective public spots and posters should be used against the threats in social networks.

References

Alcantar, M. R. C., Ballesteros, N. S., Torres, C. I., Padilla, A. A. J., & Barajas, R. E. L. (2016). Teaching experience in university students using social Networks. *World Journal on Educational Technology:* Current Issues, *8*(3), 224-230. Retrieved May 31 2018 from https://files.eric.ed.gov/fulltext/EJ1142234.pdf.

Alkan, M. F., & Bardakçı, S. (2017). Ortaöğretim öğrencilerinin sosyal ağlardan öğrenme biçimleri: nitel bir inceleme. *Kastamonu Eğitim Dergisi*, Mayıs 2017, *25*(3), 1221-1238. Retrieved June 17 2018 from http://kefdergi.kastamonu.edu.tr/ojs/index.php/Kefdergi/article/view/1315

Al-Mukhaini, E. M., Al-Qayoudhi, W. S., & Al-Badi, A. H. (2014). Adoption of social networking in education: A study of the use of social networks by higher education students in Oman. *Journal of International Education Research, 10*(2), 143-154. Retrieved June 17 2018 from https://www.learntechlib.org/p/152600/

Altındağ, A. (2015). Sosyal ağlarda sahte hesaplar. Available online: https://mediatrend.mediamarkt.com.tr/sosyal-aglarda-sahte-hesaplar/ (accessed on 23 May 2018).

Arshavskiy, M. (2014). Social Media Tools - Taking Informal Learning To New Heights. Available online: https://elearningindustry.com/social-media-tools-taking-informal-learning-new-heights (accessed on 21 October 2018).

Arslan, A. (2015). Eğitim ve Öğretimde Sosyal Medyanın Kullanımı, 191-219, Konya, Çizgi Kitapevi.

Asberg, S. (2013). Social Networks in Education: A Facebook-Based Educational Platform. Department of Computer and Information Science Master's Thesis. Linköpings Universitet, Linköping, Sweden. Retrieved 25 May 2018 from http://liu.diva-portal.org/smash/get/diva2:625460/FULLTEXT01.pdf.

Aslan, S. C. (2018, February 26). Yeni Nesil Suç Mahalli: Sosyal Medya. Available online: https://hukukiblog.com/kamu-hukuku/yeni-nesil-suc-mahalli-sosyal-medya/ (accessed on 25 May 2018).

Bersin, J. (2011). Strategic Human Resources and Talent Management Predictions for 2012. Bersin & Associates Research Report. Retrieved 19.10.2018 from http://www. bersin.com.

BoomSocial (2018). Facebook Eğitim Sektörü Hayran Sayıları. Available online: https://www.boomsocial.com/Facebook/UlkeSektor/tumu/egitim (accessed on 20.10.2018)

Bucher, K. T., & Manning, M. L. (2005). Creating safe schools. *The Clearing House: A Journal of Educational Strategies, Issues and Ideas, 7*(1), 55- 60. https://doi.org/10.3200/TCHS.79.1.55-60

Buzzetto-More, N. A. (2012). Social networking in undergraduate education. *Interdisciplinary Journal of Information, Knowledge, and Management, 7*, 63-90. Retrieved *31* May 2018 from http://www.ijikm.org/Volume7/IJIKMv7p063-090Buzzetto611.pdf.

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, *75*, June 2018, 24-35. https://doi.org/10.1016/j.cose.2018.01.015

Çakır, H., Hava, K., Gülen, Ş. B., & Özüdoğru, G. (2015). An investigation of preservice teachers' security awareness on social networking sites. *International Journal of Human Sciences*, *12*(1), 887-902. https://doi.org/10.14687/ijhs.v12i1.3142

Çetiner, M. (2015, March 22). HİKİKOMORİ. Available online: http://gunceltip.blogspot.com/2015/03/hikikomori.html (accessed on 1 June 2018).

Chen, B., & Bryer, T. (2012). İnvestigating instructional strategies for using social media in formal and informal learning. *The International Review of Research in Open and Distributed Learning*, *13*(1), 87-104. https://doi.org/10.19173/irrodl.v13i1.1027

Chvanova, M. S., Khramova, M. V., Pitsik, E. N., & Hramov, A. E. (2016). Is it possible to improve the university education with social networks: the opinion of students and teachers. Retrieved 25 May 2018 from https://ieeexplore.ieee.org/document/7751895/citations?tabFilter=papers.

