A Survey on Security Issues and Concerns to Social Networks

Kiran Malagi[1], Akshata Angadi[2], Karuna Gull[3]

[1, 2, 3] Department of Computer Science & Engineering, K.L.E.I.T, Hubli, India

Abstract: ***Social networking sites are websites designed for human interaction. Online social networks are now used by hundreds of millions of people and have become a major platform for communication and interaction between users. Under the gentle encouragement of social networking services like Facebook, Twitter, LinkedIn, Google, Yahoo, the right to privacy is being devalued with no questions asked as to how it affects our security and freedom. Even though the use of social network web sites and applications are increasing day by day but users are not aware of the risks associated with uploading sensitive information. In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information. Due to the sensitivity of information stored within social networking sites a plethora of research in the area of information security has been raised. This paper will help to look at some of these risks and identify possible solutions to protect your personal information and your company data.***

Keyword:

1. Introduction

According to Cluley "Social networks are great fun, and can be advantageous but people really need to understand that its complicated world and you need to step wisely".

Social networks are web-based applications people use to connect to others with whom they share common interests, either professionally or personally. Users post content to the application to update connections and share personal news, accomplishments, interests and more. This content can be in the form of simple text status updates, videos or photos. People use social networks to find a new job, find new clients or stay in touch with long distance friends and family. Examples of social networks are LinkedIn, Facebook, Twitter and YouTube. Social networks often offer additional applications that extend their functionality through games, quizzes which have built by third party developers and have the potential to introduce the security risks.

1.2 Types of Social Networks

There are many types of social networks available. Our paper examines the privacy and security issues & gives advices to the users using a few of them. While this paper does not address every type of social network, many of the security and privacy recommendations are applicable to other types of networks.1

- **Personal networks:** These networks allow users to create detailed online profiles and connect with other users, with an emphasis on social relationships such as friendship. For example, Facebook, Friendster and MySpace are platforms for communicating with contacts. These networks often involve users sharing information with other approved users, such as one's gender, age, interests, educational background and employment, as well as files and links to music, photos and videos. These platforms may also share selected information with individuals and applications that are not authorized contacts.

- **Status update networks:** These types of social networks are designed to allow users to post short status updates in order to communicate with other users quickly. For example, Twitter focuses its services on providing instantaneous, short updates. These networks are designed to broadcast information quickly and publicly, though there may be privacy settings to restrict access to status updates.

- **Location networks:** With the advent of GPS-enabled cellular phones, location networks are growing in popularity. These networks are designed to broadcast one's real-time location, either as public information or as an update viewable to authorized contacts. Many of these networks are built to interact with other social networks, so that an update made to a location network could (with proper authorization) post to one's other social networks. Some examples of location networks include Brightkite, Foursquare, Loopt and Google Latitude. For an in-depth discussion of locational privacy, read the ACLU of Northern California's Location-Based Services: Time for a Privacy Check-in and their Comparison Chart evaluating the privacy features of six location networks.

- **Content-sharing networks:** These networks are designed as platforms for sharing content, such as music, photographs and videos. When these websites introduce the ability to create personal profiles, establish contacts and interact with other users through comments, they become social networks as well as content hubs. Some popular content sharing networks include thesixtyone, YouTube and Flickr.

- **Shared-interest networks.** Some social networks are built around a common interest or geared to a specific group of people. These networks incorporate features from other types of social networks but are slanted toward a subset of individuals, such as those with similar hobbies, educational backgrounds, political affiliations, ethnic backgrounds, religious views, sexual orientations or other defining interests. Examples of such networks include deviantART, LinkedIn, Black Planet, Goodreads and Gay.com.

Although social networks are primarily intended for consumer use, companies are increasingly recognizing their business benefits. This creates a unique challenge for the IT department. In addition to the benefits social networks pose, they can negatively impact productivity, network bandwidth, users' privacy, data security and the integrity of IT systems (via malware and application vulnerabilities).

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 actually 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.

The potential for mischief and malicious activities arises when one or more of those contacts break your trust. When that happens, a number of things can go wrong such as:

- Your contact's account was compromised and somebody else is using it.
- You added somebody to your network that you thought you knew but, in fact, you did not.
- You added somebody you thought was trustworthy but he/she turns out not to be.
- Insufficient use of privacy controls caused you to share data with people you never intended.

Thus we can conclude that the popularity of social networking sites -- such as MySpace, Facebook, Twitter and others -- has expanded tremendously in recent years. The sites are becoming more ubiquitous for both personal and professional activities. But these sites also continue to serve as prime targets for malware distribution and scams.

1.3 Characteristics which all Social Networks satisfy

• **Storage of personal data**: Social Networks certainly satisfy this requirement – like no other IT system on earth. The biggest repository of personal images on the internet is not Flickr but Facebook (already with a staggering 30 billion images, while 14 million new images are uploaded every day). The largest number of personal profiles on the planet is held not in a government Identity registry (at least not one we know about...) or one of the much heralded Federated Identity Providers but in the data warehouses of the Social Networking providers.

