ISSN 2319-2720
Volume 9, No.2, April - June 2020
International Journal of Computing, Communications and Networking
Available Online at http://www.warse.org/ijccn/static/pdf/file/ijccn01922020.pdf
https://doi.org/10.30534/ijccn/2020/01922019

Problems in Information Security in Network Sites and Solutions

Dr. Magdi Mohammed Mohammed Ahmed Hamoda
Country Sudan, magdi1079@gmail.com
King Khalid University, College of Arts & Sciences, , Dhahran Aljanoob, KSA
Nile University – Khartoum - Sudan

ABSTRACT

Data security and computer hardware is a type of technology known as information security, which is applied to computers and networks. The goal of computer security includes protecting information, data, and the characteristics of scientific knowledge from theft, change, or natural disasters, while information and data can remain productive and available to targeted users. Computer system security terms mean the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering, or collapsing as a result of unauthorized or unreliable activities, and unplanned events, respectively, to solve information security problems on networks. Via the website. We must get to know what is related to the concept, and that information, data and device security is a type of technology known as information security, which is applied to computers and networks. The goal of computer security includes protecting scientific information, data, and scientific knowledge from theft, modification, or natural disasters, while information and data can remain productive and available to targeted users. Computer system security terms mean the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering, or collapsing as a result of unauthorized or unreliable activities, and unplanned events, respectively, to solve information security problems on networks. Via the website. We must get to know what is related to the concept and the basic structure of the social network site and other related social networks. Usually the social services network in the internet area indicates: the network address, the social network service and software, and the social network site. These three things are clearly interconnected and indispensable. It is combined to create a platform for users to communicate information.[1]

.

Key words: Security, and protection of information, privacy on social networking sites.

1. INTRODUCTION

Life became easy in terms of communication after the emergence of social networks that simplified forms of communication between societies these days. As it reflects the social image of each user. They can keep them connected and stick to their symbolic images for hours together. The network of social relationships that accumulate during your daily life can be translated simply to your "profile" and made available to all your friends to see. Then there is the "follow-up" concept that could turn the Bedouins into a Rock star. The world of photos that you directly share has made you more. It feels like everyone is out of psychological distress and individual isolation and has become amusing. ”But the more comfortable and connected we become with these sites, the more casual and neglectful we are to share personal details about ourselves with hundreds of millions of people who use a wide range of social networking sites (SNSs) , As it makes you communicate with a number of users to a number of different countries combined with each other, but there is absolutely no doubt that social networks have become an obsession for every user of the Internet these days and that the trend will increase in communication, although we do not forget that there will be problems Make use of this technique.[12]

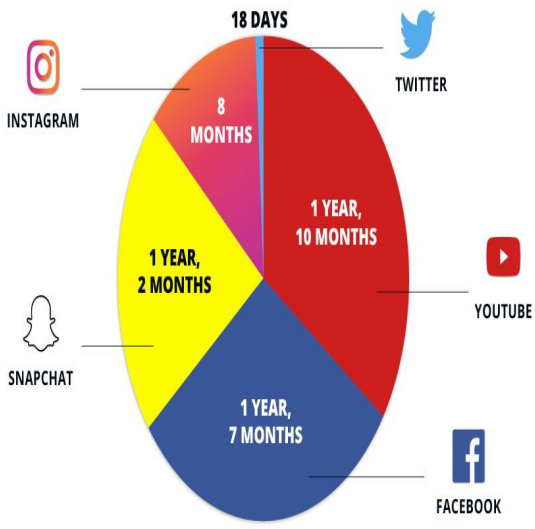

Figure 1: Indicate the number of users on social media

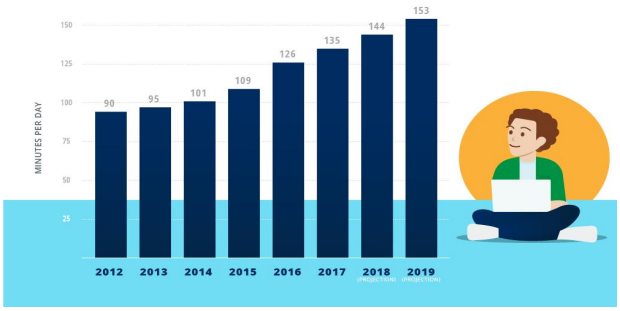

Figure: 2: Indicatesthe percentage of social media users in the world

Table 1: list of the largest social networking services

Service	Active users (in millions)
Facebook	2,498
YouTube	2,000
WhatsApp	2,000
Facebook Messenger	1,300
WeChat	1,165
Instagram	1,000
TikTok	800
QQ	731
QZone	517
Sina Weibo	516
Kuaishou	400
Snapchat	398
Twitter	386
LinkedIn	310

