INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN SCIENCE TECHNOLOGY & ENGINEERING
VOL. 1 ISSUE 2, NOV.-2012 ISSN NO: 2319-7463

Prevention of Privacy Threats in Social Networking Sites

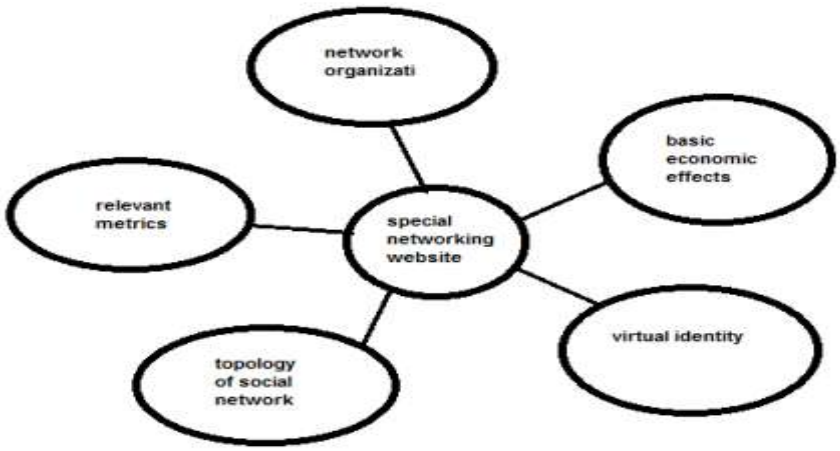
Gurpreet Singh, Gagandeep Singh, Neha Kohli
M.Tech (C.S.E), Sai Institute of Engineering & Technology, SIET, Punjab.
Assistant Professor, Sai Institute of Engineering & Technology, SIET, Punjab.

Abstract

This paper deals with Social Networking Sites and the threats pertaining to the privacy of the users in it. Though these networks offer attractive means for interaction and communication, it also raise privacy and security concerns. So it becomes important for the users to be cautious about their identity. With time as the security features are improving, equally the numbers of threats are also increasing. Hence in the end it entirely becomes the responsibility of the user to secure the information. Through research we find that an individual's privacy concerns are only a weak predictor of his membership to the network. Also privacy concerned individuals join the network and reveal great amounts of personal information. Some manage their privacy concerns by trusting their ability to control the information they provide and the external access to it. However, we find significant misconceptions among some members about the online community's reach and the visibility of their profile. The conclusion of the paper suggests measures of safety and also an idea that can be used in near future as an means to restrict the threats.

I. INTRODUCTION

Social Networking sites such as Facebook, Linkedin, My Space etc have become widely popular among the masses. People find them as attractive and easy medium for communication, maintaining the long lost contacts of colleagues as well as source of entertainment. There are now hundreds of SNS's which have all been developed to cater for a wide range of different types of users each with its own unique community and culture surrounding it.



Although the target audience, service model and purpose of each SNS varies, the main technical features remain consistent between sites, and most SNS's share the following 3 core features:

1. Allows a user to construct a public or semi-public profile within a bound system.

2. Displays a list of other users who are networked with the person and is connected with through the system.

3. Allow an individual to view and traverse between different people within the bounds of his/her network.

The relatively open and detailed nature of the information presented in the user profiles, and the lack of privacy and security control provided by SNS's and the awareness of these issue by users has led to concerns being raised by large groups of people. In particular, there has been a substantial amount of academic research focused on identity presentation and privacy concerns surrounding the use of SNS'.
Their main argument is that users may be putting themselves in harm's way both offline (e.g. Stalking) and online (e.g. Identity Theft) if they provide too much personal information through their SNS profiles. However, despite the negative coverage surrounding the issues over Privacy and Security from the use of SNS being well documented and covered extensively by academics, various organizations and the mass media in recent years, SNS's such as Facebook continue to see exponential growth in their user base (Facebook).