• **Tools for managing personal data and how it is viewed**: Social Network systems do not just store personal data, they manage it – allowing query, transfer and display of the data in the system. This is one of the main functions of Social Networks. They provide user friendly tools which allow users to define in considerable detail how their personal profiles are displayed, both in terms of visual layout and the data fields which are displayed. They also provide sophisticated tools for searching (by users) and mining (by advertisers) profile data.

• **Access control to personal data based on credentials**: This criterion is probably the most important. Any system must give its users control over who accesses which parts of their personal data. Usually this is based on knowing whether the person accessing the data fulfils certain criteria (and has credentials to prove this). Social Networks are increasingly offering this functionality. In social networks, the main boundary protecting a user's data is whether a person attempting to access it has been defined as a friend or is a member of a shared group. Recently, however, Social Networks have added features which allow users to restrict access down to the level of individual friends (or business associates) for each field of their personal profile. In other words, they are now offering very granular access control.

• **Tools for finding out who has accessed personal data**: Most of the systems provide data tracking tools so users can see who has accessed personal data. This functionality is often not fully implemented in Social Networks because users browsing other people's profiles generally prefer to remain anonymous. It is possible to install profile trackers on some Social Networks however, and many Social Networks provide quite detailed anonymous statistics on accesses to user profiles.

Even though most of the networking sites provide or satisfy all these requirements, there are own set of security concerns which can put your information systems and/or personal data at risk.

2. Motivation & Goal

Social Media's rise in popularity has created some very real problems for the Internet and its users. Social networks like Facebook and Twitter have seemingly opened the floodgates to security troubles, and over the past few weeks, this has been accentuated by a number of issues and studies.

For businesses, managing security risks via its employees can be more challenging, but is necessary, as potential risks include inadvertent disclosure of sensitive enterprise information such as financial data, corporate intellectual property and IT infrastructures. "There is no way organizations can hold back the flow of social media, so it is better to put policies and technologies in place to manage it," says David Cripps, information security officer at Investec[1].

The goal of this paper is not to stop you from participating in social networks but to enable you to use them more safely.
When you submit your paper print it in two-column format, including figures and tables. In addition, designate one author as the "corresponding author". This is the author to whom proofs of the paper will be sent. Proofs are sent to the corresponding author only.

3. Survey

A survey says that 65% of online adults use social networking sites and most describe their experiences in positive terms. Two-thirds of adult internet users (65%) now say they use a social networking site like MySpace,

Facebook or Twitter, up from 61% one year ago. That's more than double the percentage that reported social networking site usage in 2008 (29%). Pew Internet survey report states that half of all adults (50%) use social networking sites. The pace with which new users have flocked to social networking sites has been staggering; when asked about social networking sites in February of 2005, just 8% of internet users – or 5% of all adults – said they used them.

Looking at usage on a typical day, 43% of online adults use social networking, up from 38% a year ago and just 13% in 2008. Out of all the "daily" online activities that we ask about, only email (which 61% of internet users access on a typical day) and search engines (which 59% use on a typical day) are used more frequently than social networking tools.
A survey done by pewinternet.org shows the percentage of adult internet users of each gender who use social networking sites since 2005-2011 [2].

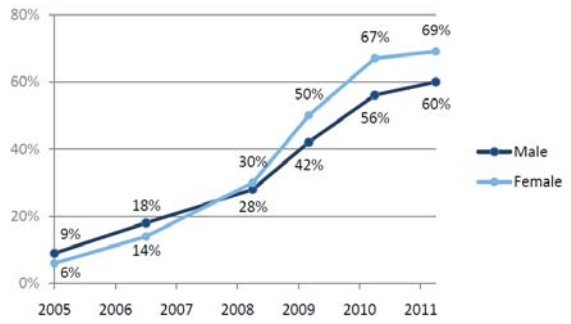

Figure.1: Percentage of adult internet users, 2005-2011

As WebProNews recently reported, based on a study from Russell Herder and Ethos Business Law, time on social networking sites has increased by 73% in the past year. Without even taking security into consideration, 51% of executives surveyed said they fear social media could reduce employee productivity, while 49% said that using social media could damage a company's reputation.

As of June 2010, twenty-two percent of all time spent on-line is social, i.e., messaging, commenting, blogging and sharing.[3] For the first time ever, social network or blog sites are visited by three quarters of global consumers who go on-line.[4] In the U.S. alone, the total minutes spent on social networking sites has increased eighty-three percent year-over-year.[5]These results are astounding for such a new media: e.g., Mark Zuckerberg launched Facebook, currently the most popular social networking site worldwide, only in February 2004. Upward trends in user membership, corporate marketing and other metrics with respect to social networking sites are expected to continue.[6] The issue of information security on social networks is paramount, but has largely been tabled by social networking sites in favor of emphasizing user growth and brand marketing. Achieving information security within the Web 2.0 arena of social networking, though, is difficult and complicated, as users tend to overlook security risks; businesses downplay the gravity of the security issues, and owners of social networking sites are somewhat conflicted by financial incentives that run contrary to privacy and security concerns.

