Anatolian Journal of Computer Sciences

Volume:6 No:1 2021 © Anatolian Science

pp:32-45 ISSN:2548-1304

How Privacy Is Threatened From Social Media Communication?

Ahmet Efe[*1], *Hamed Suliman*[2]

[*1]*Ankara Kalkınma Ajansı, İç Denetim, Ankara, Türkiye, 0000-0002-2691-7517 (icsiacag@gmail.com)*

[2]*Yıldırım Beyazit Üniversitesi, Bilgisayar Mühendisliği, Ankara, Türkiye, 0000-0001-7510-1405 (hamedmmsuliman@gmail.com)*

Received Date : Oct. 30, 2020
Acceptance Date : Dec. 27, 2020
Published Date : Mar. 1, 2021

Abstract— Users of social media sites and mobile applications are exposed to different attacks by criminals trying to steal their personal information, privacy and cookies from the sites. This article explores social media risks, how users' privacy is threatened on social media networks, threat classifications on social media, and the reasons for privacy leaks in real online social networks. In addition, effective measures are clarified against each attack to protect users' personal information.

Keywords : *Cyber Security Threats; Social Media; Online Social Networks; Zero Day Vulnerability.*

Özetçe— Sosyal medya sitelerinin ve mobil aplikasyon kullanıcıları, kişisel bilgilerini, mahremiyetlerini ve sitelerden gelen çerezlerini çalmaya çalışan suçluların farklı saldırılarına maruz kalmaktadır. Bu çalışmada, sosyal medya ağlarında mevcut olan kullanıcıların risklerini, mahremiyetinin nasıl tehdit edildiği, sosyal medyadaki tehdit sınıflandırmaları ve gerçek çevrimiçi sosyal ağlarındaki mahremiyet sızıntılarının nedenleri araştırılmaktadır. Ayrıca, kullanıcıların kişisel bilgilerini korumak için yapılan her saldırıya karşı etkili önlemleri açıklığa kavuşturulmaktadır.

Anahtar Kelimeler : *Siber Güvenlik Tehditleri; Sosyal Medya; Çevrimiçi Sosyal Ağlar; Sıfırıncı Gün Açıkları.*

1. Introduction

The use of smartphones and social media has increased, causing the increase in information crime and victims (Efe & Dalmıs, 2019). Social media is a virtual place where the user names and the general name of any platform in which diverse data and information are being disseminated, published and shared. The importance of social media is the transformation of its content into a dialogue rather than a monologue. Social media provides benefits to its users while exposing different level of risks. The large social media networks have recently passed serious security threats. When the passwords published by hackers are analyzed, it turns out that many users use very simple passwords.

Social media platforms are completely foreign solutions and our data and information are in the hands of foreigners and sometimes pass to fraudsters and hackers. We allow the use of applications to access to camera, microphone and all other data. So personal images can be recorded, microphone can transmit voices and all the files can be uploaded somewhere unknown. Three billion people in the world, 40 percent of the total population uses social media. Research shows that we spend an average of two hours a day on social media. This means half a million tweets per minute and Snapchat photo sharing. Social media has an important place in our lives. However, we still cannot answer or disregard the question like “do we sacrifice not only our time but also our mental, social and physical health on social media?”

E-government services can also be hacked by user credentials taken from social media. Turkey provided access to directly genealogical tree from the early 2018. There is a very important detail that the people who questioned the Lower Family Knowledge over the State should also know. e-government platform issued over the address www.turkiye.gov.tr. Pedigree results also revealed a great danger of personally private information. Those who reach the results in the e-government pedigree practice share the details of their family history with their surroundings; one of the most popular topics of recent days is the question of e-government pedigree. Those who question the e-government genealogy and those who share the results put themselves at great risk, because the results of the e-Government genealogy include the maiden name. Clearly sharing the maternal maiden name, which is of great importance in many important institutions, invites abusive people.

Incredible developments in communication technologies have led to new possibilities, and new problems and threats, especially in new media which is the social media. It seems necessary but problematic to adapt ethical principles, which are inadequate by not keeping up with the economic transformation in traditional media, to new media. It can be said that the most important of the principles that are insufficient in practice is privacy. While privacy was not on the agenda, especially until recent years, when new media dominated, it started to take an important place thanks to the internet age and the development of social media. The reason for this is that while there is almost no element of attack on the privacy of the individual in the traditional media, the privacy of individuals has been seriously endangered with the rapid spread of social media, which is becoming extremely widespread and intense today, and many individuals take place on these platforms. According to the 2017 information of "The Statistics Portal" website; 2.46 billion people in the world via the internet Facebook, Instagram, Twitter etc. It takes place in social media platforms that have examples such as, and uses search engines such as Google and Yahoo. These numbers almost double in a few years.

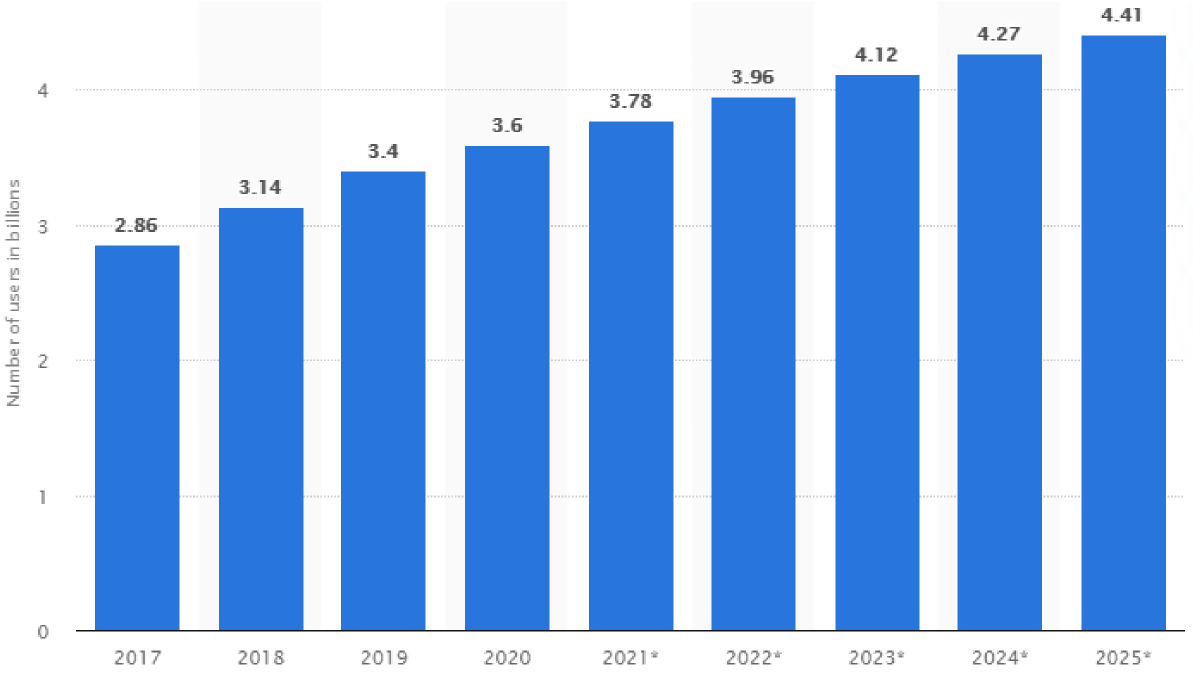

Fig. 1. Number of global social network users 2017-2025 (Statista)

