Privacy Threats on Social Networking Websites

Ayesha Shahid
Department of Software Engineering,
Foundation University Rawalpindi Campus,
Pakistan
ayeshashahid.as@gmail.com

Umair Abdullah
Department of Computer Science,
Barani Institute of Information Technology,
Satellite Town, Rawalpindi, Punjab
umair_pitafi@yahoo.com

Abstract: Widespread use of Social networking sites has increased the privacy threat for every individual. Privacy and security problem are two major issues associated with social networks, as the majority of the social network users are not cautious about the usability of the social websites. Social media sites have become latent target regarding offenders because of the occurrence of sensitive information and lack of user awareness of privacy settings. The overall aim of this paper is to enhance awareness about privacy and security issues associated with social networks and to provide guidelines to users for secure usage of social websites. Descriptive research has been conducted as it takes up the majority of online surveying and because of its quantitative nature, it is considered as conclusive. The survey results show that most of the users have their real information on social networking sites and they don't change privacy settings of their accounts on regular basis. Moreover, as per survey findings, most users accept friend requests and invitations of unknown persons on social networking sites. Results of this research study will be helpful to bring awareness among users about privacy setting and they will learn how to control the privacy settings of their accounts and what type of content should be uploaded on social networking sites.

Keywords: Social Networking, Social web sites, security and privacy issues.

1. INTRODUCTION

'Privacy' is defined as the privilege of individuals, groups or organizations to limit themselves, to what extent information about them is allowed to be communicated to others. Privacy is the right to control the personal information about individuals or groups. In this era, there are many social networking sites that have come into consideration. People with different age groups tend to join these sites and stay updated with the ongoing things in the world (Debatin, 2009; Erlandsson, 2012).

Social Networks such as Twitter, MySpace and Facebook have been emerging speedily; with over two billion users right now. Many consumers reveal a wide range of their personal information within their cultural system space. These details include contact information, demographic information, images, textual comments, videos, etc. Several consumers publish the information data freely without cautious consideration (Greschbach, 2012; Henne, 2013). Moreover, cultural system consumers generally have an advanced level of confidence towards other members of the system and tend to accept all things that friends send to them. Due to which social network websites have become the new targets that attract internet offenders and criminals. Attackers use personal data and chain of connections for spamming, phishing and malware attack. Attackers approach victim's profiles and use information which is provided in the profiles to increase the success rate of their attacks (Humphreys, 2010; Mahmood, 2013).

On the basis of practices and experiences, researchers have provided a model of networked privacy; in order to elaborate how privacy can be achieved in public networks (Henne, 2013; Newman, 2014; Parris, 2012). It is well-known that the surge in social network websites including MySpace, Facebook, Bebo and Friendster, is widely considered as a fantastic opportunity, specifically for youth. Careful analysis of the study of the topic tells about different issues created due to the privacy breach.

Social networking websites have gained tremendous popularity in the since the late 1990s and literally, not only millions but billions of people use them around the globe. Social networking has become a powerful tool for people of all ages but especially, among teenager to express and communicate with one another (Cutillo, Molva, & Strufe, 2009). It has become the easiest mode of sharing information with other people like job details, political views, photos, likes & dislikes, religious views, relationship status, etc. (Garfinkel, 2014). With many benefits associated with social networking, there are also some risks and threats linked to it. The dilemma is this that most of the users are not even aware of the risks and threats linked with social networking. Users do not comprehend that the photos and other personal information they share with each other can easily become the target of hackers and other perpetrators (Hazari & Brown, 2013).