Social network users are more vulnerable to security risks. This is the theme of another study recently released by AVG and CMO Council. Most social network users fail to perform the following basic security measures on a regular basis:

- Changing passwords (64% infrequently or never)
- Adjusting privacy settings (57% infrequently or never)
- Informing their social network administrator (90% infrequently or never)

Here are some more stats from that one:

- 21% accept contact offerings from members they don't recognize
- Over half let acquaintances or roommates access social networks on their machines
- 64% click on links offered by community members or contacts
- 26% share files within social networks
- Nearly 20% have experienced identity theft
- 47% have been victims of malware infections
- 55% have seen phishing attacks

A recent report from the Web Hacking Incidents Database (WHID) found that 19% of hacking incidents occurred on social networks in the first half of this year. They were the most heavily-targeted vertical.

Criminals are using social networks to target people in the real world. A report from The Digital Criminal, found that 38% of users of sites like Facebook and Twitter have posted status updates saying when they are away for the weekend.
But not only is social networking a threat to a company's security because of what employees might disclose, but also because social networking sites are a prime target for cyber criminals.

According to the *Cisco 2013 Annual Security Report*, the highest concentrations of online security threats are on mass audience sites, including social media. The report revealed that online advertisements are 182 times more likely to deliver malicious content than pornography sites, for example.

The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses. In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information, which can be just as damaging.

The rapid spread of false information through social media is among the emerging risks identified by the World Economic Forum in its *Global Risks 2013* report.

The report's authors draw the analogy of shouting "Fire" in a crowded cinema. Within minutes, people can be trampled to death before a correction can be made to the message. In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information.

There have been several incidents over the past year where false information transmitted on the internet has had serious consequences, according to the report.

For example, a fake tweet by someone impersonating the Russian interior minister, claiming that the Syrian president had been killed or injured, caused crude prices to rise by over $1 before traders realized the news was false.

4. Security and privacy issues associated with social networking sites

Social networking sites have become very popular avenues for people to communicate with family, friends and colleagues from around the corner or across the globe. While there can be benefits from the collaborative, distributed approaches promoted by responsible use of social networking sites, there are information security and privacy concerns. The volume and accessibility of personal information available on social networking sites have attracted malicious people who seek to exploit this information. The same technologies that invite user participation also make the sites easier to infect with malware that can shut down an organization's networks, or keystroke loggers that can steal credentials. Common social networking risks such as spear phishing, social engineering, spoofing, and web application attacks attempt to steal a person's identity. Such attacks are often successful due to the assumption of being in a trusting environment social networks create.

Security and privacy related to social networking sites are fundamentally behavioral issues, not technology issues. The more information a person posts, the more information becomes available for a potential compromise by those with malicious intentions. People who provide private, sensitive or confidential information about themselves or other people, whether wittingly or unwittingly, pose a higher risk to themselves and others. Information such as a person's social security number, street address, phone number, financial information, or confidential business information should not be published online. Similarly, posting photos, videos or audio files could lead to an organization's breach of confidentiality or an individual's breach of privacy

When it comes to privacy and security issues on social networks, the sites most likely to suffer from issues are the most popular ones example face book and twitter. But security issues and privacy issues are entirely two different beasts. A security issue occurs when a hacker gains unauthorized access to a site's protected coding or written language. Privacy issues, those involving the unwarranted access of private information, don't necessarily have to involve security breaches. Someone can gain access to confidential information by simply watching you type your password. But both types of breaches are often intertwined on social networks, especially since anyone who breaches a site's security network opens the door to easy access to private information belonging to any user. But the potential harm to an individual user really boils down to how much a user engages in a social networking site, as well as the amount of information they're willing to share.

The reason social network security and privacy lapses exist results simply from the astronomical amounts of information the sites process each and every day that end up making it that much easier to exploit a single flaw in the system. There is an exposure in potentially devastating hole in the framework of Facebook's third-party application programming interface (API) which allows for easy theft of private information. It has been found that third-party platform applications for Facebook gave developers access to far more information (addresses, pictures, interests, etc.) than needed to run the app.

This potential privacy breach is actually built into the systematic framework of Facebook, and unfortunately the flaw renders the system almost indefensible. There are many issues like

a. The question for social networks is resolving the difference between mistakes in implementation and what the design of the application platform is intended to allow
b. There's also the question of whom we should hold responsible for the over-sharing of user data?