Cimpanu, C. (2017). Sudden Rise Detected in Faceliker Malware That Manipulates Facebook "Likes". Bleeping Computer, September 27 2017. Available online: https://www.bleepingcomputer.com/news/security/sudden-rise-detected-in-faceliker-malware-that-manipulates-facebook-likes-/ (accessed on 23 May 2018).

Clothey, R. A. (2016). Community cultural wealth: uyghurs, social networks, and education. *Diaspora, Indigenous, and Minority Education*, *10*(3), 127-140. https://doi.org/10.1080/15595692.2015.1111205

Cook, S. (2018). Cyberbullying facts and statistics for 2016-2018. Available online: https://www.comparitech.com/internet-providers/cyberbullying-statistics/#gref (accessed on 28 August 2018).

Cyberbully411 (2018). Myths and Facts. Available online: https://www.cyberbully411.com/myths-and-facts (accessed on 5 June 2018).

Dadar, A. (2016). Scareware. Available online: https://www.noidentitytheft.com/scareware/ (accessed on 1 June 2018).

Dailyworld (2017, November 4). Facebook knows it has 270 mn fake accounts. Available online: https://dailyworld.in/facebook-knows-it-has-270-mn-fake-accounts/?utm_campaign=DonanimHaber&utm_medium=referral&utm_source=DonanimHaber (accessed on 10 June 2018).

Delello, J. A., Mcwhorter, R. R., & Camp, K. M. (2015). Using social media as a tool for learning: a multi-disciplinary study. *International Jl. on E-Learning* (2015), *14*(2), 163-180.

Demir, M. (2016, November 26). Sosyal Medya Hesaplarına Saldırı Türleri. Available online: https://sosyalmedyaguvenlik.blogspot.com/2016/11/sosyal-medya-hesaplarna-saldr-turleri.html (accessed on 24 May 2018).

Demir, O. (2017). Özel Hayatın Gizliliğini İhlal Suçu. Available online: http://okandemir.av.tr/ozel-hayatin-gizliligini-ihlal-sucu/ (accessed on 20 June 2018).

Dere, E., Yücel, Ü. A., & Yalçınalp, S. (2016). İlköğretim öğrencilerinin eğitsel bir çevrimiçi sosyal öğrenme ortamı olan Edmodo'ya ilişkin görüşleri. *Elementary Education Online*, 2016, *15*(3), 804-819. https://doi.org/10.17051/io.2016.49794

Descardins, J. (2018). What Happens in an Internet Minute in 2018? Available online: http://www.visualcapitalist.com/internet-minute-2018/ (accessed on 15 April 2018).

Dhanhani, A., Mizouni, R., Otrok, H., & Rubaie, Z. (2015). Analysis of collaborative learning in social network sites used in education. *Social Network Analysis and Mining*, December 2015, *5*(65). https://doi.org/10.1371/journal.pone.0194777

DiVall, M. V., & Kirwin, J. L (2012). Using facebook to facilitate course-related discussion between students and faculty members. *American Journal of Pharmaceutical Education*, *76*(2), Article 32.

Dunlap, J., & Lowenthal, P. (2009). Tweeting the night away: using Twitter to enhance social *presence. Journal of Information Systems Education, 20*(2), 129-135. https://doi.org/1755224721

Ebner, M., Lienhardt, C., Rohs, M., & Meyer, I. (2010). Microblogs in higher education – A chance to facilitate informal and process-oriented learning? *Computers & Education*, *55*(1), 92-100. https://doi.org/10.1016/j.compedu.2009.12.006

EPN (2017, October 14). Siber Saldırıların Yeni Hedefi Sosyal Medya. 14 Ekim 2017, EPN Haber Merkezi. Available online: https://epnext.com/siber-saldirilarin-yeni-hedefi-sosyal-medya/ (accessed on 19 May 2018).

Eren, B. (2018). https://twitter.com/erenbilal/status/1001416233475026945 (accessed on 1 July 2018)

Erol, Z. (2014). Sosyal Ağların Bağımlısı Mısınız? Available online: http://www.psikolik.com/threads/sosyal-a%C4%9Flar%C4%B1n-ba%C4%9F%C4%B1ml%C4%B1s%C4%B1-m%C4%B1s%C4%B1n%C4%B1z.1664/(accessed on 3 June 2018).