Because of the business models on these platforms, users who can exist free of charge on the platforms and who use these channels are forced to give a lot of personal information in return, and are abused by malicious people who have captured them. All these users create a very rich source and target audience for companies and organizations that want to advertise to the owners of the platforms mentioned. Especially in recent years, despite the news that has been mentioned a lot about this situation, people prefer to give up their privacy and not to break away from the social platforms they use.

The owners of these personal data have the right to decide which information can be published on the social media pages. We have compiled the conclusions of current research on this subject. Currently, billions of people access thousands of social media webpages in order to communicate with each other, exchange messages and have chats. For instance, utilizers of Twitter exchange more than 170 million messages every day. Furthermore, Social media provides big companies and organizations with easy mean in order to make business. Consequently, the users of social media have increased rapidly in the past several years. As a result of using social media sites, uses are capable of making managing their accounts, contact with their old friends besides making new ones. However, these accounts include personal privacy of users such as name, age, sex and personal photos and videos which are considered individual properties. While people exchange photos, videos and personal privacy on social media, they lack in the security counter measures so as to protect their data. Cyber criminals exploit personal privacy and other data of users for hacking other accounts or for other reasons. Thus, privacy and security have become the major concern in social networking environment. Available internet security programs and antivirus programmers are not capable enough as counter measures to defend the user accounts against security threats.

Generations are divided into groups based on sociological effects in various studies. Generations born between certain dates differ in their relationship with technology and the meanings they attribute to life. Differences between generations also shape the perception of privacy. A study by Çaycı (2014: 195) reveals that Generation Z, born in 1995 and later, has a different perception of privacy compared to Generation X born between 1965-1980 and Generation Y born between 1981-1994. Generation Z, defined as a generation born into technology, does not see social media as a separate reality area and shares its privacy on social media as much as it shares in real life. The concept of privacy is examined in three dimensions: space, person and information privacy. While the privacy of the place refers to protecting the physical space surrounding the individual, the privacy of the person refers to the protection from unfair interference against the individual. Information privacy means the control of processes such as collecting, storing, processing and distributing personal data (Zhumagaziyeva and Koç, 2010: 114). Considering the rapid development of information and communication technologies, discussions on the concept of privacy are mostly carried out in terms of information privacy.

The goal of this research is to illustrate the methods that are used so as to disclose of personal privacy of the users of social media. Furthermore, the research will look for the effective mechanisms to defend personal privacy. This research will answer the following questions.

- *What attacks do criminal use in order to discover the individual user' data?*
- *What are the effective mechanisms in order to defend personal privacy of the users?*

2- Privacy Threats

Privacy seep within social media networks due to the following four causes:

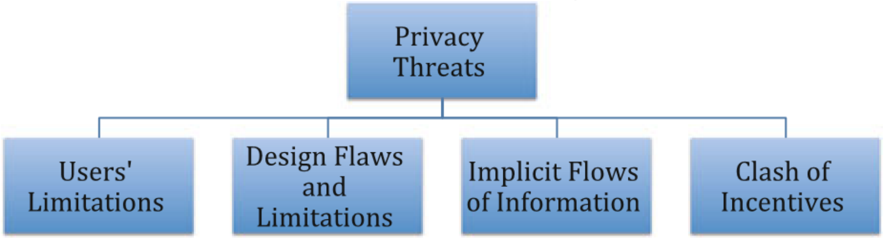

Fig. 1 Classification of the causes of uses' privacy seep**.**
Source [Mahmood, Shah. 2014].

2.1- Restriction of users:

Making resolutions by people depend on many factors such as the time amount, the available data and its order. Worst individual resolutions by people result from two things:

- Confined logic and
- Restricted memory.

People resolution creates need for the reasonable amount of time in order to take crucial decisions in a specific time for complicated issues. Similarly, when people access a social media webpages and applications, they lack in comprehensive background about how to defend their individual data. For example, although social media Networks such as Facebook include some security measures such as privacy setting, most of its users do not use them. Furthermore, most of them know little about modern attacks and possible dangers.

2.2- Restrictions and Defects of the Design

Criminals can make easily a lot of fake accounts by using fake personalities in social media networks. As a result of using inconvenient authentication procedures in social media, the criminal just need only a new email in order to make fake profile. Fake accounts lead to *Sybil attacks*. For instance, criminals can exploit their fake accounts to establish new links with covered personalities so as to attain data about some people. By using these approaches, criminals may achieve more data than using legal approaches. In addition, criminals may exploit accounts in improper way such as spreading spam emails, illegal material such as malware and phishing connections. The best countermeasures against fake accounts are use proper authentication procedure as well as powerful identification.

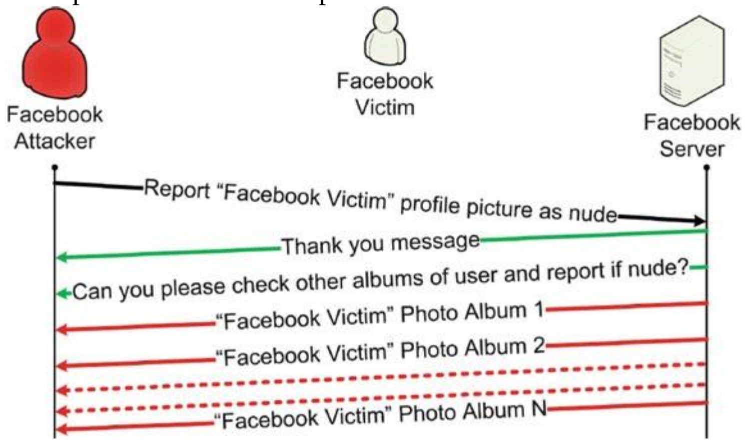
Facebook Attacker
Facebook Victim
Facebook Server
Report "Facebook Victim" profile picture as nude
Thank you message
Can you please check other albums of user and report if nude?
"Facebook Victim" Photo Album 1
"Facebook Victim" Photo Album 2
"Facebook Victim" Photo Album N

Fig. 2 Assisting Facebook identifies data seep in their protocols.
Source [Mahmood, Shah. 2014].