Keeping in mind the current risk factors, in 2014, Kaspersky Lab and B2B International jointly conducted the worldwide survey on consumer security risks. The findings of this survey are as follow. More than 78% of the respondents stated that they do not think they are in any danger of cyber-attack and were not worried about their personal information to be targeted as well and only 7% of the respondents were aware of security risks involved in social networking (Kaspersky & Furnell, 2014). On the other hand, it is also propagated that data available on social networking websites can be used by analysts, researchers or anyone who could use the data for the advertisement, fishing, spamming etc. (Qi & Edgar-Nevill, 2011, Srivastava & Geethakumari, 2015). The sensitive user information is stored on social OSN server, and due to their inherent nature of transparency, it gives researchers a chance to analyze and collect data easily (Zolait, Anizi, Ababneh, BuAsalli, & Butaiba, 2014).

The objective of the study: The objective of the study is to enlighten different privacy issues that people face while using social networking sites and deduce a possible solution to the upcoming cyber threats. In this paper we have provided the meaningful introduction to security issues in the field of Social networking and figured out basic reasons behind this threat;

on the basis these reasons, we have provided some recommendations to reduce the security risk for users.

The rest of this paper is organized as follows: Section two shows the online survey results related to social network issues. Then major cyber threats have been discussed and analyzed in terms of privacy issues, Identity theft issue, Malware issue and spam issue in section three. Section four represents few recommendations for appropriate use of social web and enhancing the privacy. And finally, the paper is concluded in Section five.

2. SURVEY RESULTS

Descriptive research has been conducted as it takes up the majority of online surveying and because of its quantitative nature, it is considered as conclusive. We have conducted an online survey on http://www.monkeytool.com/ in order to understand motives, interests, and behaviors of social web users. Survey Monkey is a web-based survey instrument; it was chosen because of its ease of use and cost effectiveness as it offers a free trial. The free trial offer provided up to 10 questions with 100 respondents. A sample of 100 is a good fit for the computer-generated research endeavors. The characteristics of the research tool include ease of use, the simplicity of the internet-based survey and easy download of data for further statistical analysis on Excel or on SPSS. Survey Monkey offers a wide range of formats and styles for questions including Likert scale (up to five ranks), drop down, multiple responses and matrix questions. In the research survey three ranked Likert scale, drop down and multiple responses styled questions were asked of the respondents.

Snowball sampling technique was applied; initially, a sample of ten respondents of university students was taken randomly taken from different Universities of Pakistan, and in order to get respondents around the globe each respondent of the initial sample of ten was encouraged to email the survey link to friends or relatives residing in other countries. Each student developed an email list which comprised of their ten personal contacts residing in different countries. The brief description of the survey and the hyperlink of the survey were sent to the list of respondents. Snowball sampling technique is a non-probability sampling type in which the data is collected through an accumulation of data as every single subject suggests further subjects (Metwally, 2012). Data was analyzed using Statistical Package for Social Sciences (SPSS). Data was coded in SPSS and frequency distribution and percentages were computed.

Survey respondents responded to 10 questions of the questionnaire which focused mainly on the privacy threats on social networking websites. Figure 1 depicts the results of the first question which was about the reliability of social networking sites to get information. The majority of the respondents (75%) don't consider social networking websites as the reliable source to get the information.

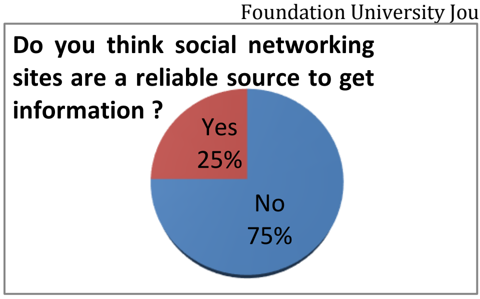

Figure 1: Social Web as source of reliable information

Figure 2 shows the results of the second question, in which the type of contents often seen on different social networking websites was asked from the respondents. Mostly people use the social networking websites to see entertainment content.