Forkner, C. B. (2016). Social Media Security: What to Watch out for... Available online: https://www.slideshare.net/CarlForknerPhD/social-media-security-what-to-watch-out-for (accessed on 30 May 2018).

Fottrell, Q. (2014). Lonely people share too much on Facebook. Available online: https://www.marketwatch.com/story/lonely-people-post-personal-details-on-facebook-2014-05-21(accessed on 20April 2018).

Fox, M. (2012). Legal risks of social media: what dietetics practitioners need to know. *Journal Of The Academy Of Nutrition And Dietetics*, November 2012, *112*(11), 1718-1723. https://doi.org/10.1016/j.jand.2012.09.004

Gaff, B. M. (2014). Corporate Risks from Social Media. *IEEE Computer Society*, 01, Jan. 2014, *47*(01), 13-15. https://doi.org/10.1109/MC.2014.9

Global Digital Report (2018). Digital in 2018. Available online: https://wearesocial.com/blog/2018/01/global-digital-report-2018 (accessed on 14 April 2018).

Gülbahar, Y., Kalelioğlu, F. & Madran, R. O. (2010). Sosyal Ağların Eğitim Amaçlı Kullanımı. Inet-tr 2010, Türkiy'de İnternet Konferansı, İstanbul.

Güneş, F. (2015, July 21). Teknoloji çağının tehlikesi: "Gizli okumaz yazmazlık". Available online: http://www.radikal.com.tr/bartin-haber/teknoloji-caginin-tehlikesi-gizli-okumaz-yazmazlik-1400825/ (accessed on 1 June 2018).

Güvenli Web (2017). Çocukların İnternet Kullanımına Yardımcı Olacak 6 İpucu Ve Ebeveyn Yaklaşımları. Available online:

http://www.guvenliweb.org.tr/blog-detay/cocuklarin-internet-kullanimina-yardimci-olacak-6-ipucu-ve-ebeveyn-yaklasimlari (accessed on 4June 2018).

Gwaka, L. T. (2015). Social Media Risks In Large And Medium Enterprises In The Cape Metropole: The Role Of Internal Auditors. Master of Technology in Internal Auditing in the Faculty of Business: Internal Audit & Information System at the Cape Peninsula University of Technology, Cape Town. Retrieved 15 April 2018 from http://etd.cput.ac.za/bitstream/handle/20.500.11838/2086/209201223_Gwaka_LT_MTech_Acc_Bus_2016.pdf?sequence=1&isAllowed=y

Hegel, Jr, K. C. (2011). To tweet or not to tweet – understanding the risks in social media. *Global Cosmetic Industry*, 179(6):56-58. Retrieved 30 June 2018 from https://www.frenkel.com/to-tweet-or-not-to-tweet-understanding-the-risks-in-social-media/

Hiatt, D., & Choi, Y. B. (2016). Role of security in social networking. *International Journal of Advanced Computer Science and Applications*, *7*(2), 2016, 12-15. Retrieved 28 April 2018 from https://doi.org/10.14569/IJACSA.2016.070202

Hoelscher, P. (2016). Phishing on Social Network - Gathering Information. Available online: https://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-attacks-by-demographic/social-networks/#gref (accessed on 4 May 2018).

Hürriyet (2018, April 2). Kime Benzediğini Gör uygulamalarındaki tehlikeye dikkat! Available online: http://www.hurriyet.com.tr/teknoloji/kime-benzedigini-gor-uygulamalarindaki-tehlikeye-dikkat-40791816 (accessed on 4 June 2018).

Insafe Network (2018). Insafe network. Available online: https://safe.si/english/insafe-network (accessed on 17 June 2018).

ISTR20 (2015). Internet Security Threat Report, Volume 20, Symantec. Available online:https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf (accessed on 7June 2018).

James, C. (2014). 5 Social Networks For Students To Get Academic Help. Retrieved 10 June 2018 from http://www.edudemic.com/social-networks-for-students/?utm_source=dlvr.it&utm_medium=twitter.