That resolution isn't likely to come anytime soon, because a new, more regulated API would require Facebook - to break a lot of applications, and a lot of companies are trying to make money off applications now. It is also true that “now there are marketing businesses built on top of the idea that third parties can get access to data on Facebook."

Since social networks are all about “friends,” getting hold of a victim's account will provide the hacker knowledge of that victim's circle of friends. Once the hacker has access, they can pose as a trusted friend, creating phishing messages containing links to malware or including malware-laden files. Because the messages purportedly come from a “friend,” the victim may be more susceptible to follow the links or open the attachments. A method has been established to gain access to the account of a specific user is getting the password. But how can this be accomplished? There are myriad ways:

- Malware: Keystroke loggers can record a user's activity, including passwords for different applications. This malware can be installed through social engineering techniques circulated via email or over a social network, like Facebook, that encourage a user to download a malicious application masquerading as a legitimate one.

- Phishing: By creating a mock login page, hackers can attempt to deceive users into divulging their login credentials. Once the hackers have the login information, they can then access the user's profile, gaining access to their network of friends and other personal information.

- Bruteforce: Hackers can repeatedly attempt to guess a user's password. This technique can be especially effective

against users with easy-to-guess passwords, like “password” or “12345.”

Hackers communicate with each other in online hacking forums, selling services to teach other hackers how to use the above methods to breach the accounts of unsuspecting users.

If users don't take the appropriate precautions to protect their social networking profiles, there can be nasty consequences – not just for the user, but also for their employers, families and greater communities.

The MilitarySingles.com, a dating website for members of the military, was compromised by hackers, resulting in the publishing of names, email addresses and passwords for more than 150,000 of the site's members. This breach was likely caused by uploading a malicious file masquerading as a .JPEG attachment on the website.

The pervasiveness of web applications, combined with the tendency of social media users to increasingly reveal private information, can create a serious security risk. In the case of MilitarySingles.com, the personally identifiable information of members of the U.S. military was accessed, giving hackers access to the email accounts of military members and, arguably, access to potentially damaging secrets.

5. Discussions

It is worth mentioning the fact that Human Resource (HR) departments are already utilizing information on social networks’ public profiles to know more about job candidates. A certain online recruitment website reports that 20% of employers use social networking sites to run searches on job applicants and 68% use search engines like Google and Yahoo! to check on candidates. Although this common practice is not strictly illegal, it might be ethically questionable.

In July 2009, the wife of a high-level government executive in the United Kingdom published personal data in a social networking site. This garnered a lot of attention, not for the confidentiality of the content but for the lack of awareness there is about the accessibility of your online content. There is also another issue at play here, which is the fact that once you publish any picture online, you lose control over it as people leech and republish it on places you do not even know. In this case, news sites were some of the first to republish the infamous family pictures originally shared by the said executive’s wife.

It wouldn’t be fair to say that the social networks have ignored security issues. They haven’t. But are they doing enough? Twitter recently began trying to block links to malicious sites when users try to post them. Facebook has spent some time trying to improve the process of helping users gain back their hacked accounts.

But the threats are still out there, and they seem to be increasing much more rapidly than they’re being eliminated. These are not easy problems no doubt that the social networks take them very seriously, but until people can really feel comfortable about the medium its potential is going to be hampered.

Companies should also recognize that analysis of the information in social conversations can produce security intelligence to improve security processes and enhance performance, according to Gartner analyst Andrew Walls.

“Analysis of public conversations can identify imminent, credible threats of physical or logical attack,” he wrote in a 2012 Gartner paper entitled *Security Tools for Control of Social Media.*

Wall also cautioned against attempts to block access to external social media because they have proved to be ineffective at controlling risks and impede the development of enterprise social media initiatives. “Unfortunately, organizations that block access to social media rarely analyze social content for security intelligence and remain ignorant as to the risk and potential of social media,” he said.

Social networking sites continue to grow in popularity as attack vectors because of the volume of users and the amount of personal information that is posted. The nature of social networking sites encourages you to post personal information. The perceived anonymity and false sense of security of the Internet may cause users to provide more information about them and their life online than they would to a stranger in person.

A company can implement technical barriers to prevent any use of Twitter, Facebook or similar applications, but then the company may have lost a valuable sales and marketing tool in its effort to protect its security or privacy.

Alternatively, the company could (and should) have an Acceptable Use Policy, a document that details how these applications and the Internet in general can be used. The policy also defines consequences for failure to comply, which might be as simple as a written reprimand or as heavy as termination of employment and legal action. You can find some excellent Acceptable Use Policy templates at the System Administration, Networking and Security (SANS) Institute.

