Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı, S. 10-15, Kasım 2020

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue, pp. 10-15, November 2020

Research Article

Sosyal Medya Kullanımında Güvenlik Riskleri ve Korunma Önlemleri

İlker Kara[1]

[1] Cankiri Karatekin Üniversitesi, Department of Medical Services and Techniques, Eldivan Medical Services Vocational School, Cankiri, Türkiye (ORCID: 0000-0003-3700-4825)

(International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) 2020 – 22-24 October 2020)

(**DOI:** 10.31590/ejosat.818375)

REFERENCE: Kara, İ. (2020). Sosyal Medya Kullanımında Güvenlik Riskleri ve Korunma Önlemleri. *Avrupa Bilim ve Teknoloji Dergisi*, (Özel Sayı), 10-15.

Öz

Sosyal medya kullanıcı tabanlı olmakla beraber büyük kitleleri bir araya getiren kullanıcıların kendi ürettiği içeriği paylaştığı online bir ağdır. Sosyal medya kişiler ve kurumlar arasındaki etkileşimi arttırması nedeniyle günümüzde aktif olarak kullanılmaktadır. Sosyal medya sahip olduğu büyük potansiyeli nedeniyle kötü niyetli kişilerinde dikkatini çekmektedir. Saldırganlarda kurbanlarına ulaşmak için sosyal medyayı aktif olarak kullanmaktadır. Kişi ve kurumları etkileyen geniş çaplı bu tehditlere karşı büyük ölçekli güvenlik yatırımları yapılsa da kesin olarak çözüm bulunamamıştır. Bu çalışmada, sosyal medyada ortaya çıkan güvenlik zafiyetleri, alınabilecek önlemler ve korunma yolları tanımlanarak son kullanıcı farkındalığı yaratılmak amaçlanmıştır.

Anahtar Kelimeler: Sosyal medya, Sosyal Ağlarda Saldırı Türleri, Güvenlik Açıkları.

Security Risks and Safeguard Measures in Social Media Usage

Abstract

The social media is a user-based online network that brings large masses together, where users share their own content. Social media is actively used today since it expands the interaction between individuals and institutions. Due to its great potential, social media also attracts the attention of malicious individuals. The attackers also use social media actively to reach their victims. Although large-scale security investments are made against these widespread threats affecting individuals and institutions, no definite solution has been found yet. In this study, it was aimed to increase awareness of end-users by identifying the security weaknesses in social media, measures that can be taken and the ways of protection.

Keywords: Social media, Types of attacks in Social Networks, Safety Vulnerabilities, Computer Security, Malware.

1. Introduction

With the advances in technology and the spread of the Internet, social media has gained a place in the lives of users and has already replaced other traditional media [1-4]. Social media, compared to traditional media platforms, has provided a free and the largest platform for social sharing [5]. The user-based social media is actively used by many brands for quick and direct communication with potential customers [6]. Social media, which is evolving and becoming gradually more widespread, has become an indispensable communication tool not only for individuals, but also for institutions and brands, and it has become a necessity for individuals and institutions to show a presence in social media. In addition to the convenience, it has brought the problem of security in social media [7-8].

The negative effects related to social media show that the new threats, dangers and types of crime emerged, in spite of the benefits of these platforms [9-10]. Despite the personal sharing, rapid access to information, and creation of communication groups, it is a fact that it's possible to jeopardize personal information through social media [11].

[1] Sorumlu Yazar: Cankiri Karatekin Üniversitesi, Department of Medical Services and Techniques Eldivan Medical Services Vocational School, Cankiri, Türkiye, ORCID: 0000-0003-3700-4825, karaikab@gmail.com

The main contributions of this paper are summarized as follows:

• Social media security weaknesses,

• Social media types of attacks, ways of protection from these attacks and what to do after an attack are discussed.