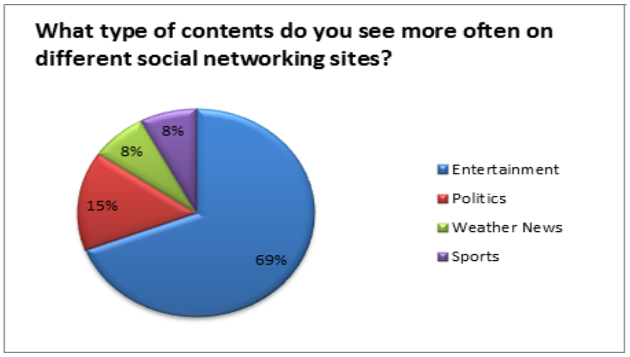

Figure 2: Type of contents accessed on social web

Question 4 of the online survey was about information seeking from friends prior to uploading their pictures or personal information on the social networking websites. As shown in Figure 3 most of the people don't seek permission from their friends before uploading their pictures and information on social networking websites. Figure 4 represents that majority of respondents share their pictures on social networking websites.

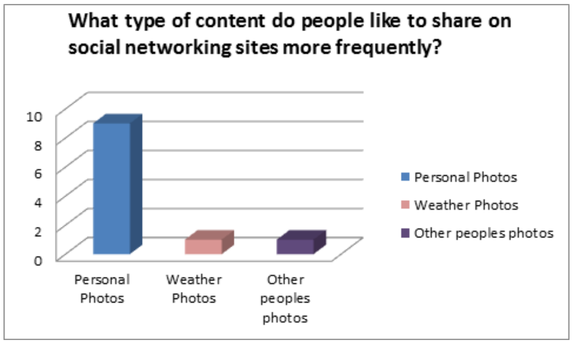

Figure 3: Type of data shared on social web

As per the results mentioned in Table No. 1 most people have their real information on social networking sites and they do not change the privacy settings of their accounts on regular basis. Mostly people don't have awareness if their account on social networking website is linked to other search engines.

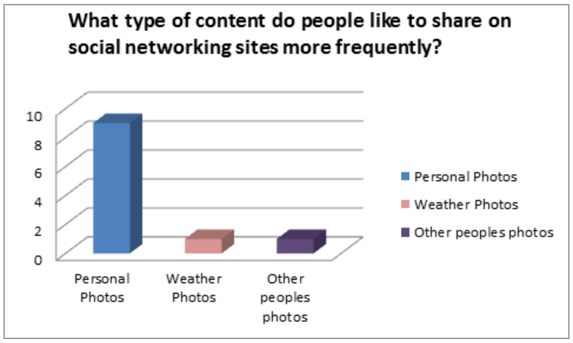

Figure 4: Type of data shared on social web

As per the survey findings mostly people receive friend requests from unknown persons and they accept those invitations or friend requests.

Table No. 1 Awareness of Privacy settings and risk of Personal Information misuse

Question	Yes %	No %	I don't Know %
Do you change privacy settings of your account on regular basis?	32.0	60.0	8.0
Are other search engines linked to your account on social networking website?	34.0	21.0	45.0
Have you ever received the friend request or invitation from an unknown person?	63.0	17.0	20.0

Have you ever accepted the friend request or invitation of an unknown person?	48.0	42.0	10.0
Does your account/s on social networking websites have your real personal information?	57.0	39.0	4.0

As per survey results tabulated in Table No. 2 mostly posts of the respondents are public.

Table No. 2 Who is mostly the audience of your posts on social networking sites?

	Frequency	Percent
Friend	33	33.0
Public	40	40.0
Customized group	23	23.0
Only me	4	4.0
Total	100	100.0

3. PRIVACY THREATS ON SOCIAL NETWORKING WEBSITES

In most cases, users got victimized due to their trust in friends as attackers are disguised as friends by breaching friends' profiles.

3.1 Privacy Issues

Users' anonymity, users' identity, and users' personal information leakage are main privacy issues discussed in this section.

3.1.1 Anonymity of Users

Many users use their original information to create their accounts on social network websites and use original name as the title of their accounts. Therefore, their personality is subjected publicly too many social networks, in addition to everyone on World Wide Web. To acquire new victims, an offender can search through social network websites.

