Threats and Anti-threats Strategies for Social Networking Websites

Omar Saeed Al Mushayt

College of Computer Science & Information Systems
Jazan University, Jazan, Kingdom of Saudi Arabia

ABSTRACT

Social networks can offer many services to the users for sharing activities events and their ideas. Many attacks can happened to the social networking websites due to trust that have been given by the users.

Cyber threats are discussed in this paper. We study the types of cyber threats, classify them and give some suggestions to protect social networking websites of variety of attacks. Moreover, we gave some anti-threats strategies with future trends.

KEYWORDS

Social Networking Websites, Security, Privacy, Cyber threats.

1. INTRODUCTION

Online Social Networks (OSN) such as Facebook, Tweeter, MySpace etc. play an important role in our society, which is heavily influenced by the Information Technology (IT). In spite of their user friendly and free of cost services, many people still remain reluctant to use such networking sites because of privacy concerns. Many people claim, these sites have made the world more public and less private – consequently a world with less morale is evolving. Some consider this social change as positive because people are more connected to each other. Nowadays almost all people use the social networking websites to share their ideas photos, videos, with their friends and relatives and even discuss many things about their daily life not only social issues but also others like politics which help lately to change the regime status in many countries such as Egypt Libya and Tunisia. in 1971 started the first communications in the form of social networks this happened in the past when the first email was send from one computer to another connected one. The data exchanged over the phone lines was happened in 1987 where bulletin board system set and web browsers were used for the first time to make to establish the principle of communication. In the following table we summarize the establishment of some famous social networking websites (see table-1)

DOI : 10.5121/ijcnc.2013.5405

year	Social networking websites
1994	Geocities
1995	The globe.com
1997	America online(AOL)
2002	Freindster
2003	Myspace
2004	Facebook
2006	Tweeter
….	…….

Table (1)

There are many types of social networking websites which fulfil the desires of different users. Some of them have their search engine [2]. Some others have tools that allow user to create their own social networks [3]. And so on.

Even, social networking websites have many advantages for users to communicate and exchanges information as we mention above, unfortunately, they have their negative impact! Most people spend all their time using such websites and forget about their duties and sometimes many use loss their life using such websites due to the illegal contents like pornographic, terrorism, religiolism and many other. See figure 2; that shows the number of users of social networking is increasing fast day by day.

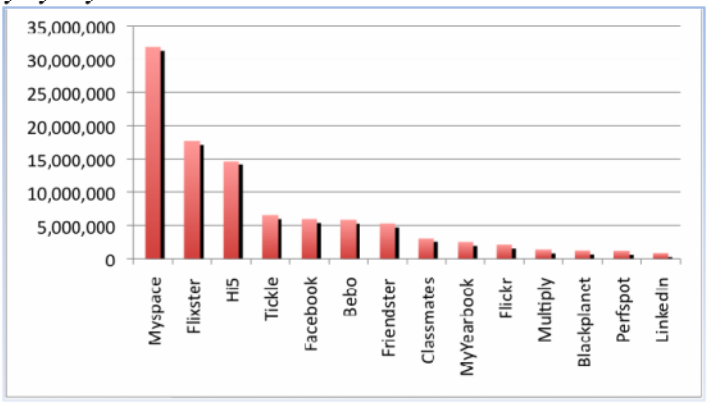

Figure 1. Number of social networks users (Rapleaf's data)

Hacker and cyber criminal have good chances to attack people using social networking websites where users generally don't take care of their sensitive and important information about themselves. Hackers can collect the needed information such as username, passwords and others to penetrate to the back account user and steal money (hackers uses what's named social engineering attack). See figure 2.

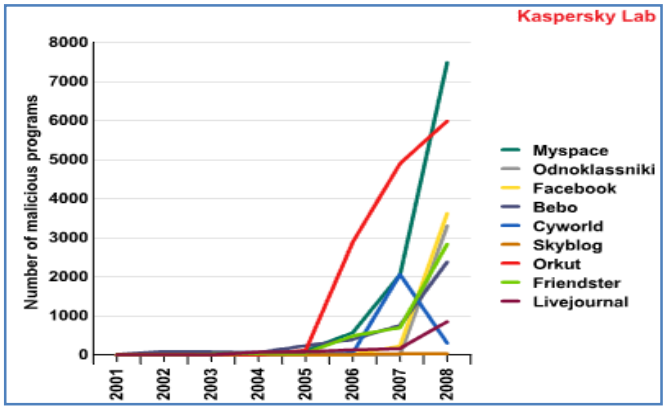

Figure 2. Number of malicious programs with social networking sites

The rest of the paper is organized as follows. Section 2 discusses the security policy background. Types of social networking websites are presented in section 3 analyses of cyber threats in social networking websites discussed in section 4. Anti-threat strategies have been recommended in section 5 . Positive Uses of Social Networks in section 6. We finished our paper with conclusion in section 7