Junco, R. R., Heiberger, G. G., & Loken, E. E. (2010). The effect of Twitter on college student engagement and grades. *Journal of Computer Assisted Learning*, *27*(2), 119-132. https://doi.org/10.1111/j.1365-2729.2010.00387.x

Kazancı, A. & Dönmez, F. (2013). Okul 2.0: Eğitimde Sosyal Medya ve Mobil Uygulamalar. Ankara: Anı Yayıncılık.

Khanse, A. (2016). What is Cybersquatting and Typosquatting–Definition & Examples. Available online:https://www.thewindowsclub.com/cybersquatting-and-typosquatting (accessed on 12May 2018).

Kist, W. (2012). Class, Get Ready to Tweet: Social Media in the Classroom. The National PTA Magazine, *38*(3), 10-11. http://files.eric.ed.gov/fulltext/EJ991339.pdf

Klimova, B., & Poulova, P. (2015). Asocial networks in education. 12th International Conference on Cognition and Exploratory Learning in Digital Age (CELDA 2015), 240-245. Retrieved 16 April 2018 from https://link.springer.com/chapter/10.1007/978-3-319-39690-3_12.

Komninou, I. (2018). A case study of the implementation of social models of teaching in e-learning: "the social networks in education", online course of the inter-orthodox centre of the church of Greece. *Tech Trends* (2018), *62*, 146–151. https://doi.org/10.1007/s11528-017-0247-4

Kroll, K. (2011). Monitoring employees' use of social media. *Compliance and Technology*, August 2011, 52-53. https://doi.org/10.1080/0144929X.2015.1004647

Lavy, V. (2015). The Effect of Social Networks on Students' Academic and Non-Cognitive Behavioral Outcomes: Evidence from Conditional Random Assignment of Friends in School. Toulouse School of Economics, Econometrics And Empirical Economics Seminar. Retrieved 29 April 2018 from https://www.tse-fr.eu/sites/default/files/TSE/documents/sem2015/eee/lavy_1.pdf.

Leichman, A. K. (2018). New algorithm identifies fake users on social networks. Available online: https://www.israel21c.org/new-algorithm-identifies-fake-users-on-social-networks/ (accessed on 1 July 2018).

Lena, M. (2016). Social Media Identity Theft, Enabling Social Security. Available online: http://www.waronidtheft.org/social-media-identity-theft/ (accessed on 11 June 2018).

Lenhart, A. (2013). Teens, Social Media and Privacy: Reputation management, third party access & exposure to advertising. Presentation to the State of Maryland's Children Online Privacy Working Group at the Attorney General's Office in Baltimore. Pew Research Internet Project. Available online:http://www.pewinternet.org/2013/06/25/teens-social-media-and-privacy-reputation-management-third-party-access-exposure-to-advertising/(accessed on 6 June 2018).

Mashable (2014). Your Private Facebook Friends List Isn't Actually That Private. Available online:https://mashable.com/2014/06/02/facebook-friends-list-privacy/#q6yzwR1qCgqq (accessed on 11 June 2018).

McBride, D., MSN, RN, CPN, CPON, and CCRN (2011). Risks and benefits of social media for children and adolescents. *Journal of Pediatric Nursing* (2011), *26*, 498–499. https://doi.org/10.1016/j.pedn.2011.05.001

Mediatrend (2015). Fotoğrafa konum bilgisi ekleme. Available online:https://mediatrend.mediamarkt.com.tr/fotografta-konum-bilgisi-ekleme/(accessed on 1 June 2018).

Menczer, F. (2018). How Many Social Media Users Are Real People? Available online: https://gizmodo.com/how-many-social-media-users-are-real-people-1826447042 (accessed on 15 June 2018).

Messner, K. (2009). Pleased to Tweet you, making a case for Twitter in classroom. *School Library Journal*, December 2009, 44-47. http://www.schoollibraryjournal.com/article/CA6708199.html

Microsoft (2018). Çevrimiçi Avcılar – Çocuk Güvenliği. Available online: https://www.microsoft.com/tr-tr/security/family-safety/predators.aspx (accessed on 10 May 2018).