The rest of this paper is organized as follows. Similar studies (social media) in the literature are reviewed in Section 2. Section 3 provides a detailed classification of security vulnerabilities in social media. Finally, the implication of the results and discussion and conclusion are given in Section 4 and Section 5, respectively.

2. Related Work

Among the innovations of the Internet brought to the virtual world, social media is the fastest-growing and widespread invention [12-14]. As an online platform, in which people communicate with each other regardless of distance, social media has evolved by strengthening the existing and new relationships [10].

These social networks, which allow people and corporate brands to define their profile and share their knowledge, have received great attention by almost everyone due to the many advantages and facilities they bring [15]. Social sharing platforms are created for individuals to share their knowledge or to get opinions of others. For this purpose, many social sharing platforms with similar or different characteristics have been developed [16].

The first social media site Geocities has been developed in 1994 [17]. In 1995, heglobe.com gave users the freedom to personalize their online experience by publishing their content and allowed them to communicate with individuals of same interests. These are the first examples of social media.

Between 1995 and 2009, there were sites, where various ethnic groups shared their personal and professional profiles [18]. As of 2009, they have become a world culture, spreading all over the world.

2.1. Types of Social Media

Social media can be defined as a social network where users can express themselves and can communicate with other users in a virtual environment that keeps their personal information. Social media users create a personality description for other users by creating profiles containing their personal information. These personal profiles usually contain brief biographies, various photographs and personal information. In addition, social media allows people to comment on other users' shares in their profiles (such as pictures or videos) by commenting or liking them as well as allowing them to share the content they liked in their own groups.

Generally, social media is used in a large area thanks to its vast potential, where political groups can make propaganda, people can make education and career plans, and where corporate brands reach their potential customers and employees through job postings.

With the use of Internet in smart mobile phones and similar devices, social media platforms are developed in order to give users instant access to information. In this way, users participate in social media actively and faster, for longer online presence. Social media can generally be grouped as follows [19]:

• Social Sharing: Facebook, Twitter, Whatsapp, Line, Messenger

• Photo Sharing: Instagram, Flicker, PhotoBucket,

• Video Sharing: YouTube, Periscope,

• Professional Networking Sites: LinkedIn, Ning.

• Blogs: Blogger.com, Wordpress

• Information sites: Wikipedia, Wetpaint, PBWiki

• Content tagging: MERLOT, SLoog

• Virtual Word: SL, Active Worlds, There, Whyville, Club Penguin, HiPiHi

In addition to the benefits of social media, it has harmful aspects such as violation of some personal information, misuse, and the loss of prestige and customers in commercial institutions. Attackers use social media to reach their victims more easily. For this purpose, specially designed malware infects victims' systems via social media. This is a major security threat for social media users [20].

2.2. Problem of Security in Social Media

Social media is the focus of attention of the individuals and corporate brands due to its higher potential, considering the number of users. This attracts malicious people. The data of corporate or personal accounts in social media are targeted for attacks to capture private information (such as banking information, personal data). This undesirable situation leads to debate on the security problems of the social media platforms [21].

Unfortunately, this threat continues to grow day by day and many users suffer moral and material damage [22]. The root cause of the security vulnerabilities in social media is the failure to comply with the principles of privacy due to the nature of these platforms, which their management and control is hidden from the users.

Social media users think that their shares are only visible to their friends or friend groups. They do not think that malicious people can see these shares and use them for their own benefit.

It is necessary to raise awareness to deal with this huge security threat that users face. Users who do not have adequate information on this issue are the targets of the attackers. This group of users often uses personal information (such as date of birth) in their social media username and passwords, posing an important security threat. When they share the answers of the secret questions, used to recover forgotten passwords, attackers easily gain access to their accounts.

Attackers also use the photos of the social media users without permission for different purposes. With these photographs, fake profiles can be opened in social media and can be used to exploit the victim's friend groups or other users. With these fake accounts, they ask for money from the user's friends, and use the victim's profile information for harassment, abuse or as a content in pornographic websites.