Even though the use of social network web sites and applications is increasingly day by day, but users are not aware of the risks associated with uploading sensitive information. The reason why cyber-conspirators prey on these networks is because users upload their personal information that commonly include their interests, social relationships, pictures, confidential information and other media content, and share this information to the whole world via SNSs, which are very easily accessible. Employees, too, unknowingly share plethora of personal information on SNS thus putting their corporate infrastructure and data at a risk. The volume and ease of accessibility of personal information available on these sites have attracted malicious people who seek to exploit this information. Due to the sensitivity of information stored within social networking sites, intensive research in information security has become an area of paramount importance. Facts reveal that most social media users post risky information online, unaware of the privacy and security concerns. Social networking sites are meant to get as many users in one place as possible on one platform and for attackers there is a lot of return-on-investment in going after them. The values at the core of networking sites – openness, connecting, and sharing with others - unfortunately are the very aspects which allow cyber criminals to use these sites as a weapon for various crimes. Without a careful security policy in place, the entertaining face of social networking could easily compromise on the social stature of an individual. The dramatic rise in attacks in the last year tell us that social networks and their millions of users must do a lot more to protect themselves from organized cybercrime, or risk failing to identity theft schemes, scams, and malware attacks. Understanding these risks and challenges should be addressed to avoid potential loss of private and personal information. Social networking must to be integrated into the information security policy and user education. [9]

2- GENERAL DESCRIPTION OF THE SOCIAL NETWORK

Solving the problems of information security on the social network website, we must learn about the basic concept and structure of the social network website and its associated social network. The social network of services in the Internet

zone usually refers to social network service, social networking programs and social network website. Clearly, these three things are interlinked and indispensable; they are combined to form a platform for users to communicate information and share feelings. [13].

3. SOCIAL NETWORK SECURITY

3.1 Summary of security of social networking sites

When there are security holes in the site itself, they can lead to unimaginable damage to information security for users. For example, most security vulnerabilities are in well-known site, which is caused by a loose site filtering that gives hackers opportunities to introduce malicious software through security vulnerabilities to obtain account information from the webmaster. With the account, hackers can modify the webpage and add malicious code across the rear stage of the site. When users view the page, it will automatically redirect the view to another Web site or start downloading the Trojan virus. At the same time, more and more users have access to the Internet through mobile phones, and security issues become worse. Many users face telephone calls being intercepted, a message and information from people who are being contacted stolen, and attacked by viruses while downloading audio or video files.

3.2 Security analysis of social networking sites

Security issues from social networking platforms not only associate with the traditional computer security network, but also contain different features of the traditional computer network. Therefore, they face different threats in their actual applications. At present, threats can be divided into two categories: traditional security threats and threats arising from mining techniques in history.[20]

4- PROS AND CONS OF SOCIAL MEDIA SITES

First: The pros of social media sites

• Social networking sites contribute to maintaining constant communication with friends and family, removing borders and distances, and keeping in touch with the most important news sites to learn about the important events that affect our lives.

• Social networking sites contribute to the exchange of experiences and cultures around the world through the dissemination of the cultures of nations and peoples, and this contributes greatly to the dissemination of the concept of acceptance of the other through the recognition of the habits of different peoples.

• From the positives of social networking sites, it helps to access and benefit from all scientific research and contributes to increasing knowledge and public culture.

Read/Z: definition of technology and what types of technology?

• Social networking sites provide more job opportunities through the design of special pages that provide their owners with a fixed income, as they can be used to promote products and thus take advantage of e-commerce that has become offering multiple opportunities for action.

• Many social media sites are trying to spread peace among religions by creating special pages for interfaith coexistence and bringing together views and ideas.

