# Security Issues in Social Networking

**Damera Vijay Kumar[†] , P S S Varma2[††] and Shyam Sunder Pabboju[†††]**

[†]Department of Information Technology, MGIT, India
[††]Department of Computer Science, MGIT, India
[†††]Department of Computer Science, MGIT, India

**Summary**
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. Social networking has transformed the way the connected masses communicate . Social network information is now being used in ways for which it may have not been originally intended. In today's socially connected workplace, information flows freely between employees and their online followers. This can pose serious risks to an enterprise's network, data, and reputation. In this paper we present several of these privacy and security issues of Social Networks

***Key words:***
*Social networks , Security, privacy, Facebook and Twitter*

## 1. Introduction

Today, social networking is as routine as sending an e-mail at home or work. Employees swap updates on Facebook and Twitter, log opinions at blogs, and upload snapshots to photo-sharing sites. The result for businesses? A digitally connected social world in which the line between personal and corporate lives is increasingly blurred. As this digital conversation swells, potential risks to businesses also rise. Simply said, not all data being shared is as innocent as weekend plans.

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.

## 2. The benefits of social Networks

Businesses are embracing social networking to cultivate an internal culture of collaboration. Additionally, it is easy to see how this free flow of information can boost productivity and autonomy. Employees working on a project will have relevant, current, and customized knowledge at their fingertips, and they can tap into a ready-built group of team players at all levels of the organization.

Outside the organization, social networking can help a business reach and engage customers, improve the customer experience, and manage its brand image. Many businesses today patrol sites such as Twitter and Facebook, for instance, to listen in on the chatter about their products and services. Their online brand ambassadors can promote new products or, if a business's reputation is threatened, use social media to move the discussion in the right direction.

Businesses also take advantage of online customer voices to create a more effective advertising campaign. Successful brands leverage customer experiences as an integral part of a product campaign and life cycle. Consider, for instance, the success of Apple. Apple customers have a tight emotional bond to the brand and track the company and its

Manuscript received June 5, 2013
Manuscript revised June 20, 2013

products on blogs, Twitter feeds, and Facebook. How deep is the connection? Apple retail stores in some cities have now become tourist attractions. Anyone can read about them on Twitter.

## 3. Facebook

Three of the most popular features of Facebook are the ability to add Friends, update your status and run applications such as games and quizzes. A "Friend" is anyone on the Facebook network whom you allow to see various levels of personal information, such as job, birth date, photos, group membership, comments and list of other Friends. You can even play online games and keep others updated on your daily life. Friends can also see Friends of Friends, meaning individuals, whom you have officially befriended and may.

### Updates

At the top of the user's Facebook profile is the Update field, which allows the user to post a sentence or paragraph regarding any topic at any time. LinkedIn has a similar field, but it does not allow as much text, and it's not possible to connect links, photos or videos with the update. Here are some examples of updates that my Facebook friends have recently posted. These are very typical:

- "Just received a job offer. Hooray!"
- "I'm tired of all the rain."
- "Looking forward to the family vacation next week at Disney World."

Although these might seem relatively harmless, the third bullet point could raise some concern. You have just told all your friends, as well as all their friends, that you will be away from home for a full week. This is comparable to putting a sign on the main road that shouts "Empty House" for passers-by to see. Even if you have a burglar alarm or neighbors keeping an occasional eye on the home, you still don't want to create the temptation for strangers (Friends of Friends) to consider helping themselves to that wonderful, new 52" flat screen TV you just purchased.

### Applications

Facebook offers thousands of applications that its users can install and run. These applications include calendars that allow Friends to be reminded when it's your birthday, tools to send Friends online greeting cards, quizzes on myriad topics and much more. (See Figure 1.).

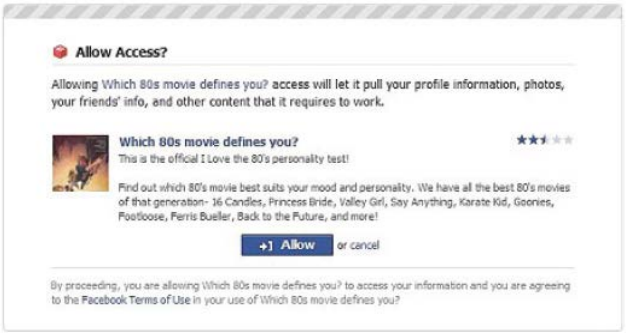


Figure 1: Even though applications provide warning messages, many users still install and run them, unaware of what they may do to your system.