2. SECURITY POLICY BACKGROUND

Social networking websites must satisfy many security issues to work successfully and to be used by people who unfortunately trust most of websites. Social networking websites should have save storage for personal data and tools for managing and securing data and control access to the saved data according some limitations. They must add some features to restrict individual data access from other users. Unfortunately most of social networks have not had applied this issues actually There are many attacks on social networks such as worms, viruses, Trojan horses and fishing websites. Malicious programs vulnerabilities and many others such as sql injection top attacks users should be worried about all types of attacks and have the right firewalls and software which protect them of being hack by cyber criminal

The more complex social networking websites need to be look a form of law prospects where many question should be address such as can we find exact evidence of the cyber crime happened any virtual world and how can a crime be committed?

3. TAXONOMY OF SOCIAL NETWORKS

In this section, we classify the existed social networking websites into groups according to country where they are used see table 2.

Table 2. Social websites according to Continent and Region

Continent/region	**Dominant social websites**
Africa	Hi5, Facebook
America (North)	MySpace, Facebook, Youtube, Flicker, Netlog
America (Central &South)	Orkut, Hi5, Facebook
Asia	Friendster, Orkut, Xianonei, Xing, Hi5, Youtube, Mixi
Europe	Badoo, Bedo, Hi5, Facebook, Xing, Skyrock, Ployaheod, Odnoklassniki.ru.V Kontakte
Middle East	Facebook
Pacific Island	Bedo

Social networking features:

- Global social network where geographical and spatial barriers are cancelled.
- Interaction where sites gives space for the active participation for the viewer and reader.
- Easy to use most social networks can be use easily and they contains images and symbols that make it easier for user interaction

We give here the example of face book which is site that helps to built relationships between users, enabling them to exchange information and personal files, photos and video clips and comments, all this is done in a virtual world cutting the barrier of time and place. Face book is consider as one of the most popular side on the World Wide Web it started by Harvard student Mark Joker Berg where he began designing a website which aims to connect with his colleges at the university and they can share their files and images, opinions and ideas

In table 2, the top five popularity social media sites:

Table 1. Top five popularity social media sites

Site Name	**Primary Shared Media**
YouTube	Videos
Flicker	Images
Digg	Book marks
Metacafe	Videos
Stumbleupon	Cool Contents

Moreover, Youtube is the third most visited Web Site after Yahoo and Google but flicker is the 39th most visited web site [5].

Types of social networks divisions depending on the service provided or targets from its inception to the following types

- Personal networks
- Cultural networks

Social networks also can be divided according to the way we communicate and services into three types

- Networks Allow For Written Communication
- Network Allow Voice Communication
- Network allow for visual Communication

4. CYBER THREATS IN SOCIAL NETWORKING WEBSITES

The most cyber threats to the social networking websites are: a) Malware; different types of virtuosos, warms and Trojan horses. For example *kopfaas* which is a type of warm electronically spread fast across the accounts of users in the social networking websites in which most time as users to update the multimedia player(flash) and when user approved downloading the malware software downloads the warm “cup face” and then this warm can penetrate to all other users connected to the one who approved the installation of the cup face. B) Phishing: this kind of a thread leads the victims to a fake website similar to the original one to steal information then the money of the objective user for example a message came from FBI on the facebook and clamed it is one of the criminal bureau of investigation in USA. D) Trojan Horses: a small code comes with major program with some hidden task of steal data. It is consider as one of popular malware which social networks give him a new spirit. Trojan become a tool for fraud and theft of bank accounts and sensitive data via social networks. E) Leakage of confidential of information as a results of a sense of social networks ,users trust all those who share information with them and unfortunately many times they may share more than they should both impersonal matters or their jobs where they works in organisation or other associations and this results in many problems of social legal ending. F) Condensed electronic links this happens when user makes short cut of the program that they use and many times this short cut leads friends of that user to another illegal websites. G) Impersonation: this is very important and sophisticated problem and may hurt the Vitim socially and politically according to the job of the person. It happens when a user creates accounts behalf of someone by his information to gain advantage of his identity and situation getting worst when other people who are link to that person and share the personal and impersonal information to him.

Lately, social networks attract thousands of users who represent potential victims to attackers from the following types (Ref: Figure 4) [6, 7]. Phishing is a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party. Phishing attacks today typically employ generalized “lures”. For instance, a hacker misrepresenting himself as a large banking corporation or popular on-line auction site will have a reasonable yield, despite knowing little to nothing about the recipient. Phishing attacks can incorporate greater elements of context to become more effective. In other forms of context aware phishing, an attacker would gain the trust of victims by obtaining information about their bidding history or shopping preferences. Phishing attacks can be honed by means of publicly available personal information from social networks [9]. First hackers and spammers who use social networks for sending fraudulent messages to victims "friend", Cybercriminals and fraudsters who use the social networks for capturing users data then carrying out their social-engineering attacks and Terrorist groups and sexual predators who create online communities for spreading their thoughts, propaganda, views and conducting recruitment.