6. Attacking Scenarios

6.1 Privacy related threats

a) Digital dossier aggregation. SNS profiles can be fetched and stored by third parties in order to create a digital dossier of personal data. Hogben et al. [7] argue that due to diminished costs of disk storage and Internet downloads it is feasible to take incremental snapshots of entire SNSs. A proof-of concept digital dossier aggregation, carried out on an early version of the most popular German SNS (meinVZ), showed that 1.074.574 profiles could be aggregated within less than four hours with a computer cluster consisting of ten computers [8]. [9] Highlighted various methods how data could be collected from Facebook. [10] Further more showed that information that is publicly available could be used to infer the social graph of SNSs users. A commercial provider [11] even offers packages for crawling social

networks which can be used to aggregate publicly available information.

b) Secondary data collection vulnerabilities. SNS members also disclose information to their Internet service providers (ISPs). While this is not solely limited to SNSs, the main difference is the extent of coherent personal data exposed to ISPs. For example to map the circle of friends without SNSs data, ISPs need to correlate information from multiple Email addresses, instant messaging, etc. Even more important is the threat of disclosure and resale of personal information to third parties, for example to providers of targeted advertisement. At the time of writing no case of secondary data collection has been documented. A recent case with AT&T [12] however illustrated how serious this threat is.

c) Face recognition vulnerabilities. SNS users provide profile images of themselves and SNSs contain shared images associated with them. Face recognition technology can be used to identify users across different SNSs, no matter if pseudonyms or fake names are being used.

d) CBIR (Content-based Image Retrieval). CBIR is a technology which deduces the location of users by analyzing and comparing common patterns in images. Hence shared images within SNSs not only disclose the identity of users but possibly the location of users as well.

e) 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 [13]. This type of attacks are done to do malicious attack or to make some page popular.

f) Neighborhood Attack: The neighborhood attacks are done by the attackers by knowing the victim's neighborhood [13]. 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.

g) Linkability from Image Metadata, Tagging and Cross-profile Images. While users control which information and media they share within a SNS, they can't control which content other users upload and link to their profile. Images might also contain metadata including the serial number of the camera used to make the pictures.

h) Difficulty of Complete Account Deletion. Users that wish to deactivate their SNS account face difficulties to do so in most cases. On the one hand because not all comments and messages sent to other users will be deleted, and on the other hand because SNS providers keep backups of account data. Most social networking sites offer the possibility to permanently delete an user account, this features are however often hidden from users. In the case of Facebook users have to follow a special link which can only be found through a search within the Facebook support center.

i) 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 [14]. 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.

6.2 Security threats

a) **Social Networking Spam**: As SNSs steadily grow they have become interesting targets for spammers. The use of SNS spamming software furthermore automates the process of sending unsolicited bulk messages. The Spam content can reach from advertising to Phishing messages. A study based on anonymized headers of 362 million messages exchanged by 4.2 million users of Facebook, claimed that 43 per cent of all messages analyzed were to be considered as Spam [15]. [16] Outlined a similar threat with context-aware spam. [14] furthermore outlined how social networking sites can be misused to automatically profile targets of spam campaigns.

b) **Cross Site Scripting, Viruses and Worms**: In order that users are able to customize the design of their profiles, SNSs often provide the possibility to post HTML code. Furthermore third party applications (widgets) are used to extend the functionality of SNSs and together with HTML code they state a risk for Cross-site scripting (XSS) vulnerabilities. Samy/JS.Spacehero for example was a XSS worm on MySpace, which infected more than one million profiles within the first 24 hours. A number of worms targeted other social networking sites like Facebook, MySpace, and Orkut [17] [18].

c) **SNS Aggregators:** Social Aggregators offer services to integrate the data from different web services and SNSs into a single platform. Popular services include Gathera, FriendFeed, Spokeo and Secondbrain. As with all single-sign-on systems, the access to multiple services (in this case SNSs) depends on only one password which if selected badly states a single point failure. These services are also used to correlate user data across different SNSs. Spokeo for example provides a charged service which aggregates data of 41 social networks with someone's Email address being the only information required. As [19] point out, SNSs providers are trying to inhibit SNS aggregators in order to "lock-in" users to their social networking service.

6.3 Identity related threats

a) **Spear Phishing using SNSs and SN-specific Phishing**: Spear Phishing attacks are targeted Phishing attacks. The information available through SNSs is harvested by scammers and used as a basis for a spear Phishing attack. SNSs are furthermore used as a medium for carrying out the Phishing attack itself, rather than using standard Email messages. Jagatic et al. [20] showed that social graph information can be misused to improve the success rate of phishing,

b) **Infiltration of Networks Leading to Information Leakage**: SNSs allow users to define who has access to their personal information, for example by giving access to certain ”friends“ or by defining restricted groups (networks). These are important features to improve the privacy issues of SNSs usage but once a closed network is infiltrated the protection is rendered useless. [21] showed that cloning of user profiles could be misused to infiltrate private networks, while [22] outlined yet another attack to infiltrate closed networks via HTTP cookie hijacking.

c) **Profile-squatting and Reputation Slander through ID Theft:** Profile-squatting is similar to domain squatting, only that instead of Internet domains persons are targeted. Fake profiles are set up in the name of someone else in order to slander her/his reputation within a certain network. Examples include the Moroccan computer engineer who set up a name of a member of the royal family [23], and an Italian soccer player who sued Facebook for defamation.