Moolenaar, N. M. and Daly, A. J. (2012). Social networks in education: exploring the social side of the reform equation. *American Journal of Education, 119*(1), (November 2012), 1-6. https://doi.org/10.1086/667762

Mora, H. M., Pont, M. T. S., Casado, G. M., & Iglesias, V. G. (2015). Management of social networks in the educational process. *Computers in Human Behavior*, *51* (2015) 890–895. https://doi.org/10.1016/j.chb.2014.11.010

Norton Team (2015). What is Scareware and How Can I Avoid It?. Available online:https://uk.norton.com/norton-blog/2015/09/what_is_scarewarean.html (accessed on 13 June 2018).

O'Connor, M. (2014). Addicted to Likes: How Social Media Feeds Our Neediness. Available online:https://www.thecut.com/2014/02/addicted-to-likes-social-media-makes-us-needier.html (accessed on 10June 2018).

OWASP (2017). Clickjacking. Available online: https://www.owasp.org/index.php/Clickjacking(accessed on 12 June 2018).

Öztürk, E. (2017, December 20). Photolurking. Available online:https://teknolojivegelisim.wordpress.com/2017/12/20/photolurking/(accessed on 10June 2018).

Pedersen, S. (2015). UK young adults' safety awareness online _ is it a 'girl thing'?. *Journal of Youth Studies*, 2013, Vol. *16*(3), 404-419. https://doi.org/10.1080/13676261.2012.710741

Pettenati, M., & Ranieri, M. (2006). Informal learning theories and tools to support knowledge management in distributed CoPs. Published 2006 in EC-TEL Workshops. Retrieved 1 March 2018 from https://www.semanticscholar.org/paper/Informal-Learning-Theories-and-Tools-to-Support-in-Pettenati-Ranieri/97028aacad36735b5d936fb6c6acc92958f01bb4.

Rahman, Md, S. (2012). Detecting Social Malware and its Ecosystem in Online Social Networks. Doctoral Dissertation, University of California, Riverside. UC Riverside Electronic Theses and Dissertations. Available online: https://escholarship.org/uc/item/3116712g (accessed on 16 June 2018).

Rivero, V. (2011). Tools For Learning: We're Talking Social Media in Education. Internet@Schools. Retrieved 26 June 2018 from http://www.internetatschools.com/Articles/Editorial/Features/TOOLS-FOR-LEARNING-Were-Talking-Social-Media-in-Education-75182.aspx.

Rodrigues, S. (2018, July 10). What is FOMO and how do I protect my child from it this summer? Available online:https://www.telegraph.co.uk/travel/family-holidays/what-is-fomo-children-summer-holidays-psychologist-loneliness/ (accessed on 29 May 2018).

Şahin, A. Y. (2018, April 4). Fomo nedir? Available online: https://www.cnnturk.com/teknoloji/fomo-nedir (accessed on 9 May 2018).

Şahin, E. (2016). Sahte Hesapların Çoğu, Meğer Eski Sevgiliyi Takip Etmek İçin Açılıyormuş. Available online:http://www.webtekno.com/internet/sahte-hesaplarin-cogu-meger-eski-sevgiliyi-takip-etmek-icin-aciliyormus-h16454.html (accessed on 9June 2018).

Sánchez-Gómez, M. C., Iglesias-Rodríguez, A., & García-Peñalvo, F. J. (2017). Digital competence, social networks and apps in education: Views and beliefs of users of the Twitter virtual domain. Fifth International Conference on Technological Ecosystems for Enhancing Multiculturality (TEEM'17) (Cádiz, Spain, October 18-20, 2017) (Article 70). https://doi.org/10.1145/3144826.3145420

Schachter, R. (2011). The social media dilemma. *District Administration*, July/August 2011, 27-33. Retrieved 2 April 2018 from https://www.districtadministration.com/article/social-media-dilemma.

Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*(2018), 283-293. https://doi.org/10.1016/j.chb.2017.10.007

Sefton-Green, J. (2004). Literature Review in Informal Learning with Technology Outside School. Futurelab Literature Review Reports 7, 2004. Available at: http://archive.futurelab.org.uk/resources/documents/lit_reviews/Informal_Learning_Review.pdf.

Shillair, R., Cotten, S. R., Tsai, H. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*(2015), 199–207. https://doi.org/10.1016/j.chb.2015.01.046

Siberg üvenlik (2016). Typosquatting Nedir? Available online: http://siberguvenlikdanismanligi.com/typosquatting-nedir/(accessed on 28April 2018).