2.3- Data's implied flux

Information seep in social media can be implicit rather than explicit. For instance, the "likes" of a user on Facebook or the videos that a user may observe give the cybercriminal the capability to infer huge amount of implicit data about users.

2.4-Concern inconsistency

Advertisements produce a lot of money for more common social media. This results in contradiction between the service providers concerns and users' benefits. Service providers need the money of advertisements in order to survive on one hand. On the other hand, they need users so as to publish their advertisement to them.

2.5-- Privacy considerations

1-Anonymity: means that users can access any webpages without discovering their own identities.

2-Unobservability: no third party can collect any data about the communicating parties and the content of their communication.

3-Unlinkability: in case of two messages. No third party should know whether the two messages were sent by the same sender or received by the same receiver.

4-Untraceability: no third party can build history of actions executed by arbitrary users inside the system (Strufe 2011).

3. Social Media Threats

Although some see cyber security and physical security as different disciplines, in fact, they are quite connected to each other. For example, the information you share on social media can be used by malicious people in real life and you can become a victim. Likewise, cyber security weaknesses can have serious consequences in the physical world. Here is the proof of how social media shares and profiles in can affect real life:

3.1. Identity Theft

Social media sites generate revenue with targeted ads based on personal information. They therefore encourage their registered users to provide as much information as possible. They do not endorse or assume responsibility to educate users on security, privacy and identity protection. While new laws are enacted every day, users are exposed to identity theft and a different kind of fraud every day.

In addition, these platforms have a ton of confidential user information and are probably vulnerable to external (or internal) cyber security attacks. For this reason, users should be aware about the information shared on social media and should especially avoid sharing such as home address, telephone, country, relationship status, school places and graduation dates, pet names, hobbies and most importantly identity card.

3.2. Theft

Who doesn't like the holiday? No doubt we all like the holiday and are trying to make the holiday. Somebody constantly share what they eat and drink on social media. Do you share your shares publicly or just see your friends? If you can see the Swarm Check-ups that are open to everyone, then thieves can see and learn about where you live. You can even discover the best way to get into your home with a street view.

According to research, Facebook or Instagram sharing platforms on one of five people by labeling the holiday place, away from home is sharing with his followers. In this way, they declare that their home is empty and somebody can check if they want. However, these shares risk the safety of home and properties. However, when it comes to the expected moment, we forget the basic safety rules and share the passport and ticket photos they need to share, and let the thieves know that they can rob their house comfortably. As you check in social media, the malicious people who know the exact location of your home can easily explore the place with Google Maps and reach their goals.

3.3. Phishing

Criminals can use social media in other ways, such as sending fake e-mail templates that invite people to connect online, stealing their credentials, or sending them to a URL designed to place malicious software on their computers. Fraudsters often people are using social media tricking to obtain personal and financial information. For example, fraudsters are able to open fake customer service accounts on Twitter, make fake comments on popular topics and shares, leave fake comments and links on live broadcast videos, create fake discounts and opportunity codes on behalf of brands, and organize fake surveys. In particular, employees carry a high risk for companies in this regard. Likewise, attackers who share noticeable news about the employees on social media can easily get access to the corporate networks by attracting the attention of the employee (Alam & El-Khatib, 2016).

3.4. Cyber Bullying

Cyber bullying is a form of harassment that uses electronic forms of communication. Bullying can be carried out by rumors, threats, sexual comments, disclosure of the victim's personal information, or hateful speech. Victims of cyberbullying tend to have lower self-esteem, increased suicidality, emotional tides and also frustrated, angry or depressed. Many studies have shown that cyberbullying can be as harmful as traditional forms of bullying. For example, with the Blue Whale game we heard recently, children and young people were given directives to commit suicide. This is an important proof of where cyberbullying can actually come from.

These risks, which are present and increasing in the digital world, have attracted the attention of researchers. In these scientific efforts, even if it was the first objective to understand the attacks on the Internet and analyze their types, it was later used to solve some programs (Donegan, 2012: 40), awareness campaigns (Dilmaç & Kocadal, 2019) and cyberbullying. It has also led to the development of official websites for public information purposes. In studies we can find in the scientific literature taken from various perspectives of cyberbullying (Erdur-Baker and Kavşut, 2007; Arsoy and Ersoy, 2015; Akca, Seçim and Ergül, 2015). For example, some researchers aimed to identify individuals' perceptions about cyberbullying (Tamer & Vatanartıran, 2016), while others focus on understanding the cyberbullying experiences and attitudes of young people in various age groups (Arsoy & Ersoy, 2015). However, it is possible to come across studies that associate cyberbullying with the frequency of Internet usage (Akça & Sayımer, 2017; Özdemir & Akar, 2011) or put the gender variable (Topçu, 2008) forward in such social media attacks. Another approach consists of studies aiming to understand and highlight the differences between cyberbullying and real-life bullying (Dilmaç, 2014; Erdur-Baker, 2010). Interactions between behaviors performed in the social media world and offline appear in other reviews. In these studies, for example, it is revealed that social media harassment is an extension of peer bullying at school (Erdur-Baker & Kavşut, 2007; Uçanok et al., 2011). Finally, on a more macro level, Turkish literature is also encountered some analysis regarding framing of cyberbullying in the print media (Narin and Unal, 2016).

3.5. Social manipulation

The interactive communication opportunity of social media has raised the individual from being passive (passive) to an active (active) position in his / her relations with the society and the state. This situation disrupted the traditional codes of individual-family, individual-society, individual-state relations and reshaped these relationships as individual-centered. Social media has now gone beyond being a news communication tool for people, and has turned into a platform for socializing and expressing oneself and participating in organized structures at all levels. In particular, social networks such as Facebook and Twitter have given their users the opportunity to establish organizations, organize, share information and ideas, and group around beliefs and thoughts, beyond meeting and messaging (Boyd & Ellison, 2008: 213). So much so that today social networks have turned into organizational tools that mobilize public opinion to change the regime and initiate a movement. This situation is evaluated as social networks have the power and opportunity to transform the perception and practice of democracy from representative democracy to participatory (direct) democracy (Çildan et al., 2012: 2). In other words, social networks not only contribute to the formation of public opinion, but also, perhaps more importantly, turn into important tools by which social movements are planned, organized, initiated and managed (Eren & Aydin, 20014).

A new series of studies at Oxford University revealed that propaganda in social media is used to manipulate public opinion in the world. According to research conducted in nine countries; it has been announced by governments and individuals that social media is widely used to support false information and propaganda. The report, which included nine countries, including Brazil, Canada, China, Germany, Poland, Ukraine and the United States, also includes details of social manipulation and the spread of false news. Considering that approximately 45% of the social media population is a bot account, we can say that social manipulation and perception management are the most important risks that threaten our future.