Many social media platforms place commercial advertisements because of the user potential they have, and these ads can direct users to different malicious websites by using weaknesses of users. Attackers can use fake profiles to trap especially younger users for the abuse and harassment.

3. Irelated Classification of Security Vulnerabilities in Social Media

In social media, online games as well as chat, image and video sharing and instant communication are the most preferred entertainment tools or applications. This good, useful, fun, or adorable view of social media is often preferred by attackers for their malicious intentions.

Social media, which is almost impossible to ignore due to its benefits, brings many threats and dangers. The list of the most common threats today are as follows:

3.1. Malicious Software

Malicious software is a generic name for specific software designed to disrupt the operation of the target system, steal information from the user, or enable unauthorized access to target systems [22-23].

Virus software, Worms, Trojan horse, backdoor, Ransomware, and spyware software are among the malicious software [24-25]. Malwares can be classified according to their functions and purposes [26]. Most of the known types of malicious software are as follows [27]:

• Adware: These malwares display advertisements, prepared by commercial brands to reach the user, on the user's screen without the consent of the user. The user is forced to click the ad to close it. In this way, the attackers make profit by referring the user to the commercial firms of the ads.

• Spyware: The malwares are designed to collect data without the user's consent and knowledge. Spyware malwares are usually kept hidden in a downloaded software, and infect the user's system without being noticed. Unlike Adware, they collect personal information from the user, in addition to displaying ads of specific companies.

• Keylogger: An attacker, who wants to capture personal data, sends this application first by email, etc. to monitor and record key presses in the victim system.

• DNS Routing: The attacker routes the network traffic of the victim to a fake but looks authentic social media website that prompts user to enter his/her email and password. This fake website displays a false error message that tells user that he/she entered incorrect password, and then redirects user to the actual website.

• Virus: These malicious software are designed to delete files on the system or stop the operations of the target system completely. Viruses can replicate themselves and spread by infecting different systems. There are many varieties of viruses according to their intended use.

• Trojans: They infect the victim's system usually by a downloaded attachment or a specially designed e-mail to update a program that is usually out of date without being noticed by the user. There are various types of malicious software depending on the design objective, such as modifying or deleting the files in the system, and opening a backdoor to provide a remote access to the attacker for stealing user's personal information.

• Rootkit: Similar to Trojans, they provide remote access to the attacker.

• Exploit Attacks: Finding and using several vulnerabilities in operating systems and programs are called exploit attacks. This software can access the passwords of the user in the infected system.

• Ransomware: Ransomware is one of the most important cyberthreats in recent years. What makes ransomware unique is its higher success rate and unfair profit. The ransomware infects the system through the misleading shares in social media and deceptive attachments in e-mails sent by the attacker. After infecting the victim's system, the ransomware encrypts the files and demands money for allowing access the encrypted files in the system. And, they ask virtual money bitcoin for the transfer. The number of ransomware has increased with the widespread use of bitcoin throughout the world.

Ransomware can be divided into two types [28]. The first one is the locker-ransomware. This type of ransomware usually locks the user's system and requires the victim to pay a fee to have access. The attacker leaves the locked computers open only to allow the user to interact with ransomware and make ransom payments [29-30].

The second type is the crypto-ransomware that prevents access to files by encrypting the victim's personal files. This kind of ransomware is designed to find and encrypt valuable data stored on the computer. The victim cannot access the encrypted data unless the decryption key is received. In both cases, the victim is forced to pay ransom fees.

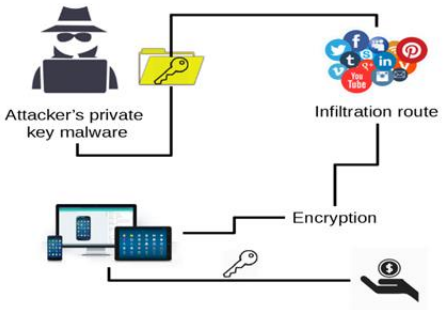

Figure 1. How Ransomware Works.