Simonova, I., & Poulova, P. (2015). Social networks and mobile devices in higher education: pilot project. 2015 IEEE 39th Annual International Computers, Software & Applications Conference, 851-856. https://doi.org/10.1109/COMPSAC.2015.192

Sırt, T. (2017, July 2). Hediye çeki oltalarına dikkat. Available online: https://www.sabah.com.tr/yazarlar/sirt/2017/07/02/hediye-ceki-oltalarina-dikkat (accessed on 29May 2018).

Sorte, S.R. & Rathod, S. B. (2016). Social networking sites as informal learning tool. *Indian Journal of Physiology And Pharmacology*, April 2016, *60*(4), 403-406.

Sözcü (2018, February 8). İnternette yeni skandal Deepfake! Başınıza gelirse ne yapacaksınız? Available online: https://www.sozcu.com.tr/2018/ekonomi/internette-yeni-skandal-deepfake-basiniza-gelirse-ne-yapacaksiniz-2210669/(accessed on 28May 2018).

Talay, Y. (2017). Kamuda Çalışanların Sosyal Medya Kullanımı ile Oluşabilecek Güvenlik Riskleri. Available online: http://docplayer.biz.tr/32078581-Kamuda-calisanlarin-sosyal.html#show_full_text (accessed on 23 May 2018).

Talwar, S. (2018, July 3). How deepfake videos are dangerously blurring the lines of reality. Available online:https://www.dailyo.in/technology/deepfake-lok-sabha-polls-2019-narendra-modi-donald-trump-fake-video/story/1/25267.html (accessed on 9 June 2018).

Tan, A. (2015). Sosyal Ağlarda İşlenebilen Su çlar Nelerdir? Available online: http://www.aydogantan.av.tr/sosyal-aglarda-islenebilen-suclar-nelerdir/ (accessed on 3 June 2018).

Taş, E. (2018, February 7). Phishing (kimlikavı) Nedir? Available online: https://www.akilligundem.com/phishing-kimlik-avi-nedir/ (accessed on 23May 2018).

Tenenbaum, J. S., & Zottola, A. J. (2011). Don't take risks with social media. *Nonprofit World*, *29*(4), July/August 2011, 6-9. Retrieved 24 May 2018 from file:///C:/Users/hp/Downloads/snpo_1820.pdf

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, *26*, 277–287. https://doi.org/10.1016/j.chb.2009.11.014

Trinder, K., Guiller, J., Margaryan, A., Littlejohn, A., & Nicol, D. (2008). Learning From Digital Natives: Bridging Formal and Informal Learning. Research Project Report. Final Report for the Higher Education Academy, 2008. Available online http://www.academy.gcal.ac.uk/ldn/LDNFinalReport.pdf (accessed on 21October 2018).

Uzun, H. (2016). Impact of Social Media on Knowledge Quality: Fake Accounts. *Academia Journal of Social Sciences*, 2016, *1*(2), 1-31. Retrieved 21 June 2018 from http://bsyayinevi.com/wp-content/uploads/2017/07/ajs2_1.pdf.

Wang, Q., Chen, W., & Liang, Y. (2011). The Effects Of Social Media On College Students. MBA Student Scholarship. Paper 5. Retrieved2 April 2018 from http://scholarsarchive.jwu.edu/mba_student/5.

Weaver, D., Viper, S., Latter, J., & McIntosh, C. (2010). Off campus students' experiences *collaborating online, using wikis. Australasian Journal of Educational Technology, 26*(6), 847-860. https://doi.org/10.14742/ajet.1046

wmaracı (2018). Bot Takipçi Nedir? Bot Takipçi Satışı ve Bot Takipçi Kasma. Available online: https://wmaraci.com/nedir/bot-takipci (accessed on 2 June 2018).

Yılmaz, B. (2015). Hukukta Yeni Bir Alan: Sosyal Medya Hukuku. Available online: http://www.ankarabarosu.org.tr/siteler/ankarabarosu/hgdmakale/2015-1/16.pdf (accessed on 25 June 2018).

Zernetska, O. (2017). Cybersecurity On Us Social Networks. Available online:http://www.americanstudies.histoy.knu.ua/wp-content/uploads/2017/01/Zernetska-O.pdf (accessed on 14 June 2018).