6.4 Social threats

a) **Stalking:** SNSs can be misused by perpetrators to contact their victims but also to gather information on them. SNSs users often disclose location data via their pictures (see CBR) or personal information.

b)**Cyber-bullying and grooming**: Cyber-bullying are aggressive attacks and bullying attempts carried out over the Internet, while cyber-grooming refers to attempts by adults to approach minors via the web to abuse them sexually. One of the most infamous cases involving cyber-bullying, the ”Megan Meier case”, led to the suicide of a teenage girl .In the Meg Meier case the perpetrator exploited the ease of setting up a fake profile, which was also used in a recent cyber-grooming case .[24] outlined possible automated social engineering attack on basis of social networking sites.

This is really the tip of the iceberg. As social media continue to mash into everyday culture, like e-mail, hackers will continue to exploit lapses and holes. There is progress to be made, and it likely will be made. Once we get over that hump, this social web thing should really take off.

7. Suggestions

There are ways to manage the risks. Here we list some general tips for users while Using Social Networks.

It's important for social media users to take the following precautions:

1. Ensure that any computer you use to connect to a social media site has proper security measures in place.
2. For starters, you should only publish information that you are perfectly comfortable with, depending on what you want to accomplish. In a dating site, you will want to state your age but not your exact birthday. In a site where you plan to meet your high school friends, your year of graduation is probably the most important thing and date of birth will not be something you need to share at all. This may sound logical on a security standpoint but many people do not give it a second thought when opening their accounts.
3. Configure privacy settings to allow only those people you trust to have access to the information you post. Also, restrict the ability for others to post information to your page. The default settings for some sites may allow anyone to see your information or post information to your page; these settings should be changed. Become familiar with the privacy settings available on any social network you use. On Facebook, make sure that your default privacy setting is "Friends only". Alternatively, use the "Custom" setting and configure the setting to achieve maximum privacy.
4. Review a site's privacy policy. Some sites may share information such as email addresses or user preferences with other parties. If a site's privacy policy is vague or does not properly protect your information, do not use the site.
5. Remove your information from Google search crawlers. Don’t share your birthday, age, or place of birth. This information could be useful to identity thieves and to data mining companies. A research study by Carnegie Mellon University found that Social Security numbers can be predicted based on publicly-available information, including your birthday, age and place of birth. The Social Security Administration began assigning randomized number series on June 25, 2011. Unfortunately, the more predictable Social Security numbers will remain in effect for individuals born before June 25, 2011. If you do consider posting your birthday, age or place of birth, restrict who has access to this information using the site’s privacy settings. Also, some social networking sites allow you to show your birth month and day, but hide the year.
6. Stay aware of changes to a social network’s terms of service and privacy policy. You may be able to keep track of this by connecting to an official site profile, for example Facebook’s Site Governance. Consider subscribing to an RSS feed for Tosback, a project of the Electronic Frontier Foundation to track changes in website policies (covers some but not all social networks).
7. Be careful when you click on shortened links. Consider using a URL expander (as an application added to your browser or a website you visit) to examine short URLs before clicking on them. Example of URL expanders include LongURL, Clybs URL Expander and Long URL Please. Use caution when clicking a link to another page or running an online application, even if it is from someone you know. Many applications embedded within social networking sites require you to share your information when you use them. Attackers use these sites to distribute their malware.
8. Be very cautious of pop-up windows, especially any that state your security software is out of date or that security threats and/or viruses have been detected on your computer. Use your task manager to navigate away from these without clicking on them, then run your spyware and virus protection software.
9. Delete cookies, including flash cookies, every time you leave a social networking site.
10. Remember that whatever goes on a network might eventually be seen by people not in the intended

audience. Think about whether you would want a stranger, your mother or a potential boss to see certain information or pictures. Unless they are glowing, don't post opinions about your company, clients, products and services. Be especially cautious about photos of you on social networks, even if someone else placed them there. Don't be afraid to untag photos of yourself and ask to have content removed.