3.2. Hacking

The attackers design specific password cracking programs to own accounts on social media platforms, which are widely used today. They perform malicious attacks for capturing user accounts, automatic tweets, and link-sharing/commenting through bots, by taking advantage of the user's carelessness or system exploits.

The accounts owned can then be added to bot nets. With this bot network, organized attacks can be made to the desired systems or networks. Unfortunately, social media is unprotected against bot attacks.

3.3. Attacks for Collecting Personal Information

These attacks are made to collect personal information from the individuals, groups or brands targeted at social media. Attackers can collect specific information, such as user name, date of birth, etc. using especially the metadata content of the photographs shared in social media. They use this information for gaining access to user accounts and use the victim's profile information for harassment, abuse or as a content in pornographic websites.

3.4. Social Media Security Measures

Measures to be taken on social media platforms can be considered as personal and legal measures [20]. Personal precautions require user awareness. User awareness covers a wide range of areas from knowing the features of the social media platform to its technical infrastructure. Legal measures are intended to eliminate the damages that may arise without limiting the freedom of users at the local and international level.

3.5. Personal Measures

Awareness about the threat of attack lies at the heart of the measures to be taken. Personal information should not be given in detail in social media accounts. Although there is a legally-specified age limit on social media platforms, this rule is usually ignored. The threat poses risks to both adult and younger users. Families should protect their children from the threats and dangers of social media. Necessary training should be provided and awareness should be raised in children in this regard.

Identity information should never be shared on social media platforms. In particular, giving information such as photos, home addresses and location notifications attract malicious people. In addition, giving location notification paves the way for thieves. In order to prevent social engineering attacks, individuals should not be participated in political, sportive, etc. group, which they are not familiar with, and should not accept such friendship requests.

Some working groups (such as police, soldiers) create social media groups according to their district, working area or specialty. Individuals in these groups should be very careful considering that attackers will try to infiltrate these groups. If not mandatory, these groups should never be created.

Technological measures that can be taken are as follows: Before being a member of a social media platform, privacy policy, terms and conditions of use should be read in order to understand the threat and danger that can be encountered. The things can be done one the platform and the worst-case scenario should be considered before starting to use the platform.

Attackers use e-mail as the most common method of infiltration through social media. For this reason, one should not open such fake e-mails with suspected origins. AntiSpam products should be used in user e-mail systems. Remote access port should be changed (when possible, port numbers should have at least five digits), restricted accounts and strong passwords should be generated for remote-access users and remote access should be closed when not used. As a basic security measure, the software of all systems should be up-to-date, systems should be protected with a reliable Internet Security software, sandbox and spam filters should be used to protect against malware.

3.6. Legal Measures

The legal measures that can be taken are as follows: Users need to fully read and understand the membership agreements on social media platforms, and they need to be aware of the risks and threats that can be encountered because of the information they share. The "Convention on Cybercrime", which is the first international convention on the crimes committed through the Internet and computer networks, covers the protection of freedoms, human rights and security in a virtual environment and the reduction of risks. The convention has been ratified by 33 countries. This convention has articles on crimes such as "illegal access", "data interference with", "system interference", "misuse of devices", "computer-related forgery", "computer-related fraud", "offenses related to child pornography", and "offences related to infringements of copyright and related rights". The parties to the convention cooperate in the fight against these crimes. In the legal sense, increasing the number of states that sign this convention will be effective in the fight against crime.

4. Results and Discussions

The ongoing advances in communication technologies and methods have enabled a very intense and fast flow of information in the online environment, especially on social media platforms, using the advantages offered by the Internet. Governments, online stores, advertising companies or malicious attackers want to control this flow of information for different purposes to be used for their own benefit.

This leads to violations in the online security and privacy in the Internet infrastructure, and transforms the social media platforms increasingly insecure and privacy-free environments.