Manipulations can easily be accomplished using fake accounts. LinkedIn's latest transparency report[1] (July – December 2019) shows they took action on 11.2 million fake accounts. Most (93%) were blocked by automated defenses, but more than 85,000 fake accounts were only addressed once members reported them.

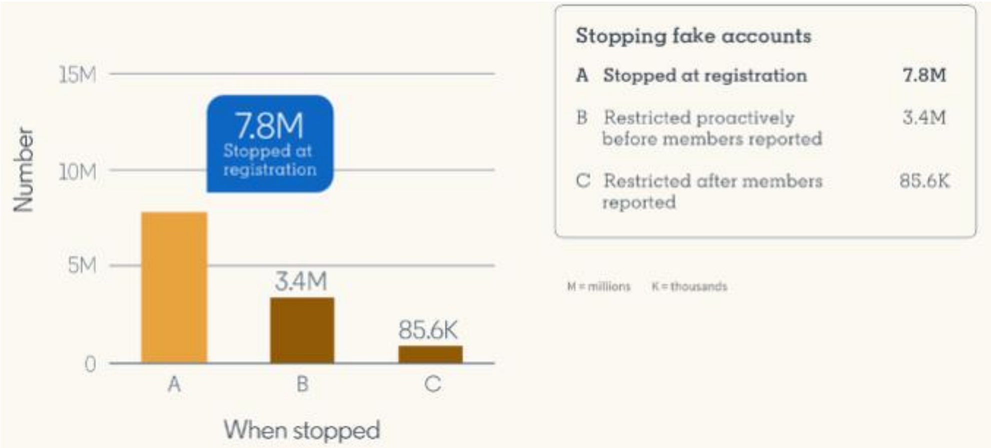

Fig. 2. Depiction of closed face accounts in the LinkedIn (Statista.com)

Likewise, Facebook estimates that fake accounts[2] represented approximately 5% (1.5B) of their worldwide monthly active users (MAU) during Q2 2020. They blocked 99.6% before users reported them.

[1] For further details see: https://about.linkedin.com/transparency/community-report#content-violations-2019-jul-dec

[2] For further details see: https://transparency.facebook.com/community-standards-enforcement#fake-accounts

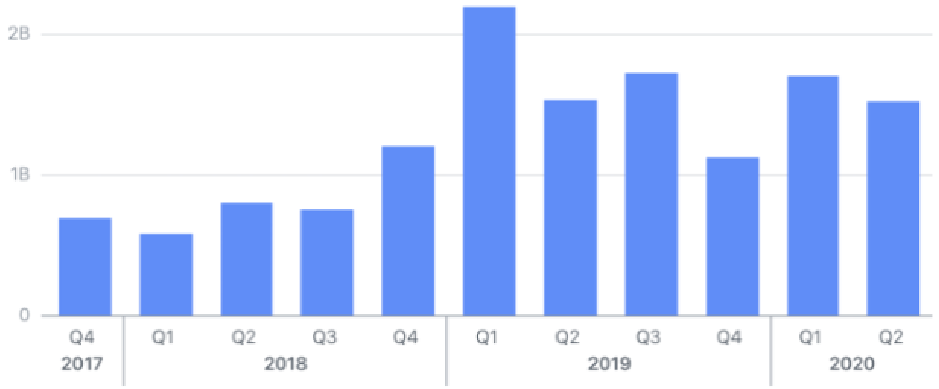

Fig. 3. Depiction of closed face accounts in the Facebook (Statista.com)

As is shown in the fig above, just for the Linkedin and Facebook there are billions of accounts that are found to be fake. These accounts are dynamic and when some are closed then they open other in order to achieve their false objectives through social media manipulation. The manipulations continue to be one of key counter campaigns for elections both national and international domains. They are transnationally effective.

Fake accounts are widely being used to manipulate perceptions of people before and during political elections. Rumors have been increasing in Turkey for election results recently. Information Technologies and Communication Authority (BTK) of Turkey increased the measures to ensure continuous communication of both social media and communication for the elections to be held. BTK will coordinate the service continuity of social media platforms such as Whatsapp, Twitter, Facebook and Instagram with the operators. In addition, a special unit will serve to prevent the spread of manipulative news in social media. At the USOM Center within the BTK Building, 100 experts who will serve on election days to fight cyber-attacks, reach the source of provocative shares, and share it with the relevant authorities. BTK President gave information about the activities at the headquarters of the National Center for Cyber Incidents Intervention Center (USOM) on what to do in the fight against cyber-attacks. The USOM headquarters will be used as a crisis center during the election and 100 white-hat experts will be on duty for election security on 24-hour basis on Election Day. BTK Chairman[1] reported that news sites and especially on the social media increased disinformation and manipulation activities, served by certain circles and quickly spread the spread of news that threatens the security of election publications that will be followed carefully. The main security measures to be taken before the election were shared with 970 institutions and organizations as of 25 April 2018. The USOM Security Operations Center monitors cyber-attacks at the infrastructure level with operators and Internet Service Providers in the communication sector. Critical institutions and organizations open to the service continuity of the Internet services are followed.

4. Social Media Communication Risk Analysis

Social media risks continue to be one the biggest threats for personal privacy and confidentiality. As a resent example Facebook[2] , the popular social media platform, was greatly shaken by the Cambridge Analytica scandal at the beginning of 2018. With the scandal, it was revealed that the personal information of 50 million Facebook users was used without permission and some brands temporarily suspended Facebook activities after this scandal. Finally, in July 2018, after the company announced its second-quarter data, the value of shares fell more than 20%. However, a last-minute development indicates that the troublesome days for Facebook will continue in the coming days. According to the latest breaking news shared by the Independent newspaper, Facebook has been exposed to a hacker attack, and 50 million people's personal information revealed in this attack. Facebook also acknowledged that such an incident occurred. According to the company's statement, security vulnerability in the code of the social media site caused this situation. According to the vulnerability, this vulnerability allows hackers to capture people's sessions and view their most specific information.

[1] For detailed information see: https://www.sabah.com.tr/gundem/2018/06/24/sosyal-medya-guvenligini-100-hacker-saglayacak

[2] For detailed information see: https://www.bbc.com/news/topics/c81zyn0888lt/facebook-cambridge-analytica-data-breach

This vulnerability is related to the “View from Another's View” feature, which allows users to see their profile through the eyes of other users. The social media platform discovered the vulnerability and began to examine it immediately. However, for now, it is a mystery about who uses this vulnerability and how it is used. In addition, Facebook did not disclose whether they knew who was affected by this hacking attack. According to the issue, this vulnerability has been closed and the “View from Another” feature is currently disabled. As a first job, the security codes will be reset so that a person who has forced access to any account will be removed from the account. Nevertheless, of course, this does not mean that someone has unauthorized access to other’s account.