Second, the top five bad things social media has caused

1) Weak human relations...
2) Lack of sources and many rumors...
3) Lost times...
4) A lot of negative news... [14]
5) Enhance narcissism

And the disadvantages of social networking sites in general

•The individual has become a channel for spreading news without monitoring or ensuring its authenticity to society

•Social media is addictive for many users because they spend a long time browsing these sites and this causes a great waste of time.

• Social media is a privacy violation of many individuals, especially celebrities, to post their own photos and inform them without censorship.

• Social media isolates many individuals when they are away from social life due to the excessive use of social media.

Lack of parental controls on social media, and therefore the entry of children and adolescents to completely immoral sites, which poses great risks for children and adolescents.

• The emergence of the term fake e-commerce, through which some phantom transactions that cannot be pursued often are made, and this is a waste of money for some users.

• Disseminating false and largely unreliable news and rumors, and thus some news floundering, that their credibility is often unverifiable. [17]

5-SECURITY ISSUES FROM SOCIAL NETWORKING PLATFORMS

Not only associate with the traditional computer security network, but also contain different features of the traditional computer network. Therefore, they face different threats in their actual applications. At present, threats can be divided into two categories: traditional security threats and threats arising from mining techniques in history.

5.1. Traditional Security threats

Conventional security threats can be categorized as follows:

1) Contact sub-sections

Traditional messages are usually communicated through e-mails, especially including various types of commercials and malicious links. In social networking sites, by paying for friends of users, this unwanted information is spread between wider and expanded at faster speed in the Internet.

2) Third-party programmer and plug-ins

Like other platforms, social networking sites also offer a free open interface for application programs. Any user can develop an embedded program according to his or her needs. While providing convenience to users, these are the most hidden risks that contain huge.

3) Disable System availability

By increasing Network load, redirecting user requirements and malicious network data, hackers can affect the proprietary network and system service to steal user information.

4) Stealing username and password

This is the most conventional attack, which can also cause the greatest damage. Stealing the username and password means all the personal information of the user in the social network website exposed to the hacker. Next, the hacker can do anything without discovering the user's identity.

6- OTHER WAYS TO SECURE AN ACCOUNT

Typing a username and password into a website is not the only way to identify yourself on the web services you use.
a) Multi-factor authentication uses more than one form of authentication to verify an identity. Some examples are facial recognition, iris recognition, voice ID, and finger scanning.
b) Two-factor authentication uses a username and password and another form of identification, often a security code in the form of a "Captcha", or likewise. One of the main reasons why social media has so many loopholes is the trust factor. We think that the people we are dealing with are our friends, our colleagues, our favorite sports teams, magazines, or food brands and thus they cannot be "fake" or "criminals". This is the point where the actual criminals take advantage of your trust to retrieve your information.[18]

7- CONVENTIONAL ATTACKING SCENARIOS

1. CBIR (Content Based Image Retrieval): In this scenario, the attacker can know the location of a user by matching the patterns of the images associated with the profile of the user 1. These types of attacks are done to know the current location of the user.
2. Click jacking: This is another type of attack scenario in which attacker posts some videos or post to the victim and when victim clicks on the page, some malicious actions are performed. This is common in Facebook with the name like jacking that is when a user likes a page, a picture or a video the user is trapped by the attackers [4]. This type of attacks are done to do malicious attack or to make some page popular.
3. NeighborhoodAttack: Theneighborhood attacks are done by the attackers by knowing the victim's neighborhood [4]. It means the attacker knows the friends of the victim. Attacker uses the relationship among these friends and based on this relationship tries to identify the victim.

8- NEW ATTACK STRATEGY WATERING HOLE

In January 2013, the attackers used to a new approach to make SNSs user insecure. The attack was done on Facebook. The attackers hacked a mobile developer forum and when developers visited the forum; their system got infected with a MAC Trajon [5]. This attack was not done to steal profile information or funds, but it was done to infect the system of developers. After attacks on Facebook, the same attack was done on many other companies, not only on SNS, but on their insecure sites as well.