The protectiveness the measures that can be taken against the security vulnerabilities and weaknesses of in social media platforms, which include personal measures, technological measures and legal measures, is still controversial. Is it possible to identify threats on social media platforms in advance?

Many social media platforms can be used for strategic, available, operational threat intelligence purposes with their accessible and widespread data. This gives the social media platform security and operational units a great advantage for detection of potential threats and attacks in advance. These perceived threats are evaluated by security teams to help eliminate or isolate the threats and prevent them from becoming a problem or to solve potential problems.

These measures to be taken will help raise and awareness about the security vulnerabilities of social media platforms as well as a better understanding of the importance of critical and sensitive data kept on social media platforms.

5. Conclusion

Today, social media has become a platform for both commercial and ordinary users. Thanks to social media, new job descriptions or even new occupations have been formed. Companies can get user feedback and comments about their products in social media. Using these open source data, they can learn about the target audience and the criticism and demands about the products. It is possible to see whether the message given by a politician leads to the desired reaction, through research on the social media data. Ads designed to politically direct undecided masses are sent to users without their consent to create a public perception.

Despite its many benefits, social media can harm personal or corporate reputation when used improperly. It may cause bankruptcy of companies or layoffs. In addition, the collection of open source big data from the social media users can be used for different purposes or even transformed into alternative products. Attackers look for recent security vulnerabilities in social media. And, they use personal and institutional data for profit.

The biggest disadvantage of the crimes committed in the virtual environment is that the probability of arresting and punishing the perpetrator of this crime is quite low. Therefore, there is a huge increase in the crimes committed in the virtual environment all over the world. Checking social media security and privacy settings once a month will reduce the possibility of being attacked. The majority of social media users provides correct personal information in their profiles. It should be kept in mind that social engineering attacks on social media are extensive and that one should be careful about the information to be shared.

The vast majority of users are aware that personal information can be misused. In spite of this, e-mail address, personal photos and birth dates are frequently shared by users on their profiles. Users also provide location information on social platforms. In this case, malicious people can find users in shared venues, or those who know that they are outside can also commit a burglary. Social media

users are vulnerable to spam or malware attacks. For this reason, it is important that users do not open e-mails that they are not sure about their origin, and that have active spam or anti-malware filters in their e-mail boxes.

It is forbidden for third parties to use other people's accounts without consent. However, it is known that attackers open face accounts by using profile information of other social media users, and use their photos without the permission of the users. In order to prevent this, it can be recommended that unknown individuals should not be added to social media groups or that safe friend groups should be created to share important information only with them. Finally, end-to-end encryption of the user data can be recommended as an important measure that can be applied by the social media applications in order to prevent third-parties to access confidential data of users.

Acknowledgment

The author was the sole contributor to this paper. This article does not contain any studies with human participants or animals performed by the author. No potential conflict of interest was reported by the author.