Many of the applications were designed by Facebook end-users. Although the applications on Facebook may look harmless, and in fact most probably are, there are always some that may deliver malicious content to your computer. This holds true not only to Facebook, but also to other social networking sites and to the Internet in general, when downloading from the web or opening attachments in email messages. Therefore, make certain that your computer has a proper and functional firewall, as well as up-to-date antivirus/anti-malware software, and only install or run these applications if they are from a trusted source or approved by your corporate IT department.

## 4. Twitter

Twitter is an online application that allows you to post brief comments (tweets) on any topic. Other users on the Twitter network can become followers of your tweets, such that they receive the updates whenever you send them. Both Twitter and Facebook users must be very careful about the personal information that they tweet and how it may be used. Employers must be especially attentive to the information that is posted and how it can affect their company. For example:

- "The boss just laid off 32 employees. I hear there may be more coming on Wednesday."
- "Rumor has it that the Acme Widgets acquisition fell through."
- "Working to troubleshoot a major software bug we just found."
- "I just posted a funny video of myself frying a rodent at the restaurant where I work."

Each of the four statements can have serious public relations and financial consequences for the company whose employee tweeted or posted the information. The impact can be even more serious if that company


Figure 2: Users can post a "tweet" on any topic, as well as receive the tweets of those they are following.

is publicly owned. The first two statements will create a public perception that the company is doing poorly or will continue to experience loss, and shareholders may begin to sell off their stocks, reducing the value of the company. The third statement will raise concern amongst the company's customers who have purchased the software, possibly tempting them to investigate competitors' solutions. And the fourth statement, which actually occurred to a well-known, nationwide fried chicken company in 2008, will certainly give customers second thoughts about going to visit the restaurant, even if the video wasn't real.

### Acceptable use policies

Unfortunately, there is no simple solution to manage these issues. Certainly 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, but just know that you will need to customize them to fit your company's culture and HR needs.

Beyond Acceptable Use Policies, however, companies will still have a difficult time restricting what employees do at home. Employees will have their own Twitter and Facebook accounts, set up websites like AcmeWidgetsSux.com and put all levels of derogatory and inflammatory comments, whether true or not, onto those sites. Although the company may have legal recourse when this occurs, the damage may already have been done and the cleanup can be a very expensive and involved undertaking.

## 5. Why social media may be hazardous to the corporate network

As the adoption of social networking grows exponentially, Every organization have begun to understand that they must change the way they safeguard their networks and sensitive data. They are concerned about the risks of social networking, and rightly so. As we have seen, employees may easily leak critical (and regulated) information via social media. And ambitious cyber criminals can gain access to sensitive data by infecting networks with malicious code that connects to Web 2.0 platforms, such as Facebook and Twitter.

Cyber attacks are dangerously effective on social media because they often generate seductive messages that appear to come from trusted friends. The subject lines such as "You look just awesome in this new video" direct unsuspecting users to sites that employ phishing schemes or malware to obtain sensitive personal information.

In addition to personal and proprietary information considerations, data leakage can violate confidentiality mandates. A recent study published in the Journal of the American Medical Association found that 13 percent of medical school deans surveyed reported student violations of patient confidentiality via social media.

Another threat comes from anything-goes commentary by employees or the public that can cause serious reputational damage when opinion becomes negative or untruthful. Thanks to the instant flow of information and opinions, a public relations blip can quickly become disastrous as it ricochets among consumers and customers. These malicious comments can be very difficult to remove or address effectively.

Meanwhile, legal ownership of information on social sites remains uncharted territory. Content created on a social network might become the property of the network; yet if the data is posted using corporate equipment (a personal computer or smart phone), the business might be held legally accountable. In the event of legal disputes and e-discovery, companies might be required to disclose information posted on social networking sites.