9- PREVENTION STRATEGIES

Limit the "amount" - Limit the amount of personal information you post. Do not disclose information such as your residential address or information about your upcoming schedule or your daily routine. Also, be considerate when posting information, including photos, videos and other media content

1. Internet is always "public" Always remember that anything that you post on the internet is always available to the public. Thus, it is your responsibility to post information that you are comfortable with anyone seeing. This includes your personal information and photos you post and those in which you are tagged in.Also, once you post information online, you cannot delete it. Even if you remove the information from a site, cached [6]
2. be sceptical - Do not believe in all that you read online. People make many mistakes and do post false or misleading information about different topics, including their own identity information. This is not necessarily done with a malicious intent since it could be unintentional, an exaggeration of any topic, or simply a joke that one may misinterpret. Take appropriate precautions, though, and make sure you verify the authenticity of any information before taking any action. As said before, common sense should matter more.[7]

10- PROPOSED SECURITY PROTOCOL

Security is one of the significant challenges, which limit users
From taking the full advantage of cloud computing.
Accordingly, many users have concerns about saving their
Sensitive data in insecure place. Therefore, we need a protocol
That verifies confidentiality, authenticity, integrity, and
Non-repudiation of data transmission in the cloud.[25]

11- DIFFERENT LAYERS SECURITY

There are a lot of researches being conducted to offer a
Dependable distinct architecture of security, which can assure
the security and privacy of data. [6]

11.1 Perception Layer

Perception Layer is IoT architecture bottom layer which offer
a variety of hardware security features. It provides four
Essentialprinciples, which are Data Privacy, verification,
Sensitive information Privacy and Assessment of Risk.

11.2 Network Layer

The network layer that can be wired or wireless is also having
the risk of various types of attacks. Because of the openness of
Wireless waterway, infrastructure can be observed without

Difficulty by the hackers. The security of the network layer is divided into 3 categoriesAs shown in the figure below[26].

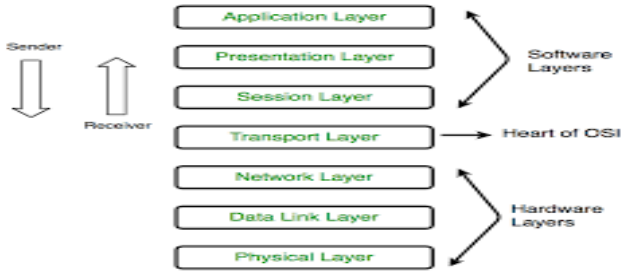

Figure 3: The security of the network layer is divided into 3 categories

12- CONCLUSION

Computer system security terms mean the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering, or collapsing as a result of unauthorized or unreliable activities, and unplanned events, respectively . That information, data and device security is a type of technology known as information security, which is applied to computers and networks. The goal of computer security includes protecting scientific information, data, and scientific knowledge from theft, modification, or natural disasters, while information and data can remain productive and available to targeted users.That information, data and device security is a type of technology known as information security, whichis applied to computers and networks. The goal of computer security includes protecting scientific information, data, and scientific knowledge from theft, modification, or natural disasters, while information and data can remain productive and available to targeted users. Computer system security terms mean the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering, or collapsing as a result of unauthorized or unreliable activities

REFERENCES

1-Fogel J，NehmadInternet social network communities Risktaking，trust。Andprivacyconcerns J-J]·Computers in Human Behavior，2009，25 (1)：53

2-Valter F E，BattistonS，Schweitzer F·A model of a trust based recommendation system on a social networkAutonomous Agents and Multi-Agent Systems，2008，16 [1]-57

3- Sun Jian, Zhu Xiaoyan, liuMomeng, Privacy research to social network security.Journal of network security technology and application, 2011, [10] 76-79.

4-Company Info". Facebook Newsroom. Archived from the original on November 15, 2015. Retrieved April 12, 2018.

5-Thelwall, Mike 2009. Chapter 2 Social Network Sites. Social Networking and the Web. Advances in Computers. 76. pp. 19–73. Doi: 10.1016/S0065-2458(09)01002-X. ISBN 9780123748119.

6-India records highest social networking growth Rate: Study". News.biharprabha.com. IANS. July 26, 2014. Archived from the original on August 3, 2014. Retrieved July 26, 2014.

7- Kaplan, Andreas M.; Heinlein, Michael (January 2010). "Users of the world, unite! The challenges and opportunities of Social Media". Business Horizons. 53 (1): 59–68. doi:10.1016/j.bushor.2009.09.003.

8- The wall, Mike 2009. Chapter 2 Social Network Sites. Social Networking and the Web. Advances in Computers. 76. pp. 19–73. Doi: 10.1016/S0065-2458(09)01002-X. ISBN 9780123748119.