11. Do not assume privacy on a social networking site. For both business and personal use, confidential information should not be shared. You should only post information you are comfortable disclosing to a complete stranger.
12. Don't publicize vacation plans, especially the dates you'll be traveling. Burglars can use this information to rob your house while you are out of town.
13. Turn off a social network's information sharing functionality. For example, Facebook's "Platform" should be turned off so your browsing history cannot be tracked. If you use a location-aware social network, don't make public where your home is because people will know when you are not there. In fact, you should be careful when posting any sort of location or using geotagging features because criminals may use it to secretly track your location. For the same reason, be careful not to share your daily routine. Posting about walking to work, where you go on your lunch break, or when you head home is risky because it may allow a criminal to track you.
14. Be aware that your full birth date, especially the year, may be useful to identity thieves. Don't post it, or at a minimum restrict who has access to it.
15. Don't post your address, phone number or email address on a social network. Remember scam artists as well as marketing companies may be looking for this kind of information. If you do choose to post any portion of this, use privacy settings to restrict it to approved contacts.
16. Use caution when using third-party applications. For the highest level of safety and privacy, avoid them completely. If you consider using one, review the privacy policy and terms of service for the application.
17. Be careful who you add as a "friend," or what groups or pages you join. The more "friends" you have or groups/pages you join, the more people who have access to your information. If you receive a request to connect with someone and recognize the name, verify the account holder's identity before accepting the request. Consider calling the individual, sending an email to his or her personal account or even asking a question only your contact would be able to answer.
18. Prune your "friends" list on a regular basis. It's easy to forget who you've friended over time, and therefore who you are sharing information with.
19. If you receive a connection request from a stranger, the safest thing to do is to reject the request. If you decide to accept the request, use privacy settings to limit what information is viewable to the stranger and be cautious of posting personal information to your account, such as your current location as well as personally identifiable information.
20. Be wary of requests for money, even if they are from contacts you know and trust. If a contact's account is compromised, a scam artist may use his or her name and account to attempt to defraud others through bogus money requests.
21. In the event that your social networking account is compromised, report it to the site immediately and alert your contacts. You will need to change passwords, but proceed with caution because your computer security may have been compromised. Malware, including key-logging software, may have been installed on your computer. If you use online banking, do not log on from the computer that may have been compromised until you have ensured your computer security is intact.
22. If you are using a social networking site that offers video chatting, pay attention to the light on your computer that indicates whether or not your webcam is in use. This will help you avoid being "caught on camera" by accident.
23. Be sure to log off from social networking sites when you no longer need to be connected. This may reduce the amount of tracking of your web surfing and will help prevent strangers from infiltrating your account.
24. Implement restrictions on social media if necessary: The MilitarySingles breach shows that carelessness on social media sites can have potentially dire consequences. Organizations should take necessary precautions to ensure that members are protected from potential breaches via social media, even if that means restricting them from participating.
25. As long as social networking continues to be a preferred forum for connecting and communicating with other people, hackers will turn their attention to subversion.

7.1 How is it possible to identify the legitimate messages from the hoaxes?

a) Use an up-to-date email client such as Microsoft Outlook 2007, Outlook Express or Mozilla Thunderbird which have spam filtering enabled and checks for "phishing" messages (phishing messages are falsified emails that use these tactics to obtain your username, password or other personal information).
b) Never open an attachment unless it's from someone you know, and you are expecting to receive it. If you have any doubt, then contact the individual and ask if he/she actually did send it.
c) Use up-to-date antivirus/anti-malware software on your computer to block any harmful files that you may have accidentally opened.
d) Always use common sense on the web and in email; take an extra moment or two to think about what you have received or are about to do. For example, would Twitter really email an invitation in a zipped attachment? Not likely.

8. Conclusion

Love it or hate it, social media is part of the business world. With increasing use of SNSs, the associated security risks are also increasing tremendously. As long as threats remain so prevalent, so will reluctance. That goes for businesses and

individuals alike. Yes, social media adoption continues to grow rapidly, but there are many still out there who do not see the point, at least at the price of security. In this paper, we have discussed some of the privacy and security concerns and prevention techniques that helps user to be careful while working on social media. We have also discussed few stuffs related to the issues concerned with social media, listed the threats & lastly we added up few suggestions for users.

This paper further helps to develop the tools or help the developers of sites to add up the privacy settings to build a well versed SNS's. Users provide personal information about them including their interests, social relationships, current occupation, pictures and other media content, and share this information via SNSs platforms. Further we can look at what businesses can do to keep consumers safe while keeping their brand from being tarnished if an account is hacked or spoofed.

