International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228219

Social Network and Data Security Issues

Dr. Magdi Mohammed Mohammed Ahmed Hamoda
Department of Computer Science, College of Arts & Sciences, King Khalid University, Dhahran Aljanoob, KSA

Article Info
Volume 8, Issue 2
Page Number : 149-154

Publication Issue :
March-April-2022

Article History
Accepted: 01 March 2022
Published: 30 March 2022

ABSTRACT

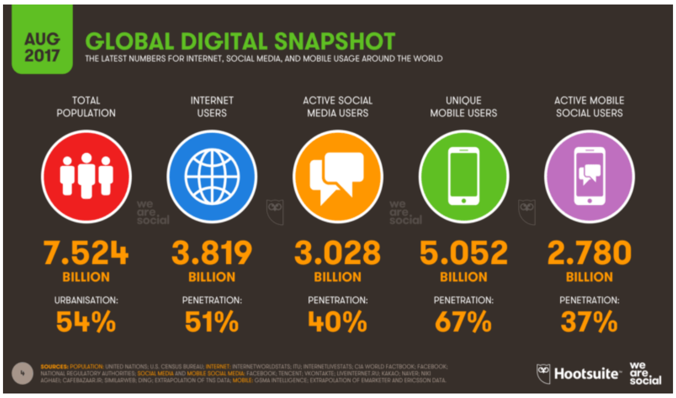
Computer security is a branch of technology known as Information Security, as it is applied to computers and networks. The objective of computer security involves the protection of information and property from theft and corruption, or natural disasters, while information and property can remain productive and accessible to their intended users. Computer system security terminology means the collective processes and mechanisms through which information, sensitive and valuable services are protected from dissemination, and tampering with or collapsing caused by unauthorized or unreliable activities, and unplanned events, respectively to solve the problems of information security on the social network website. We have to 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.

Keywords : Social Networking Sites, Cyber Criminals, Cybercrime, Social Network Security, Security Analysis, Security Threats, CBIR

I. INTRODUCTION

Social networks are one of the easiest forms of communication these days. They reflect the social image of a person. They can keep you glued to your avatar for hours together and make you forget about the whole physical world around you. The network of social relations that build up during your everyday life can be simply translated onto your "profile" and made available for the whole of your friends to see. Then there is a concept of "following" that can turn a nomad into a Rockstar. The world of pictures you share live has only made your presence felt more. It all seems so entertaining that one would seldom think of leaving this "world" and becoming an offline monk. But the more comfortable and attached we become with these sites, the more casual and careless we are to share personal details about ourselves. People, hundreds of millions of them, use a wide variety of social networking sites (SNSs) that seem no less than a menu card in a restaurant. Facebook, the world's leading social networking site, for example, has more users than the population of many of the countries combined. There is absolutely no doubt that social networks have become a part of every internet user these days and the trend is only set to increase.

Figures -1 suggest that there were about



https://thenextweb.com/contributors/2017/08/07/number-social-media-users-passes-3-billion-no-signs-slowing/

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's 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.

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.

II. 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.

III. 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.

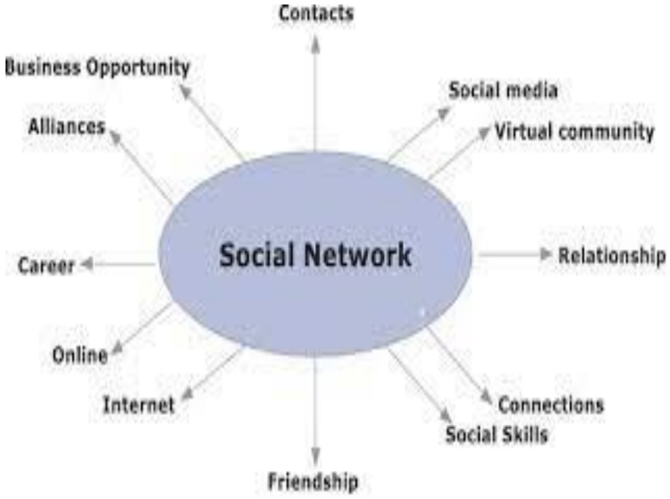
Second: disadvantages of social networking sites

- Social media sites are an addiction to many users because they spend considerable time browsing these sites and this is causing a great waste of time.
- Social media sites are a violation of privacy for many individuals, especially celebrities, for publishing their own photos and telling them without censorship.
- Social media sites isolate many individuals as they move away from social life due to excessive use of social media sites.
- The lack of parental control over social media sites and, consequently, the entry of children and adolescents to completely immoral sites, which pose significant risks to children and adolescents.
- The advent of the term counterfeit electronic commerce, through which some fictitious transactions are held that cannot often be legally prosecuted, and this is a waste of money for some users.
- Publish false and unreliable news and rumours dramatically, thus floundering in some of the news that its credibility is often not verifiable.

IV. 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.

Figure -2 Social network security: Issues, challenges, threats, and solutions , science Direct.com



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 programme 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 isn't 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 favourite 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.

7- Attacking Scenarios

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. This type of attacks are done to do malicious attack or to make some page popular.

3. Neighbourhood Attack :The neighbourhood attacks are done by the attackers by knowing the victim’s neighbourhood. 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. 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 company, 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 can't delete it. Even if you remove the information from a site, cached

2. Be sceptical - Don't 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.

V. ACKNOWLEDGMENTS

National Natural Science Foundation (61373148), National Social Science Fund (12BXW040); Shandong Province Natural Science Foundation (ZR2012FM038, ZR2011FM030); Shandong Province Outstanding Young Scientist Award Fund (BS2013DX033), Science Foundation of Ministry of Education of China(14YJC860042).

VI. REFERENCES

[1]. Fogel J，Nehmad E．Internet social network communities：Risk taking，trust。 and privacy concerns J- J]．Computers in Human Behavior ，2009，25(1)：53.

[2]. Valter F E，Battiston S，Schweitzer F．A model of a trust based recommendation system on a social network[J]．AutonomousAgents and Multi-Agent Systems，2008，16(1)：57.

[3]. Sun Jian, Zhu Xiaoyan, liu Momeng, etc. Privacy research to social network security [J]. Journal of network security technology and application, 2011, (10) : 76-79.

[4]. Kim Youngae，Phalak Rasik．A trust prediction framework in rating-based experience sharing social networks without a Web of Trust[J]．Information Sciences，2012 ，191(5)：128.

[5]. Westerman D，Spence RP，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，2012．28：19.

[6]. Wu Huxin, Wu Bo, zhang Ming. Social networks risk's influence on the national information security [J]. Contemporary spread, 2010. (01) : 75-76.

[7]. 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.

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

[9]. 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.

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

[11]. 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

[12]. 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.

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

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

[15]. GUNDECHA, P., BARBIER, G., JILIANG, T., & HUAN, 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:10.1145/2630421

Cite this article as :

Dr. Magdi Mohammed Mohammed Ahmed Hamoda, "Social Network and Data Security Issues", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 2, pp. 149-154, March-April 2022. Available at doi : https://doi.org/10.32628/CSEIT228219
Journal URL : https://ijsrcseit.com/CSEIT228219