3.1.2 Users Profile and personal Information

Offenders are appealed Personal information like username, contact information, connection status, educational history, current and previous connections etc., The key problem associated with users' profiles is leakage of personal information (Erlandsson, 2012). Main causes of profiles' information leakage are; poor privacy settings and use of third party applications. Many users aren't cautious about their solitude settings. Most of the users start their account as public so that everyone can access and see their information. Similarly, several cultural network sites like Facebook allow Application Programming Interfaces (APIs) for third-party programmers to develop applications that may operate on their platforms. When users let third party application gain access to their data, these applications may access user's data without user's consent and use it in an offensive way.

3.1.4 Identify Theft Issues

Profile Cloning and Social Phishing are two main methods of identity theft on social sites. These methods have been discussed as follow;

3.2 Profile Cloning

Stealing identity of a user working in the social network environment is often known as profile cloning. Users with the public profile are potential victims of this technique. Public profile lets muggers obtain complete data from profile very easily, and then attackers can copy or duplicate their profile data to create a fake similar profile with factually correct information. Further division of profile cloning is in two categories; existing profile cloning and cross-site profile cloning. For existing profile cloning, criminals make a fake account of user - already existing on the social website - by utilizing its personal actual information and picture (in order to boost reliance). Most of the social network users accept requests from anyone they know without confirmation. For the cross-site profile, cloning offender steals page of a user from one social network site and then produce a new similar page on another social network site on which the victim does not have the account. Then offender makes use of people contact list from the listed social networking site to deliver friends requests to any or all these contacts in another social network site. This process is effective as there is account for that specific user.

3.2.1 Social Phishing

Throughout phishing assault, assailants present you with an artificial site which usually looks legitimate to help tempt subjects into giving their own private and very sensitive facts including financial facts, code, and acknowledgment files towards the website. With the use of personal information from social sites, phishing attacks have becomes more and more successful. Offenders may send a phishing site to subjects using the names of victim's friends.

3.3 **Malware Issues**

This specific area explains the way spyware advances all over internet sites. Degrees of well-known social program spyware, Koobface, MySpace in addition to Twitter Earthworms are being reviewed.

3.3.1 Malware spreading Across Social Network

Considering that the principal notion involving social networking sites will depend on the partnership between customers within the multilevel, so spyware can just spread via most of these interconnections. Almost every other social network websites fail to determine whether the embedded links are malicious or not. Thus, an intruder may use this flaw. Unsafe URLs might route users to malicious websites, and then provide malicious data to victim's computer in order to take files, as well as to make use of victim's computer in order to assault people.

Social Network API

Third party applications can easily be the reason for MySpace or Facebook owner's data loss as previously mentioned above. In such cases, these types of applications can be probable causes of spyware disease due to the fact all people can easily have accessibility to your purposes. These applications may look authentic, but inside these may contain a destructive link that leads people to the destructive domain and spreads spyware.

3.3.2 Malware Example

In this section two most famous social network malware i.e. Twitter worms and Koobface, have been discussed.

3.3.2.1 Twitter worms

Twitter Worm is the worms which are distributed through Twitter. Twitter worms (e.g. Profile Spy worm and Goo.gl worm) have several designs. This section describes two samples of Twitter worms;

a. Profile Spy Worm: This worm propagates by tweeting a web link to download something to a third party application named "Profile Spy" (a phony application which allows account proprietors to discover who has considered their profiles). In order to have the form, individuals are required to enter data, allowing an opponent to obtain user's data. When victim's consideration is usually modified, it may retain tweeting detrimental communications for their own purpose.

b. Goo.gl worm: These worms are the shortened Google URLs to cheat people so they can click on them. People are redirected to a fake anti-virus website by this sham link. The web page can certainly pop-up a new warning that will pollute the user's personal computer and get to have his or her fake anti-virus request that is actually the damaging code.