References

[1] Ceron A. Internet, news, and political trust: The difference between social media and online media outlets. Journal of Computer-Mediated Communication, 2005;20(5):487-503.
[2] Rice E. Barman-Adhikari, A. Internet and social media use as a resource among homeless youth. Journal of Computer-Mediated Communication, 2014;19(2):232-247.
[3] Primack BA, Shensa A, Escobar-Viera CG, Barrett EL, Sidani JE, Colditz JB, James AE. Use of multiple social media platforms and symptoms of depression and anxiety: A nationally-representative study among US young adults. Computers in human behavior, 2017;69:1-9.
[4] Humphreys L, Von Pape T, Karnowski V. Evolving mobile media: Uses and conceptualizations of the mobile Internet. Journal of Computer-Mediated Communication, 12013; 8(4):491-507.
[5] Lee CS, Ma L. News sharing in social media: The effect of gratifications and prior experience. Computers in human behavior, 2012;28(2):331-339.
[6] Sashi CM. Customer engagement, buyer-seller relationships, and social media. Management decision, 2012;50(2);253-272.
[7] Leavitt N. Mobile security: finally, a serious problem? Computer, 2011;(6):11-14.
[8] Joshi P, Kuo CC J. (2011, July). Security and privacy in online social networks: A survey. In Multimedia and Expo (ICME), 2011 IEEE International Conference on (pp. 1-6). IEEE.
[9] Grégoire Y, Salle A, Tripp TM. Managing social media crises with your customers: The good, the bad, and the ugly. Business Horizons, 2015;58(2):173-182.
[10] Weinberg BD, Pehlivan E. Social spending: Managing the social media mix. Business horizons, 2011;54(3):275-282.
[11] Goh DHL, Ang RP, Chua AY, Lee CS. (2009, October). Why we share: A study of motivations for mobile media sharing. In International Conference on Active Media Technology (pp. 195-206). Springer, Berlin, Heidelberg.
[12] Kietzmann JH, Hermkens K, McCarthy IP, Silvestre BS. Social media? Get serious! Understanding the functional building blocks of social media. Business horizons, 2011;54(3):241-251.
[13] Bakardjieva M, Smith R. The Internet in everyday life: Computer networking from the standpoint of the domestic user. New Media & Society, 2001;3(1):67-83.
[14] Herring SC. Computer - mediated communication on the Internet. Annual review of information science and technology, 2002;36(1):109-168.
[15] Kotler P, Zaltman G. Social marketing: an approach to planned social change. The Journal of Marketing, 1971;3-12.
[16] Kaplan AM, Haenlein M. Users of the world, unite! The challenges and opportunities of Social Media. Business horizons, 2010;53(1):59-68.
[17] Forkosh BA, Hershkovitz A. A case study of Israeli higher-education institutes sharing scholarly information with the community via social networks. The Internet and Higher Education, 2012;15(1):58-68.
[18] Kwon O, Wen Y. An empirical study of the factors affecting social network service use. Computers in human behavior, 2010;26(2):254-263.
[19] Dawley L. Social network knowledge construction: Emerging virtual world pedagogy. On the Horizon, 2009;17(2):109-121.
[20] Zhang Z, Gupta BB. Social media security and trustworthiness: overview and new direction. Future Generation Computer Systems, 2018;86:914-925.
[21] Gupta R, Brooks H. Using social media for global security. John Wiley & Sons. 2013.
[22] Makridakis A, Athanasopoulos E, Antonatos S, Antoniades D, Ioannidis S, Markatos EP. Understanding the behavior of malicious applications in social networks. IEEE network, 2010;24(5).
[23] Liu BH, Hsu YP, Ke WC. Virus infection control in online social networks based on probabilistic communities. International Journal of Communication Systems, 2014;27(12):4481-4491.
[24] Abraham S, Chengalur-Smith I. An overview of social engineering malware: Trends, tactics, and implications. Technology in Society, 2010;32(3):183-196.
[25] Kunwar RS, Sharma P. (2016, March). Malware Analysis: Tools and Techniques. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (p. 144). ACM.
[26] Santos I, Brezo F, Sanz B, Laorden C, Bringas PG. Using opcode sequences in single-class learning to detect unknown malware. IET information security, 2011;5(4):220-227.
[27] Rao UH, Nayak U. (2014). Malicious software and anti-virus software. In The InfoSec Handbook (pp. 141-161). Apress, Berkeley, CA.
[28] Kara, İ., Aydos, M. (2019). The ghost in the system: technical analysis of remote access trojan. International Journal on Information Technologies & Security, 11(1).
[29] Kara, I. (2019). A basic malware analysis method. Computer Fraud & Security, 2019(6), 11-19.
[30] Kara, İ., Aydos, M. (2019, October). Detection and Analysis of Attacks Against Web Services by the SQL Injection Method. In 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-4). IEEE.
[31] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
[32] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
[33] K. Elissa, “Title of paper if known,” unpublished.
[34] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
[35] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
[36] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.