References

[1] www.computerweekly.com.
[2] Pew Research Center's Internet & American Life Project surveys: February 2005, August 2006, May 2008, April 2009, May 2010, and May 2011.
[3] http://blog.nielsen.com/nielsenwire/online_mobile/social-media-accounts-for-22-percent-of-time-online/Id.
[4] http://www.nielsen-online.com/pr/pr_090602.pdf
[5] http://www.professionalexperts.net/articles.php?article_id=49;
[6] http://www.pcworld.com/businesscenter/article/202333/take_advantage_of_increased_time_spent_on_social_networking.html.
[7] G. Hogben. Security Issues and Recommendations for Online Social Networks. Position Paper. ENISA, European Network and Information Security Agency, 2007.
[8] Hagen Fritsch. StudiVZ - Inoffizielle Statistiken vom Dezember 2006. online, 2008. [Retrieved 2008-11-29].
[9] J. Bonneau, J. Anderson, and G. Danezis. Prying data out of a social network. In First International Conference on Advances in Social Networks Analysis and Mining, 2009.
[10] J. Bonneau, J. Anderson, R. Anderson, and F. Stajano. Eight friends are enough: social graph approximation via public listings. In Proceedings of the Second ACM EuroSys Workshop on Social Network Systems, pages 13–18. ACM, 2009.
[11] 80legs. http://80legs.com/.
[12] EFF. Some lessons from the at&t/facebook switcheroo, 2010. [Online; accessed 10-March-2010],http://www.eff.org/deeplinks/ 2010/01/some-lessons-att-facebook.
[13] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin. Persona: An online social network with user-defined privacy. ACM SIGCOMM Computer Communication Review, 39(4):135–146, 2009.
[14] M. Balduzzi, C. Platzer, T. Holz, E. Kirda, D. Balzarotti, and C. Kruegel. Abusing Social Networks for Automated User Profiling. 2010.
[15] S. Golder, D.M. Wilkinson, and B.A. Huberman. Rhythms of social interaction: messaging within a massive online network. Arxiv preprint cs.CY/0611137, 2006.
[16] G. Brown, T. Howe, M. Ihbe, A. Prakash, and K. Borders. Social networks and context-aware spam. In Proceedings of the ACM 2008 conference on Computer supported cooperative work, pages 403–412. ACM New York, NY, USA, 2008.
[17] SophosLabs. Large scale orkut virus outbreak not cool, 2009. [Online; accessed 12-March-2010], http://www.sophos.com/blogs/sophoslabs/v/ post/900.
[18] SophosLabs. Xss worm targeting chinese website, 2009. [Online; accessed 12-March-2010], http://www.sophos.com/blogs/sophoslabs/v/ post/6208.
[19] J. Bonneau and S. Preibusch. The Privacy Jungle: On the Market for Privacy in Social Networks. In Eighth Workshop on the Economics of Information Security (WEIS), 2009.
[20] A. Felt and D. Evans. Privacy protection for social networking APIs. 2008 Web 2.0 Security and Privacy (W2SP'08), 2008.
[21] Leyla Bilge, Thorsten Strufe, Davide Balzarotti, and Engin Kirda. All your contacts are belong to us: Automated identity theft attacks on social networks. In 18th International World Wide Web Conference, April 2009.
[22] Markus Huber, Martin Mulazzani, and Edgar Weippl. Who on earth is "mr. cypher": Automated friend injection attacks on social networking sites. In Proceedings of IFIP/SEC 2010, 2010. to appear.
[23] BBC News. Jail for Facebook spoof Moroccan. online, 2008. [Retrieved 2008-12-01].
[24] Markus Huber, Stewart Kowalski, Marcus Nohlberg, and Simon Tjoa. Towards automating social engineering using social networking sitesComputational Science and Engineering, IEEE International Conference on, 3:117–124, 2009.

Author Profile

Mr. Kiran B. Malagi is from Hubli, India. He has born on 8th July 1981. He has received the B.E degree in Computer Science and Engineering from Visvesvaraya Technological University, India in the year 2005 and the M.Tech degree in Computer science and Engineering from the Visvesvaraya Technological University, India in the year 2010. He has been working in the area of data mining and social networking since 2010. He worked as Lecturer and head about 6 years .He is currently working as an Assistant Professor in K.L.E.I.T, Hubli, India since 2010.

Akshata B. Angadi received the BE degree in Computer Science from Visvesvaraya Technological University, India in 2011. She is currently working as a Lecturer in K.L.E.I.T., Hubli since 2011. She has attended many conferences. She has published 2 papers on Data Mining, 1 paper on Cloud computing & 1 paper on Mobile application in International Journals. She has also published 2 National papers in Conference Proceedings.

Karuna Gull is from Hubli, India. She has born on 7th June 1974. She has received the B.E. degree in Electronics and Communication from Karnataka University, India in the year 1996 and the M.Tech degree in Computer science and Engineering from the Visvesvaraya Technological University, India in the year 2008. She

has been working in the area of data mining and social networking since 2009. She has published 3 papers on Data Mining, 1 paper on Cloud Computing & 2 papers on Image Processing in International Journals. She has also published 5 National and 4 International papers in Conference Proceedings. She has also attended many of the workshops and conferences held in different places on High Impact Teaching Skills, Embedded System Using Microcontroller, Information Storage and Management (ISM), Data Mining, and many more. She worked as a Lecturer and Senior Lecturer for about 10 years. She is currently working as an Assistant Professor in K.L.E.I.T., Hubli, India since 2011.