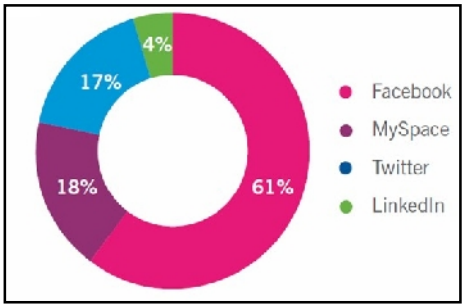

Figure 4. Threats percentage on social networks (Sophos 2010 Security Threat Report)

Now, how can you protect your privacy in social networking websites?
There are many procedures, which help us to protect as much as possible our privacy when using social networks

- Be careful and don't write any sensitive information in your profile page bulletin board, instant messaging or any other type of participation and electronic publishing in internet so that the identity could be protected against the thefts or security threats
- Be skeptical because social networking websites are full of illegal users, hackers and cyber criminals
- Be wise man and thinks twice before you write any think when using social networking websites
- Be polite and do not publish any illegal picture and video and even don't write any abnormal messages and also reflects your personal impacts and be ambassador to all others on the internet
- read the privacy policy of all social networks before using them

Cyber threats that might the users face can be categorized into two categories.

4.1. PRIVACY RELATED THREATS

Privacy concerns demand that user profiles never publish and distribute information over the web. Variety of information on personal home pages may contain very sensitive data such as birth dates, home addresses, and personal mobile numbers and so on. This information can be used by hackers who use social engineering techniques to get benefits of such sensitive information and steal money.

4.1.TRADITIONAL NETWORKS THREATS

Generally, there are two types of security issues: One is the security of people. Another is the security of the computers people use and data they store in their systems. Since social networks have enormous numbers of users and store enormous amount of data, they are natural targets spammers, phishing and malicious attacks. Moreover, online social attacks include identity theft, defamation, stalking, injures to personal dignity and cyber bulling. Hackers create false profiles and mimic personalities or brands, or to slander a known individual within a network of friends.

5. ANTI THREATS STRATEGIES

Recent work in programming language techniques demonstrates that it is possible to build online services that guarantee conformance with strict privacy policies. On the other hand, since service providers need private data to generate revenue, they have a motivation to do the opposite. Therefore, the research question to be addressed is to what extent a user can ensure his/her privacy while benefiting from existing online services. A novel approach, called NOYB (None Of Your Business), was discussed in [7], which provides privacy while preserving functionalities provided by service providers. Users willingly share personal identifying information, but do not have a clear idea of who accesses their private information or what portion of it really needs to be accessed. OSNs can be examined from a viewpoint of characterizing potential privacy leakage [10]. That is, we can identify what bits of information are currently being shared, how widely they are available, and what users can do to prevent such sharing. The third-party sites that track OSN users play a major role in these kinds of attacks causing privacy leakage on popular traditional websites. In the long run, we can identify the narrow set of private information that users really need to share to accomplish specific interactions on OSNs so that privacy can be enhanced further. Privacy can also be preserved by restricting the ability to recover the real data from the fake data to authorized users only.

In this section we present the different types of cyber threats in social networks and found the most of threats happens due to the factors which are listed as below:

a) Most of the users are not concern with the importance of the personal information disclosure and thus they are under the risk of over disclosure and privacy invasions.
b) Users, who are aware of the threats, unfortunately choose inappropriate privacy setting and manage privacy preference properly.
c) The policy and legislation are not equipped enough to deal with all types of social networks threats which are increase day by day with more challenges, modern and sophisticated technologies.
d) Lack of tools and appropriate authentication mechanism to handle and deal with different security and privacy issues.

Because of the above mentioned factors that cause threats, we recommended the following strategies for circumventing threats associated with social website:

a) Building awareness the information disclosure: users most take care and very conscious regarding the revealing of their personal information in profiles in social websites.
b) Encouraging awareness -raising and educational campaigns: governments have to provide and offer educational classes about awareness -raising and security issues.
c) Modifying the existing legislation: existing legislation needs to be modified related to the new technology and new frauds and attacks.
d) Empowering the authentication: access control and authentication must be very strong so that cybercrimes done by hackers, spammers and other cybercriminals could be reduced as much as possible.
e) Using the most powerful antivirus tools: users must use the most powerful antivirus tools with regular updates and must keep the appropriate default setting, so that the antivirus tools could work more effectively.
f) Providing suitable security tools: here, we give recommendation to the security software providers and is that: they have to offers some special tools for users that enable them to remove their accounts and to manage and control the different privacy and security issues.