3.3.2.2 Koobface

Koobface is a worm which grows throughout social internet sites such as MySpace and Facebook. This worm is distributed through communications directed between friends on social networking websites. They normally contain movie URLs to attract users to select it. Any time end users comply with the hyperlink, in addition, to trying to enjoy the actual movie; many people will get a newer version update. When the end users set up the actual plug-in, his or her computers get corrupted. Now, the actual enemies may get his or her data, or perhaps utilize his or her computer to attack others computers.

3.4 Spam Issues

An average junk mail strike via email most likely is not effective in an attack that the majority of the users are generally attentive about their emails. A successful brand new way of spam attack is being introduced on Social a network which is more successful. This section illustrates spam attacks on social networking website, and email spam attacks that make use data from social websites.

3.4.1 Social networks under Spam Attack

On social websites, spam is available in the form of the post on a wall, news feed, and information spam. These spasms may include advisements or hyperlinks that victims may click through that link. These links can result in dangerous malware websites or phishing websites. This sort of spam is generated from spam applications and artificial fake profiles. For artificial page, it is often found with the name of some celebrity's page. It attracts many people to become friends, and then disseminate to victims' friend's list. For spam request, once users grant the use of the application, the application may spam users via wall post and might self-distribute to a friend's wall.

3.4.2 Email based spam Attack

Email is actually one of the favorite interaction media, and thus it becomes a target of online attacks. Spam has been a problem for email users for an extended time. Numerous mail messages which are currently being dispatched each day are comprised mainly involving spam mail. Social networks usually are wonderful options to have good electronic mail deals with, in addition to e-mail user's information that is personal. Although social networks allow customers to help keep their information private but attackers could still work with user's data by using first and last name from his or her email address.

4. RECOMMENDATIONS TO AVOID PRIVACY ISSUES

Some recommendations are mentioned below in order to avoid privacy and security issues of social networking:

1. For starters, please make sure that any computer system you use to connect to a social media website has adequate security measures.

2. You should clearly set out the goals for publishing any information and publish only that material you are absolutely comfortable with. For instance, on a dating website, you might need to enter your age, but you do not need to enter a correct birthdate. From a security point of view, this may sound very reasonable but most of the users ignore these simple steps to protect their privacy.

3. It is of utmost importance to have such privacy settings which will give access to only trustworthy people to see and comment on your post. Also, confine the access for others to post anything to your page. The standard privacy settings for most of the social networking websites may permit anyone to publish information to your page or see your information; users should remember to change these settings.

4. Most of the users do not bother to review a website's privacy policy. Some social networking websites may share information such as user preferences or email addresses with third parties. It is strongly recommended that do not use that social networking website if a site's privacy policy is ambiguous or does not appropriately protect your information.

5. Get rid of your information from Google search crawlers. Never share your age, place of birth or birthday. This information can be helpful for data mining organizations and identity thieves. Carnegie Mellon University conducted a research and concluded that based on publically available information i.e. age, place of birth or birthday, Social Security numbers can be anticipated.

6. The user must be one step ahead of the changes in social networking website’s terms of service and privacy policy. A user can keep track of the changes by staying connected to an official site profile, for instance, Governance which is Facebook’s site.

7. Make sure to delete cookies, including flash cookies, every time you are logged out from a social networking website.

8. Another precaution would be to ‘turn off’ the option which enables social networking websites to share information. For instance, Facebook's option of ‘Platform’, by turning it off, this will put a stop on tracking of browser history. Users should also be extremely cautious when publishing any kind of geo tagging or location features because in the wrong hands this information can be very harmful. Moreover, never share your daily activities to anyone like where you take breakfast or lunch, how do you reach your workplace e.g. bus, walk or subway or when are you leaving your workplace, all of this information can be very helpful for people with criminal intent.