II. PRIVACY THREATS

User's private information can easily be used by the hackers through the different applications introduced in the Social Networking sites for the entertainment purpose. One may unintentionally reveal information to unauthorized individuals by performing certain actions. Hence the only way to overcome coming into such situation is to be aware of various threats and act smartly.

The following are some common threats to social networking services:

A. Viruses

The popularity of social networking services gives room to the attackers to target users with the least effort. By creating a virus and embedding it in a website or a third-party application, an attacker can potentially infect millions of computers.

B. Tools

Attackers may use tools that allow them to take control of a user's account. The attacker could then access the user's private data and the data for any contacts that share their information with that user. An attacker with access to an account could also pose as that user and post malicious content.

C. Social engineering attacks

Attackers may send an email or post a comment that appears to originate from a trusted social networking service or user. The message may contain a malicious URL or a request for personal information. If you follow the instructions, you may disclose sensitive information or compromise the security of your system.

D. Identity theft

Attackers may be able to gather enough personal information from social networking services to assume your identity or the identity of one of your contacts. Even a few personal details may provide attackers with enough information to guess answers to security or password reminder questions for email, credit card, or bank accounts.

E. Third-party applications

Some social networking services may allow you to add third-party applications, including games and quizzes that provide additional functionality. Be careful using these applications—even if an application does not contain malicious code, it might access information in your profile without your knowledge. This information could then be used in a variety of ways, such as tailoring advertisements, performing market research, sending spam email, or accessing your contacts.

F. Professional and Personal Implications

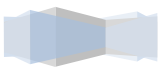
You may risk professional opportunities, personal relationships, and safety by posting certain types of information on social networking services.

G. Business data

Posting sensitive information intended only for internal company use on a social networking service can have serious consequences. Disclosing information about customers, intellectual property, human resource issues, mergers and acquisitions, or other company activities could result in liability or bad publicity, or could reveal information that is useful to competitors.

H. Professional reputation

Inappropriate photos or content on a social networking service may threaten a user's educational and career prospects. Colleges and universities may conduct online searches about potential students during the application process. Many companies also perform online searches of job candidates during the interview process. Information that suggests that a person might be unreliable, untrustworthy, or unprofessional could threaten the candidate's application. There have also been many instances of



people losing their jobs for content posted to these services. Although the legality of some of these terminations is still being debated, posting certain comments may affect your credibility and professional reputation.

I. Personal relationships

Because users can upload comments from any computer or smart phone that has internet access, they may impulsively post a comment that they later regret. According to a survey conducted by Retrevo, 32 percent of people who post on a social networking site regret they shared information so openly. Even if comments and photos are retracted, it may be too late to undo the damage. Once information is online, there is no way to control who sees it, where it is redistributed, or what websites save it into their cache.

J. Personal safety

You may compromise your personal security and safety by posting certain types of information on social networking services. For example, revealing that you will be away from home, especially if your address is posted in your profile, increases the risk that your home will be burglarized. An important element to remember about social networking services is that users may post information about other people. Without even realizing it, you may put someone else at risk by posting a comment or photo that could compromise that person's privacy or security. Sometimes, posting negative content about someone else is intentional. Social networking services have become channels for conducting cyber-bullying, a growing problem that can lead to significant psychological trauma.

III. Proceed with Caution/Safety

Social networking services are useful and enjoyable, but it is important to take proactive steps to protect your computer, your personal information, and your company data. By protecting yourself, you also help to protect the people you are connected to on these services.

A. Limit the amount of personal information you post

Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when posting information, including photos, about your connections.

B. Remember that the internet is a public resource

Only post information you are comfortable with anyone seeing. This includes information and photos in your profile and in blogs and other forums. Also, once you post information online, you can't retract it. Even if you remove the information from a site, saved or cached versions may still exist on other people's machines.\

C. Be wary of strangers

The internet makes it easy for people to misrepresent their identities and motives Consider limiting the people who are allowed to contact you on these sites. If you interact with people you do not know, be cautious about the amount of information you reveal or agreeing to meet them in person.