6. FUTURE TRENDS OF SOCIAL NETWORKING WEBSITES

In spite of the development and advanced technologies in social networking websites adjustment, a few are listed as below:

a) A need for more improvements for social networks so that they can allow users to manage their profiles and connecting tools.
b) A need for convergence and integration of social networks and future virtual worlds.
c) Needs for data integration from different networks, i.e. identification of all contents related to specific topic. This needs particular standards and sophisticated technology supported by social networks providers.
d) Many social networks need standard application programming interfaces, so that users can import and export their profiling information by using standard tools. (For example, Facebook and Google have applied new technologies that allow user data portability among social websites, representing a new source of competition among social networking service).

Moreover, virtual worlds have distinct virtual economies and currency that based on the exchange of virtual goods. Games are one of the newest and most popular online application types on social websites. Here, we have to mention the importance of privacy and security to save users from fraudsters who attempt to steal social networking credentials and online money.
Finally, we have to mention that the advances in the social websites and mobile-phone usage will effect on the growing of using mobile social networking by adding more features and application not only to mobiles, but also to social televisions for future chat, email, forums, and video conferencing [8, 9].

7. RISKS PREVENTION AND THREATS VULNERABILITIES

In this Section, we supply with some important recommendations to help social network users stay save by applying the followings:

a) Always have very strong passwords on your emails and other social web sites
b) Limiting the provided personal information in the social web sites as much as you can
c) Change your passwords regularly, so that your information can be out of reach by hackers.
d) Provide with the minimum amount of information to the website and internet due to the publicity of the internet.
e) Don't trust online others and don't answer on special questions from unknown users or companies i.e. be sceptical.
f) Check privacy policies and be aware of unknown emails and links provides by unknown users.
g) To prevent detecting emails address by spammer techniques, write the email: xyz@hotmail.com as xyz at hotmail dot com.

8. THE POSITIVE USES OF SOCIAL NETWORKS

- Social networks can take advantages in the following pros
- Personal communication is the most common use and perhaps the first spark of social network today was to personal communication between friends
- Learning use the most positive fraud of social network should be in the area of e-learning which allow participation of all parties to communicate with each other in the system of education can be used as a multimedia classes in school and so on

- Governmental use most of governmental departments today are communicating with the public through social networking websites by offering many governmental services online and applying what's named e-government
- Offering e-news for all people.
- Unless we reap the advantages of social networking websites, we should take care of defamation harassment, fraud , extortion and violation of private rights and public as well.

9. CONCLUSION

Although social networking websites offer advanced technology of interaction and communication, they also raise new challenges regarding privacy and security issues. In this paper, we briefly described the social networking web sites, summarized their taxonomy, and highlighted the crucial privacy and security issues giving some essential antithreats strategies with the perspective of the future of the social networking websites.

REFERENCES

[1] http://www.onlineschools.org/blog/history-of-social-networking/
[2] Social networking sites searchengine, /http://findasocialnetwork. com/search.phpS.
[3] B. Stone, Is Facebook growing up too fast, The New York Times, March 29, 2009
[4] "Using Facebook to Social Engineer Your Way Around Security",http://www.eweek.com/c/a/Security/Social-Engineering-Your-Way-Around-Security-With-Facebook-277803/ 05.20.2010
[5] www.securelist.com, «"Instant" threats», Denis Maslennikov, Boris Yampolskiy, 27.05.2008.
[6] Won Kim , Ok-Ran Jeong, Sang-Won Lee , "On Social Websites" , Information Systems 35 (2010), 215-236.
[7] Kaven William, Andrew Boyd, Scott Densten, Ron Chin, Diana Diamond, Chris Morgenthaler, " Social Networking Privacy Behaviors and Risks" ,Seidenberg School of CSIS, Pace University, White Plains, NY 10606, USA.
[8] Abdullah Al Hasib, "Threats of Online Social Networks", IJCSNS, Vol. 9, No 11, November 2009.
[9] Anchises M. G. de Paula, "Security Aspects and Future Trends of Social Networks", IJoFCS (2010) , 1, 60-79.
[10] D. Boyd, N. Ellison, Social network sites: definition, history, and scholarship, Journal of Computer-Mediated Communication 13 (1) (2007) article 11.
[11] Gilberto Tadayoshi Hashimoto, Pedro Frosi Rosa, Edmo Lopes Filho, Jayme Tadeu Machado, A Security Framework to Protect Against Social Networks Services Threats, 2010 Fifth International Conference on Systems and Networks Communications.
[12] "Data Loss Prevention Best Practices", http://www.ironport.com/pdf/ironport_dlp_booklet.pdf 05.20.2010.
[13] "The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained", http://us.trendmicro.com/imperia/md/content/us/trendwatch/researcha and analysis/the_real_face_of_koobface_jul2009.pdf 05.19.2010.