Below, we have outlined basic risks from social media in four main categories:

4.1. Geotagging Risks

Location extraction, also called “toponym extraction,” is a field covering geoparsing, extracting spatial representations from location mentions in text, and geotagging, assigning spatial coordinates to content items (Stuart at al, 20018). Geotagging adds geolocation data to photos, videos, and websites and text messages via location-sensitive applications. This technology helps users create an image and information file based on the location of a mobile device or desktop computer.

You must be cautious when activating geotag features on mobile, location-based applications, or certain camera devices, as this may create confidentiality and security risks. Be sure to disable geotagging features in sensitive locations. If the Location feature is turned on, malicious people can easily learn exactly where you are, where you work or where you live.

4.2. Followers Risks

Teenagers sometimes try different clothes from the environment to be liked or different. In social media as a response to it; share photos that are open, naked or exhibiting your body. It is not very difficult to see the drawbacks of this situation.

A tracker is a generic term that explains who can view your posts and / or comment on your posts. Keep in mind that your followers' accounts may change hands and may display a post with information about you. You may have intentionally shared something with your friends’ control, but the people they share with may be out of your control. Group friends of friends can often consist of very large groups; we can't know many of them or associate them with results, so choose your friends and followers wisely on social networks.

4.3. View Profile Risks

There are many characteristics of children and young people who are not satisfied with themselves during their identity development periods. In the period when they should struggle to change them; fake accounts they create on social media, they can easily identify themselves as completely different. This may adversely affect developing and maturing identity processes.

A profile is a general term for identifying information that is specifically linked to a person. In order to better express ourselves to the environment in social media, we generally fill in the profile information. However, there are significant risks of sharing this information on social networks. People who use social media as a method of searching for possible malicious information such as identity theft, fraud, fraud or aggression are actively using it. You should keep in mind that every information you share on your profile can be used by malicious people.

4.4. Sense of privacy and deception risks

In adolescence, a sense of privacy develops. So, the young person's own secrets are formed. However, all kinds of intimate conversations, including private relations, are conducted through social media. This prevents the formation of the feelings of privacy of young people. Teenagers want to be recognized as an adult in their adolescence. Abuse has become a common occurrence for unapproved young people in inappropriate relationships on social media.

5. Categories of Attacks and Defense Mechanisms

There are various types of attacks that are used by criminals in order to attain the personal privacy of users, and cookies from social media WebPages. One of the most common attacks is the Identity theft type which contains neighborhood attack, de-anonymization attack, cross-site profile cloning attack, social phishing. Spam attack contains email-based spam attack, fake account, cross-site scripting attack and clickjacking attacks are among the type of malware attacks. Fig.4. clarifies the types of social media attacks. (Khizar Hameed 2017).

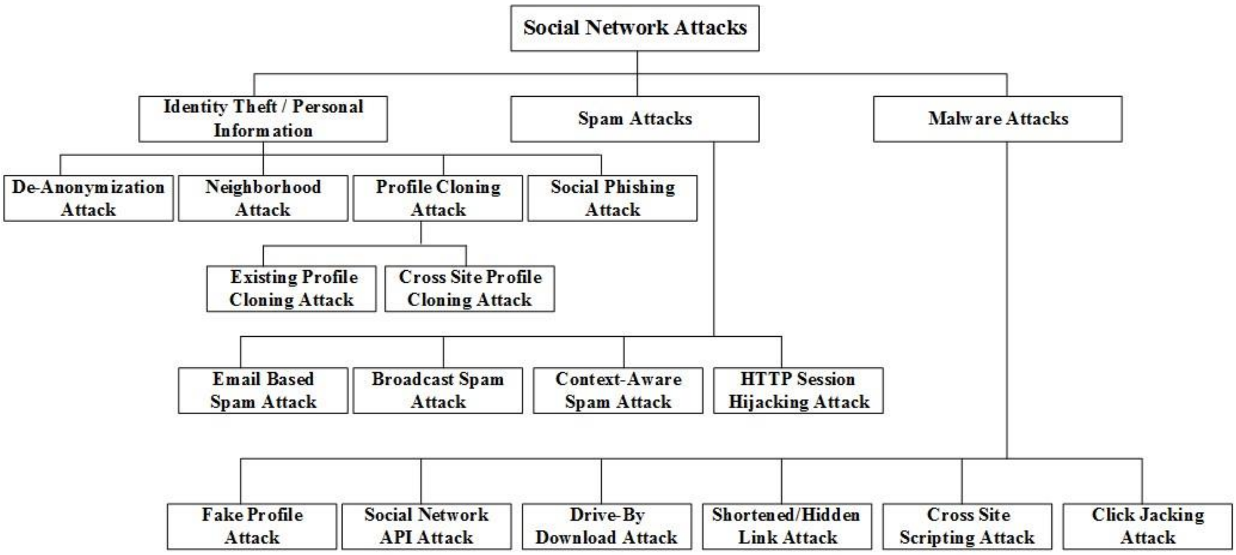

Fig 4: Classification of Social Network Sites Attacks (Khizar Hameed 2017)

There are many attack types that are based on the zero-day exploits published in the Exploit-DB website as are shown below examples the details of which can be traced in the hyperlinks in the table.