D. Be sceptical

Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities. This is not necessarily done with malicious intent; it could be unintentional, an exaggeration, or a joke. Take appropriate precautions, though, and try to verify the authenticity of any information before taking any action.

E. Evaluate your settings

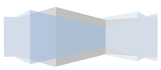
Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile, but you can customize your settings to restrict access to only certain people. There is still a risk that private information could be exposed despite these restrictions, so don't post anything that you wouldn't want the public to see. Sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate.

F. Be wary of third-party applications

Third-party applications may provide entertainment or functionality, but use caution when deciding which applications to enable. Avoid applications that seem suspicious, and modify your settings to limit the amount of information the applications can access.

G. Use strong passwords

Protect your account with passwords that cannot easily be guessed. If your password is compromised, someone else may be able to access your account and pretend to be you.



H. Check privacy policies

Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam. Some sites will continue to send email messages to anyone you refer until they join.

I. Keep software, particularly your web browser, up to date

Install software updates so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.

J. Use and maintain anti-virus software

Anti-virus software helps protect your computer against known viruses, so you may be able to detect and remove the virus before it can do any damage. Because attackers are continually writing new viruses, it is important to keep your definitions up to date.

IV. Discussion and Future Work

Online social networks offer exciting new opportunities for interaction and communication, but also raise new privacy concerns. Among them, the Facebook stands out for its vast membership, its unique and personally identifiable data, and the window it offers on the information-relevant behaviour of millions of young adults. Age and student status obviously are the most significant factors in determining FB membership. However, we observe that privacy attitudes also play a role, but only for the non undergraduate population. In fact, most of highly privacy concerned undergraduates still join the network. While a relative majority of FB members are aware of the visibility of their profiles, a significant minority is not. The 'aware' group seems to rely on their own ability to control the information they disseminate as the preferred means of managing and addressing their own privacy concerns. In addition, misunderstanding or ignorance of the Facebook (the Company)'s treatment of personal data are also very common. Keeping in mind the vast population already into the Social networking sites and the future population that will enter into it proper initiative should be taken by the authorities of the social networking sites to filter the unwanted users as well as the unwanted applications.

V. Measurement of precaution

A**.** SSN in US and ADHAR

Taking in account the identification number (SSN in US and ADHAR in India) of individuals of various countries a rule should be made to enter the identification number and a email id (which is visited by the user frequently) along with other necessary details while making a account in the SNSs' allowing a person to make a single account in a website. Also, this information should only be for the purpose of verification and not for display in the user profile pages of website. The details in the SSN could be matched with the information provided by the user and in case of any discrepancy no account should be allotted.

B**.** Biometrics

Password leakage is becoming a very important problem for the users of social networking sites. If a person gets to know the password of any other person, he tries to login through his account and gather certain confidential or private data thus violating the terms and conditions of the sites which sometimes results as a major problem for the victim users.
This problem can be resolved by using the biometric technology which if implemented with these sites for user login rather than using passwords can provide user with more secure and trustworthy communication platform. Biometric provides certain schemes for the identification of the authenticated and correct users. Using these schemes, only the correct user's entry is allowed through his account. Thus, no one can take the advantage of others account and cannot reveal his personal and private information. The study of measurable biological characteristics. In terms of computer security, biometrics refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked.
In other words, "Biometrics is an automated method of recognizing a person based on physiological or behavioural characteristics."

Several biometric identification schemes are:
Face: The analysis of facial characteristics.
Fingerprint: Unique fingerprints of every individual.
Hand geometry: The analysis of the shape of the hand & the length of the fingers.
Retina: Analysis of capillary vessels located at the back of the eye.
Iris: Analysis of the colored ring that surrounds the eye.
Signature: The analysis of the way a person signs his name.
Voice: Analysis of tone, pitch, and frequency of person.