5. CONCLUSION

Although social networking websites offer electrifying modern chances for interaction and communication yet these also elevate privacy concerns. In this paper, multiple major features and benefits of social networking have been discussed which made this technology among the most popular internet technologies of the era. Social media sites have become latent target regarding offenders because of the occurrence of sensitive information. We have also highlighted privacy problem as one of many major issues because many users are not cautious of what they present on their social networking sites. Multiple dilemmas related to crucial privacy and security threats including personality theft, spam click rate, and spyware issue are also highlighted in the study. Finally, we have listed few recommendations to enhance the security so that users can get advantage from the websites rather than the suffering of its downsides. The online community websites generally encounter new kinds of adware and spyware. Although, social networking websites try to smear different perceptional methods to prevent such dilemmas and to guard their customers yet attackers may generally discover new techniques to separate through these defenses. It is requisite that social networking users must be familiar with each one of these threats and become more cautious when using them; else instead of bringing blessing to the user, the online social networks will become a perilous influential tool for spammers and others to harm the users.

REFERENCES

Cutillo, L., Molva, R., & Strufe, T. (2009). Safebook: A privacy-preserving online social network leveraging on real-life trust. IEEE Communications Magazine, 47(12), 94-101. http://dx.doi.org/10.1109/mcom.2009.5350374

Debatin, B. e. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication15.1 , 83-108.

Erlandsson, F. M. (2012). Privacy threats related to user profiling in online social networks. Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom). . IEEE.

Garfinkel, S. (2014). Leaking Sensitive Information in Complex Document Files--and How to Prevent It. IEEE Security & Privacy, 12(1), 20-27. http://dx.doi.org/10.1109/msp.2013.131

Greschbach, B. G. (2012). The devil is in the metadata—New privacy challenges in Decentralised Online Social Networks. IEEE International Conference . Pervasive Computing and Communications Workshops (PERCOM Workshops).

Hazari, S. & Brown, C. (2013). An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites. Journal Of Information Privacy And Security, 9(4), 31-51. http://dx.doi.org/10.1080/15536548.2013.10845689

Henne, B. C. (2013). Snapme if you can: privacy threats of other peoples' geo-tagged media and what we can do about it. Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks. . ACM .

Humphreys, L. P. (2010). How much is too much? Privacy issues on Twitter. IEEE. Conference of International Communication Association, Singapore.

Kaspersky, E. & Furnell, S. (2014). A security education Q&A. Information Management & Computer Security, 22(2), 130-133. http://dx.doi.org/10.1108/imcs-01-2014-0006

Mahmood, S. (2013). Security and Privacy Preserving in Social Networks. . Springer Vienna.

Metwally, E. (2012). Survey Research Methods20121Earl R. Babbie. Survey Research Methods. Belmont, CA: Wadsworth, Inc 1990. Journal Of Organizational Change Management, 25(1), 186-188. http://dx.doi.org/10.1108/09534811211199655

Newman, J. J. (2014). Press Start to Track?: Privacy and the New Questions Posed by Modern Videogame Technology. American Intellectual Property Law Association (AIPLA) Quarterly Journal .

Parris, I. F. (2012). Facebook or Fakebook? The effects of simulated mobile applications on simulated mobile networks. Ad Hoc Networks 12.

Qi, M. & Edgar-Nevill, D. (2011). Social networking searching and privacy issues. Information Security Technical Report. http://dx.doi.org/10.1016/j.istr.2011.09.005

Richards, N. M. (2014). Privacy and Intellectual Freedom. Unwin.

Srivastava, A. & Geethakumari, G. (2015). Privacy landscape in online social networks. International Journal Of Trust Management In Computing And Communications, 3(1), 19. http://dx.doi.org/10.1504/ijtmcc.2015.072461

Weir, G. R. (2011). The threats of social networking: Old wine in new bottles? Information security technical report 16.2 .

Zolait, A., Anizi, R., Ababneh, S., BuAsalli, F., & Butaiba, N. (2014). User awareness of social media security: the public sector framework. International Journal Of Business Information Systems, 17(3), 261. http://dx.doi.org/10.1504/ijbis.2014.064973