Date	Title	Author
2018-12-14	Facebook And Google Reviews System For Businesses 1.1 - Remote Code Execution	Ihsan Sencan
2018-12-14	Facebook And Google Reviews System For Businesses 1.1 - SQL Injection	Ihsan Sencan
2018-12-14	Facebook And Google Reviews System For Businesses - Cross-Site Request Forgery (Change Admin Password)	Veyselxan
2018-05-29	Facebook Clone Script 1.0.5 - Cross-Site Request Forgery	L0RD
2018-05-29	Facebook Clone Script 1.0.5 - 'search' SQL Injection	L0RD
2017-12-11	Facebook Clone Script 1.0 - 'id' / 'send' SQL Injection	Ihsan Sencan
2017-12-07	FS Facebook Clone - 'token' SQL Injection	Dan°
2017-02-24	Joomla! Component JO Facebook Gallery 4.5 - SQL Injection	Ihsan Sencan
2017-02-16	Joomla! Component Spider Facebook 1.6.1 - SQL Injection	Ihsan Sencan
2014-09-07	WordPress Plugin Spider Facebook - 'facebook.php' SQL Injection	Claudio Viviani
2013-01-07	Facebook for Android - 'LoginActivity' Information Disclosure	Takeshi Terada
2015-06-03	Seagate Central 2014.0410.0026-F - Remote Facebook Access Token	Jeremy Brown
2015-04-02	phpSFP Schedule Facebook Posts 1.5.6 - SQL Injection	@u0x
2011-11-30	WordPress Plugin flash-album-gallery - 'facebook.php' Cross-Site Scripting	Am!r
2014-12-02	WordPress Plugin Nextend Facebook Connect 1.4.59 - Cross-Site Scripting	Kacper Szurek
2016-01-13	WhatsUp Gold 16.3 - Remote Code Execution	Matt Buzanowski
2006-05-17	Ipswitch WhatsUp Professional 2006 - Authentication Bypass	Kenneth F. Belva
2006-05-12	Ipswitch WhatsUp Professional 2006 - '/NmConsole/ToolResults.asp?sHostname' Cross-Site Scripting	David Maciejak
2006-05-12	Ipswitch WhatsUp Professional 2006 - '/NmConsole/Navigation.asp?sDeviceView' Cross-Site Scripting	David Maciejak
2006-02-22	Ipswitch WhatsUp Professional 2006 - Remote Denial of Service	Josh Zlatin-Amishav
2005-11-03	IPSwitch WhatsUp Small Business 2004 Report Service - Directory Traversal	Dennis Rand
2005-06-22	Ipswitch WhatsUp Professional 2005 SP1 - 'login.asp' SQL Injection	anonymous
2004-09-03	Ipswitch WhatsUp Gold 7.0/8.0 - Notification Instance Name Remote Buffer Overflow	anonymous
2012-07-22	ipswitch whatsup gold 15.02 - Persistent Cross-Site Scripting / Blind SQL Injection / Remote Code Execution	muts

Date	Title	Author
2010-07-14	IPSwitch WhatsUp Gold 8.03 - Remote Buffer Overflow (Metasploit)	Metasploit
2004-10-04	IPSwitch WhatsUp Gold 8.03 - Remote Buffer Overflow	LoWNOISE
2019-05-03	Instagram Auto Follow - Authentication Bypass	Veyselxan
2018-10-30	Instagram Clone 1.0 - Arbitrary File Upload	Ihsan Sencan
2018-08-28	Instagram App 41.1788.50991.0 - Denial of Service (PoC)	Ali Alipour
2018-07-11	Instagram-Clone Script 2.0 - Cross-Site Scripting	L0RD
2016-11-21	WordPress Plugin Instagram Feed 1.4.6.2 - Cross-Site Request Forgery	Sipke Mellema
2018-08-23	Twitter-Clone 1 - 'code' SQL Injection	L0RD
2018-08-21	Twitter-Clone 1 - Cross-Site Request Forgery (Delete Post)	L0RD
2018-08-21	Twitter-Clone 1 - 'userid' SQL Injection	L0RD
2014-09-08	WordPress Plugin Xhanch My Twitter - Cross-Site Request Forgery	Voxel@Night
2014-09-08	WordPress Plugin WP to Twitter - Authentication Bypass	Voxel@Night
2012-11-23	Twitter for iPhone - Man in the Middle Security	Carlos Reventlov
2010-12-07	WordPress Plugin Twitter Feed - 'url' Cross-Site Scripting	John Leitch
2010-06-06	ReVou Twitter Clone 2.0 Beta - SQL Injection / Cross-Site Scripting	Sid3^effects
2010-05-29	Nucleus Plugin Twitter - Remote File Inclusion	AntiSecurity
2010-04-04	Joomla! Component redTWITTER 1.0 - Local File Inclusion	NoGe
2009-05-26	minitwitter 0.3-beta - SQL Injection / Cross-Site Scripting	YEnH4ckEr
2009-05-01	MiniTwitter 0.2b - Remote User Options Changer	YEnH4ckEr
2009-05-01	MiniTwitter 0.2b - Multiple SQL Injections	YEnH4ckEr
2009-01-30	Revou Twitter Clone - Cross-Site Scripting / SQL Injection	nuclear
2008-12-21	ReVou Twitter Clone - Arbitrary File Upload	S.W.A.T.

Table 1. Some Examples of Zero-Day Exploits over Social Media Such As Facebook, Whatsup, Instagram and Twiter

Zeroday (Zeroday vulnerabilities) are software or hardware defects that were previously unknown or undetected, but that contain vulnerabilities that will lead to serious attacks. Zeroday vulnerabilities are mostly vulnerabilities that are difficult to detect until the attack occurs. The Zeroday attack happens when the attacker exploits the vulnerability demonstrated in the table above and spreads the malware before the developers have time to release a patch or fix. Therefore, this vulnerability has been named as zeroday.

There are many attacks relating to privacy such as: In identity theft / personal privacy attack, spam attacks and malware attacks. The attacker primary purpose is to obtain the personal privacy of users. Personal privacy contains name, address, date of birth, etc. Criminals usually look for their targeted users by using the social network search engine then send friendship request to them. After confirming the friendship by the users, criminals are capable of using personal privacy of these users. These are some kinds of identity theft / personal privacy attacks.

5.1. Identity theft / Personal Information

Identity theft can be attained through De-Anonymization Attack Neighborhood Attack and Profile Cloning Attack.

5.1.1- De-Anonymization Attack: In de-Anonymization attack, the essential purpose of the criminal is to attain the personal privacy of the users whether they are alone or in combinations. The criminal utilized the history stealing approach to attain the websites that the targeted users visited before. In history stealing method, the criminal attempt to discover the browsing history of the utilizer after delivering a list of URL to him. An approach of Identity Separation is used to save the data of the social utilizer from de-anonymization attack.

5.1.2- Neighborhood Attack: In neighborhood attack, the criminal gathers the data of a specific user through his neighbors. Based on this data, the criminal capable of discovering personal data of this specific user. Table 2 mentions defense methods against this attack.

5.1.3 Profile Cloning Attack

The purpose is to steal the identity of a user of the social media sites in particular of whom make their profiles public. Criminals can extract personal privacy of public profiles easily in order to make fake profiles. Table 1 contains the defense methods against this attack.

5.2- Spam Attacks

On the social media webpages, the spam attack is prevalent. After making fraudulent email, The criminal forwards a lot of emails. Directing the traffic of a specific user to misled webpages. Often, this is the aim of the criminal. Social media webpages provide means for a lot of people to contact with each other. Malicious links and mischievous sites in social media are used to deceive the users when they access them since these may helm to malware sites or phishing sites. Spam attacks are prevalent and more dangerous in social media sites. URL sharing is a core attraction of existing social media systems like Twitter and Facebook. Recent studies find that around 25% of all status messages in these systems contain URLs, amounting to millions of URLs shared per day. With this opportunity comes challenges, however, from malicious users who seek to promote phishing, malware, and other low-quality content. (Cui et al, 2011; Rodrigues et al, 2011; Cao, 2015)

5.3-Malware Attacks

The top three social media issues negatively experienced by organizations include: employees sharing too much information, the loss of confidential information and increased exposure to litigation (Wilcox et al, 2014). Other equally important results include losses concerning employee productivity and increased risk of exposure to virus and malware (Almeida,2012).