C. Why biometrics

Certain factors are responsible which add weight to the benefits of biometric technology when used for user authentication in various networking sites. Some of them are:

- Identification through biometric techniques can provide extremely accurate, secured access to information, fingerprints; retinal & iris scan can produce absolutely unique dataset when done properly.
- Automated biometric identification can be done very rapidly & uniformly, with a minimum of training.
- Your identity can be verified without resort to documents that may be stolen, lost or altered.
- Minimize the opportunity for ID fraud, buddy punching.
- Replace hard to remember passwords which may be shared or observed.

Though these techniques have many advantages, it has certain **limitations** too. Some of those limitations are listed as under:

- It provides expensive security solution.
- For people affected with diabetes, the eyes get affected resulting in differences.
- The voice of a person differs with age. Also, when the person has flu or throat infection, the voice changes or if there is too much noise in the environment, this method may not authenticate correctly. Thus, this method of verification is not workable all the time.
- The fingerprints of those people working in chemical industries are often affected. Therefore these companies cannot use the fingerprint mode of authentication.

VI. Methodology

Facebook being the hub for millions of users for networking was used for critically analysing the security concerns related to user authentication. Through an offline survey, certain questions were created to capture the perceptions of trust, internet privacy concern, information sharing, general use of the site, & the development of new relationships. Study through the research survey indicated that users will express very strong concerns about privacy of their personal information, but be less vigilant about safeguarding it.
We found that users find the biometric techniques easy to learn and they want to get it implemented in these sites. They seem to be satisfied with the working capabilities of the technology as it not only facilitates the proper use of social networking sites but also provides them with the more secure and reliable communicating platform as compared to earlier.
Based on this survey we prepared a chart as under:

REFERENCES

[1].petworkshop.org/2006/preproc/preproc_03.pdf#search=%22Awareness%2C%20Information%20Sharing%2C%20and%20Privacy%20on%20the%20Facebook%22 [5-6].

[2]. www.w3.org/2008/09/msnws/papers/The_Future_Of_Social_Networking.html [6].

[3.]itde.nova.edu/students_scholarship/EDD6000/Cecconi/Documents/Pdf_8012/A3_Cecconi.pdf [1-2].

[4].www.scribd.com/doc/44725515/Privacy-Security-Concerns-over-Social-Networking-Sites-Does-it-really-matter [2].

[5]privacyinsocialnetworksites.wordpress.com/ [6]http://www.antiphishing.org/consumer_recs.html [3-4].

[7]www.fabernovel.com/socialnetworks.pdf [1].

[8]www.deitel.com/ResourceCenters/Web20/SocialNetworking/SocialNetworkingResearch/tabid/1307/Default.aspx[5].

AUTHOR'S BIOGRAPHY

Er. Gagandeep Singh is working as a Assist. Professor Department of Computer Science & Engineering, Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India. He obtained his B.Tech (Computer Science Engineering) from Sri Sai Institute of Engineering & Technology, Punjab, India, M. Tech (Computer Science & Engineering from ACET, Manawala, Punjab, Presently, India he has 4 years of research and UG & PG teaching experience. He has 7 research papers to his credit in various international journals and conferences. He is member of International Association of Engineers HONG KONG and International Association of Computer Science & Information Technology, SINGAPORE. His areas of research and interest include Web Security, Software Engineering.

Mr. Gurpreet Singh is pursuing M. Tech in Computer Science & Engineering from Sai Institute of Engineering & Technology. He did his B.Tech degree in Computer Science & Engineering from Sri Sai Institute of Engineering College, Ptk, Punjab, India. His area of interest is Distributed Database, software Engineering

Neha Kohli is pursuing M. Tech in Computer Science & Engineering from Sai Institute of Engineering Technology. She did her B.Tech degree in Computer Science & Engineering from Amritsar College of Engineering & Technology, Manawala, Amritsar, Punjab, India. Her area of interest is Network Security, software Engineering.