## 6. How businesses can balance security and social networking

Let's face it: There is no stopping the two-way flow of information. Instead, PricewaterhouseCoopers believes, businesses should embrace social media and adopt a proactive strategy to safeguard corporate networks and data. The strategy must be two-pronged: It must set forth policies and procedures that govern the use of social networks and corporate information, and it must use technology that helps protect the safety and integrity of data and the corporate network. This multilayered approach requires that the business and technology sides of the company unite and fully commit to the initiative. The two must analyze content and policies in detail, as well as determine the right mix of enterprise technologies available to monitor, classify, and manage data.

### What are the precautions I should take?

Below are some helpful tips regarding security and privacy while using social networking sites:

- Ensure that any computer you use to connect to a social media site has proper security measures in place. Use and maintain anti-virus software and keep your application and operating system patches up-to-date.
- 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.
- Use strong and unique passwords. Using the same password on all accounts increases the vulnerability of these accounts if one becomes compromised.
- If screen names are allowed, do not choose one that gives away too much personal information.
- 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.
- 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.
- Use discretion before posting information or commenting about anything. Once information is posted online, it can potentially be viewed by anyone and may not be retracted afterwards. Keep in mind that content or communications on government-related social networking pages may be considered public records.
- 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.

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.

## 7. Conclusion

Social networking sites can be valuable sales and marketing tools, as well as fun diversions. Inherent in these applications are security risks that can put the individual or a company in a compromising position or at serious risk. Aside from not using these sites at all, end-user education, alongside documented policies and procedures, is the most fundamental protection that exists. A well-informed user will not only help to maintain security, but will also educate others on these issues and establish best practices which can be standardized and updated as applications mature or as new applications come along.

## References

[1] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee,"Measurement and analysis of online social networks," in Proceedings of the 5th ACM/USENIX Internet Measurement Conference (IMC'07), October 2007.

[2] "Global internet use reaches 1 billion," http://www.comscore.com/press/release.asp?press=2698.

[3] "Facebook statistics, " http://www.facebook.com /press/info.php?statistics.

[4] A. Tootoonchian, K. K. Gollu, S. Saroiu, Y. Ganjali, and A. Wolman,"Lockr: social access control for web 2.0," in WOSP '08: Proceedings of the first workshop on Online social networks. New York, NY, USA:ACM, 2008, pp. 43–48.

[5] Becker, "Bluetooth security & hacks," http://gsyc.es/_anto/ubicuos2/bluetooth security and hacks.pdf.

[6] "Api - facebook developers wiki," http:// wiki. developers .facebook.com/ index.php/API.

[7] S. Guha, K. Tang, and P. Francis, "Noyb: privacy in online socialnetworks," in WOSn '08: Proceedings of the first workshop on Online social networks. New York, NY, USA: ACM, 2008, pp. 49–54.

[8] "Facebook connect," http://developers.facebook.com/ connect.php.

[9] Cutillo, R. Molva, and T. Strufe, "Privacy preserving social networking through decentralization," in WONS L 2009,

6th International Conference on Wireless On-demand Network Systems and Services. New York, NY, USA: ACM, 2007, pp. 357–366.
[10] Y. Katz and J. Golbec, "Using social network-based trust for defaultreasoning on the web," Journal of Web Semantics, 2007.

**Vijay Kumar Damera** received his B.E and M.Tech, from Osmania Univ. and JNTU in 2004 and 2010, respectively. He is working as a Assistant Professor (from 2006) in the Dept. of Information Technology ,MGIT, Hyderabad ,AP,India. His research interest includes Information Security, Compiler Design , Data Mining and Computer Forensics.

**Satya Shekar Varma** received his B.Tech and M.Tech, from JNT Univ. in 2006 and 2010, respectively. He is working as a Assistant Professor (from 2007) in the Dept. of Computer Science ,MGIT, Hyderabad ,AP,India. His research interest includes Information Security, Network Programming , Data Mining and Computer Algorithms.

**Shyam Sunder Pabboju** received his B.Tech and M.Tech, from JNT Univ. in 2005 and 2010, respectively. He is working as a Assistant Professor (from 2006) in the Dept. of Computer Science ,MGIT, Hyderabad ,AP,India. His research interest includes Information Security, Data Base Security , Data Mining and Ware housing