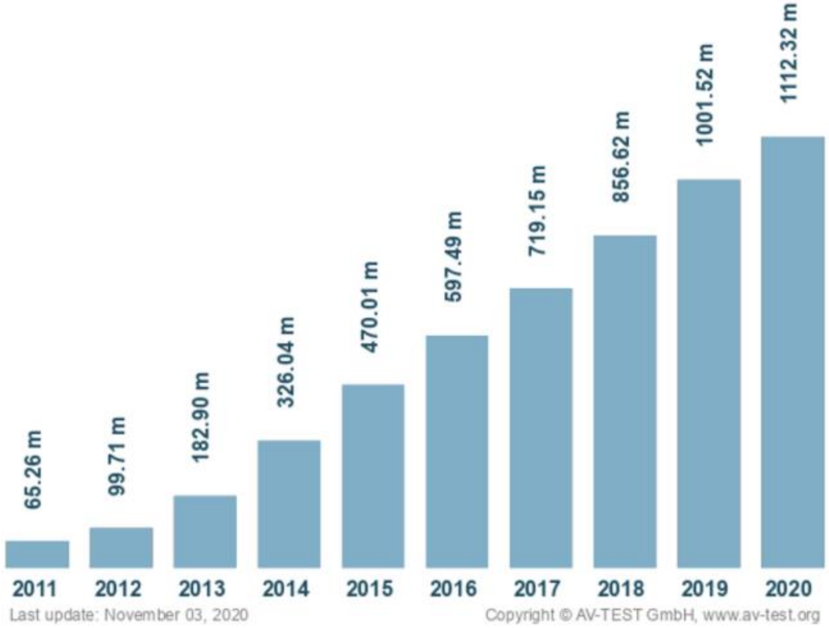

Fig. 4 Numbers of Malware Produced each year

The goal of malware attacks is to attain the personal privacy of the users. One of the most common malware attacks is fake profile and Sybil attack. Criminals can make easily a lot of accounts by using fake personalities in social media networks. As a result of using convenient authentication procedures the criminal just need only a new email in order to make fraudulent profile. Fraudulent accounts led to Sybil *attacks* which can be used improperly. For instance, criminals can exploit their fraudulent accounts to establish new links with covered personalities so as to attain data about some people. By using these fraudulent approaches, they may achieve more data than using legal approaches. In addition, criminals may exploit fraudulent accounts in improper way such as spreading spam emails, illegal hurtful material such as malware and phishing connections. The best countermeasures against fake accounts are use proper authentication procedure as well as powerful identification. Below Table 1. Shows details of main attacks on the social media platforms.

Categories	**Attacks**	**Countermeasures**	**Attacker Goals**	**Link Method**
Identity theft/ Personal Information Attack	DeAnonymization	Identity Separation	Personal Information, Identity	Indirect
	Neighborhood Direct	Proposed Schemes	Privacy	Indirect
	Profile Cloning	Educate the Social User	Personal Information, Identity	Direct
	Existing Profile Cloning	Educate the Social User	Personal Information, Identity	Direct
	Cross-Site Profile Cloning	Educate the Social User	Personal Information, Identity	Direct
	Social Phishing	Educate the Social User	Personal Information	Indirect
Spam Attack	Simple Spam Attack	Spam filtering/blocking software	Personal Information Malicious Script	Direct
	Email-Based Spam	Spam filtering/blocking software	Personal Information Malicious Script	Direct
	Broadcast Spam	Spam filtering	Personal Information	Indirect
	Context-Aware Spam	Avoid to Share Secret Information	Indirect Personal Information	Direct
	HTTP Session Hijacking	Server use randomized session ID	Cookies	Direct
Malware Attack	Fake Profile	Accept Request after Proper Conformation	Personal Information	Direct
	Social Network API	Proper Authentication Mechanism	Personal Information	Indirect
	Drive-by Download	Educate the Social User	Malicious Script	Indirect
	Shortened and Hidden Links	Educate the Social User	Personal Information	Indirect
	Cross-Site Scripting	Educate the Social User	Cookies	Direct , Indirect
	Clickjacking	Educate the Social User	Malicious Script	Indirect

Table 2: A Classification of Social Network Sites Attacks (Khizar Hameed 2017).

6. Conclusions

Wherever we are, social media gives us the freedom to communicate with our beloved ones whenever we want. But there is a price for this freedom: We cannot realize how social media threatens and harms our real-life relationships because of our seemingly happy digital lives. People's alcoholic, obscene, and similar, ineligible photos with the tendency to share, is a clear proof that social media can damage offline relations.

Although people communicate less face-to-face, about half of the respondents believe that the quality of their relationship is not affected at all, and that their relationship is even better because they connect online with their loved ones. Even though the quality of our relations is improved, people cannot objectively evaluate their online communications. Under some circumstances, people perceive their online communication as hyper personal communication and therefore, they can misread messages on social media and add more comments than necessary.

The research shows that social media does not always make people happy, although it helps to facilitate communication channels, time frames and distance obstacles. It can force relationships, but also makes people feel bad because they are constantly compared to the lives of others. "Like" and the search for social approval lead people to share an increasing amount of private information on social media platforms and risk not only their own, but also their friends, family and colleagues' privacy. For those who decide to leave social media, the fact that they will lose a lifetime of digital memories, including photos and interactions, makes this difficult.

To protect themselves and their relations, people should be more cautious about the information they share on social media and more knowledgeable about the cyber world. This not only reduces risks in the online world, but also prevents damage to relationships in the offline world. For the social media threats and risks to be taken under control there should be some certain measures to be taken into consideration:

> 1-Education of users of social media networks against cyber-attacks is one of the effective counter measures in order to protect their personal information. The appropriate content for security of information and protection of privacy needs to be included in all curriculum of schools in line with their level of needs and understanding.
>
> 2-There are security approaches for many criminal attacks while there are defend mechanisms for the rest attacks. But the attackers are always playing first since security measures tend to be reactionary rather than being proactive due to ever innovative cutting-edge technology and high level of motivation of criminals.
>
> 3-Global social media networks should use developed techniques so as to protect personal information of their users since hackers can crack passwords easily using hacking algorithms.

REFERENCES

Akça, E.B., Sayımer, İ. ve Ergül, S. (2015). "Ortaokul Öğrencilerinin Sosyal Medya Kullanımları ve Siber Zorbalık Deneyimleri." Global Media Journal Tr Edition, Spring, 5(10): 71-86.