9-Joseph, R. (1993), Touch Me—Feel Me—Feed Me— Kiss Me!, The Naked Neuron, Springer US, pp. 71–98, doi:10.1007/978-1-4899-6008-5_4, ISBN 978-0-306-44510

10- KimYoungae，PhalakRasik·A trust prediction framework in rating-based experience sharing social networks without a Web of TrustInformation Sciences，2012，191 [5]-128·

11- WatermanD，SpenceRP，Van Der Heide B·A social network as information：the effect of system generated reports of connectedness on credibility on Twitter [J]·Computers in Human Behavior，2012·28：199·

12- Wu Huxin, Wu Bo, zhang Ming. Social networks risk's influence on the national information security

13- Michael Lang, Jonathan Devitt, Sean Kelly, Andrew Kinneen, John O'Malley, Darren Prunty"Social Networking and personal Data Security: A Study of Attitudes and Public Awareness in Ireland" 2009 International Conference on Management of e-Commerce and e-Government.

14- Barnes, S. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9). doi:10.5210/fm.v11i9.1394

15- Kumar, A., Gupta, S. K., Rai, A. K., & Sinha, S. (2013). Social Networking Sites and Their Security Issues. International Journal of Scientific and Research Publications, 3(4), 3.

16- Verma, A., Kshirsagar, D., & Khan, S. (2013). Privacy and Security: Online Social Networking. International Journal of Advanced Computer Research, 3(8), 310-315.

17- Deng, X., Bispo, C. B., & Zeng, Y. (2014). A Reference Model for Privacy Protection in Social Networking Service. Journal Of Integrated Design & Process Science, 18(2), 23-44. Doi: 10.3233/jid-2014-0007

18- Bertot, J. C., Jaeger, P. T., & Hansen, D. (2012). The impact of polices on government social media usage: Issues, challenges, and recommendations. Government Information Quarterly, 29(1), 30-40.

19- Vladlena, B., Saridakis, G., Tennakoon, H., &Ezingeard, J. N. (2015). The role of security notices and online consumer behavior: An empirical study of social networking users. International Journal Of Human - Computer Studies, 8036-44. doi:10.1016/j.ijhcs.2015.03.004

20- Kim, H. J. (2012). Online Social Media Networking and Assessing Its Security Risks. International Journal Of Security & Its Applications, 6(3), 11-18.

21- Gundecha, P., BARBIER, G., Jilliang, T., &Human, L. (2014). User Vulnerability and Its Reduction on a Social Networking Site. ACM Transactions on Knowledge Discovery from Data, 9(2), 12:1-12:25. Doi: 10.1145/26304214.

22-Della Porta, D &Mosca, L 2005, 'Global-net for global movements? A network of networks for a movement of movements', Journal of Public Policy, vol. no. 1, pp. 165–190.

23- Granqvist, Manne 2005, The information society: visions and realities in developing countries, in O Hemer& T Tufte (eds), Media and glocal change: rethinking communication for development, CLACSO, Nordicom, Buenos Aires, Göteborg, pp.285 – 296.

24- Heinlein, M & Kaplan, MA 2010, 'Users of the world unite! The challenges and opportunities of social media', Business Horizons, vol. 53, pp. 59-68.

25- Dr. AbdelrahmanElSharifKarrar et al., "Security Protocol for Data Transmission in Cloud Computing" International Journal of Advanced Trends in Computer Science and Engineering, 7(1), January – February 2018, 1- 5 http://www.warse.org/IJATCSE/static/pdf/file/ijatcse01712018.pdf

26- ZeyadHalabi, AbdelrahmanKarrar, "Internet of Things (IoT) : An overview Based on Security Challenges" International Journal of Computing, Communications and Networking, 7(4) October – December 2018, 333-335 http://www.warse.org/ijccn/static/pdf/file/ijccn01742018.pdf

27.https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.geeksforgeeks.org%2Flayers-of-osi-model%2F&psig=AOvVaw3qdgmbHSb_rfOyXXpSysCK&ust=1593876702158000&source=images&cd=vfe&ved=2ahUKEwiAgLrGs7HqAhUL_6QKHZgLDg8Qr4kDegUIARCiAQ