Almeida, F. (2012) Web 2.0 technologies and social networking security fears in enterprises. arXiv preprint arXiv:1204

Alam S. and El-Khatib K. (2016). Phishing Susceptibility Detection through Social Media Analytics. *In Proceedings of the 9th International Conference on Security of Information and Networks (SIN '16). Association for Computing Machinery, New York, NY, USA, 61–64. DOI:https://doi.org/10.1145/2947626.2947637*

Arsoy, A. ve Ersoy, M. (2015). "Üniversite Öğrencilerinin Sosyal Ağlardaki Siber Zorbalık Tutum ve Davranışları." İletişim Çalışmaları. (Der.) Özgür A.Z. ve İşman A*., Sakarya Üniversitesi Yayını: Sakarya, (134),* 353-368.

Bhutkar, Pallavi Powale & Ganesh. 19,July 2013. "Overview of Privacy in Social Networking Sites (SNS)." *International Journal of Computer Applications* 74.

Borazjani, Amirhossein Mohtasebi &Pernian. 2010. "Privacy Concerns in Social Networks and Online Communities." *VALA.*

Boyd, Danah M. & Nicole B. Ellison (2008), "Social Network Sites: Definition, History, and Scholarship", *Journal of Computer-Mediated Communication, 13* (2008),210-230.

Cao C., Caverlee J. (2015) Detecting Spam URLs in Social Media via Behavioral Analysis. In: Hanbury A., Kazai G., Rauber A., Fuhr N. (eds) *Advances in Information Retrieval. ECIR 2015. Lecture Notes in Computer Science, vol 9022. Springer,* Cham. https://doi.org/10.1007/978-3-319-16354-3_77

Cui, A., Zhang, M., Liu, Y., Ma, S. (2011) Are the urls really popular in microblog messages? In: *CCIS*

Çaycı, B. (Şubat, 2014). International Trends and Issues in Communication & Media Conference, Dubai.

Çildan, Cihan, Mustafa Ertemiz, H. Kaan Tumuçin, Evren Küçük ve Duygu Albayrak (2012), "Sosyal Medyanın Politik Katılım ve Hareketlerdeki Rolü", *Akademik Bilişim, Erişim*: 05.09.2013, ab. org.tr/ab12/bildiri/205.doc

Dilmaç, J.A. ve Kocadal, Ö., (2019). "Prévenir le cyberharcèlement en France et au Royaume-Uni : une tâche impossible*?." Déviance et Société, 43(3):* 421-459

Donegan, R. (2012). "Bullying and Cyberbullying: History, Statistics, Law, Prevention and Analysis." Elon Journal Of Undergraduate Research in Communications, 3(1): 33-42

Efe, A , Dalmış, A . (2019). Review of Mobile Malware Forensic . The Journal of International Scientific Researches , 4 (3) , 264-282 . DOI: 10.23834/isrjournal.566676

Erdur-Baker, Ö. ve Kavşut, F. (2007). “Akran zorbalığının yeni yüzü: Siber zorbalık.” Eurasian Journal of Educational Research, (27), 31-42.

Eren V., Aydın A. (2014) Sosyal Medyanın Kamuoyu Oluşturmadaki Rolü ve Muhtemel Riskler *KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi* 16 (Özel Sayı I): 197-205

Gangopadhyay, Dr.Saswati. June 2014. "Social Networks Sites and Privacy Issues Concerning Youths." *Global Media -Indian Edition* Vol. 5/No.1.

Khizar Hameed, Nafeesa Rehman. 2017. "Today's Social Network Sites:A n Analysis of Emerging Security Risks an d their Counter Measures." *International Conference on Communication Technologies (ComTech).* IEEE.

Mahmood, Shah. 2014. *Online Social Networks: Privacy Threats and Defenses.* London: University College London.UK.

Moinuddin, Mohit Gambhir & M N Doja &. 2015. "Novel Trust Computation Architecture for Users Accountability in Online Social Networks." *2015 IEEE International Conference on Computational Intelligence & Communication Technology.*

Narin, B. Ve Ünal, S. (2016). “Siber Zorbalık İle İlgili Haberlerin Türkiye Yazılı Basınında Çerçevelenişi.” *Akdeniz Üniversitesi İletişim Fakültesi Dergisi, (26),* 9-23.

Özdemir, M. ve Akar, F. (2011). “Lise öğrencilerinin siber zorbalığa ilişkin görüşlerinin bazı değişkenler bakımından incelenmesi.” *Kuram ve Uygulamada Eğitim Yönetimi, 17(4),* 605- 626.

Rodrigues, T., Benevenuto, F., Cha, M., Gummadi, K., Almeida, V. (2011) On word-of-mouth based discovery of the web. In: *SIGCOMM*

Sinnott, Shuo Wang & Surya Nepal & Richard. 2016. "Privacy-protected Social Media User Trajectories Calibration."

Strufe, Leucio Cutillo & Mark Manulis and Thorsten. 2011. *Security and Privacy in Online Social Networks.* Eurecom ,Sophia Antipolis ,France.

Stuart E. Middleton, Giorgos Kordopatis-Zilos, Symeon Papadopoulos, and Yiannis Kompatsiaris (2018) Location Extraction from Social Media*: Geoparsing, Location Disambiguation, and Geotagging. ACM Trans*. Inf. Syst. 36, 4, Article 40 (October 2018), 27 pages. DOI:https://doi.org/10.1145/3202662

Tamer, N. ve Vatanartıran, S. (2016). “Ergenlerin Teknolojik Zorbalık Algıları ve Buna Yönelik Teknolojik Zorbalık Farkındalığı Eğitimi: Pilot Uygulama.” *Yeni Medya Çalışmaları II. Ulusal Kongre Kitabı, Alternatif Bilişim Derneği*: 54-66.

Uçanok, Z., Karasoy, D. ve Durmuş, E. (2011). Yeni Bir Akran Zorbalığı Türü Olarak Sanal Zorbalık: Ergenlerde Yaygınlığı ve Önemi. *108K424 no’lu TUBİTAK Projesi.*

Wilcox H., Bhattacharya M., Islam R. (2014) Social Engineering through Social Media: An Investigation on Enterprise Security. In: Batten L., Li G., Niu W., Warren M. (eds) Applications and Techniques in Information Security. ATIS 2014. *Communications in Computer and Information Science, vol 490. Springer*, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-45670-5_23

Zhumagaziyeva, A., Koç, F. (2010). Kültürel Etkileşimde Kadınların Giysi Alışkanlıklarındaki Değişimin Mahremiyet Açısından İncelenmesi (Kazakistan ve Türkiye Örneği). *E-Journal of New World Sciences Academy, 5(2),* 113-131.